Verified Voting

February 23, 2026

The Honorable Melissa Wells
Chair
Government, Labor, and Elections Committee
Maryland House of Delegates
145 Lowe House Office Building
Annapolis, Maryland 21401
Via email

Dear Chair Wells and Committee Members,

On behalf of Verified Voting, I am writing in opposition to House Bill 1066 which would allow ballot return via the internet for certain voters. Verified Voting is a nonpartisan nonprofit organization with a mission to strengthen democracy for all voters by promoting the responsible use of technology in elections. Since our founding in 2004 by computer scientists, we have acted on the belief that the integrity and strength of our democracy rely on citizens' trust that each vote is counted as cast.

Ballot return via the internet (including mobile, email, fax, or website portal) fails to confer that trust. The security risks associated with electronic ballot return are severe, well-documented, and broadly acknowledged by the federal government's top security agencies and the nation's leading cybersecurity experts. At present, no known technology can secure ballots returned over the internet.

A joint analysis from the Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) classifies electronic ballot return as high risk, capable of enabling attacks that could alter or disrupt election results at scale. As stated in the analysis, "Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results and can occur at scale."[1]

Other agencies have been equally clear. The Department of Defense has stated that it does not advocate transmitting cast ballots electronically under any method.[2] The Department of Homeland Security has likewise advised that online voting is not recommended at any level of government at this time.[3]

Congress shares these concerns. The U.S. Senate Select Committee on Intelligence concluded that no system of online voting has yet established itself as secure, and urged states to resist

[1] CISA, EAC, FBI, and NIST, Risk Management for Electronic Ballot Delivery, Marking, and Return, 2020/2024.

[2] DOD statement quoted in Greg Gordon, McClatchy, April 16, 2015.

[3] DHS statement quoted in Sarah Horwitz, Washington Post, May 17, 2016.

adopting internet voting.[4]

Independent cybersecurity experts mirror these findings. A working group convened by the University of California, Berkeley—including pioneers in cryptography and election security—determined that the technology required to secure online ballot return does not exist today, and that a single attacker could potentially alter thousands or even millions of votes.[5] The group further emphasized that online voting lacks the basic safeguards present in other online transactions, because the secret ballot prevents voters from verifying that their vote was received and counted as cast. Currently, no certification standards exist for electronic ballot return systems.

Electronic ballot return also carries multiple unique vulnerabilities, including malware, denial-of-service attacks, spoofing, identity fraud, and breaches that could expose voters' private information.[6] Any one of these could compromise an election; several could do so without detection.

Recently, a group of computer scientists and security researchers reaffirmed that while electronic ballot return methodologies continue to be researched, it is still not yet suitable for use in public elections. According to this group, "it has been the scientific consensus for decades that internet voting is not securable by any known technology. Research on future technologies is certainly worth doing. However, the decades of work on [electronic ballot return] systems has yet to produce any solution, or even any hope of a solution, to the fundamental problems."[7]

For these reasons, we respectfully urge you to reject House Bill 1066 which would allow electronic ballot return for certain voters. Implementing electronic ballot return would run counter to the unified assessment of national security experts, cybersecurity professionals, federal intelligence agencies, and leading academic researchers. The risks—to ballot confidentiality, integrity, and public confidence—simply outweigh any potential benefits at this time.

We appreciate your leadership and your commitment to ensuring both accessibility and security in our elections.

Sincerely,

C.Jay Coles
Deputy Director of Legislative Affairs

[4] SSCI, Russian Active Measures, Vol. 1.

[5] UC Berkeley CSP, Working Group Statement on Internet Ballot Return, 2022.

[6] Ibid.

[7] Appel, Andrew, "Internet Voting Is Insecure and Should Not Be Used in Public Elections - CITP Blog, 2026."

BRENNAN CENTER FOR JUSTICE

February 23, 2026

The Honorable Melissa Wells
Chair
Government, Labor, and Elections Committee
Maryland House of Delegates
145 Lowe House Office Building
Annapolis, Maryland 21401

Dear Chair Wells and Committee Members:

I am writing to you on behalf of the Brennan Center for Justice at NYU School of Law to oppose House Bill 1066, which would enact law to allow the electronic return of marked ballots via the Internet for municipal elections. The Brennan Center is a national nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Brennan Center has a long history of partnering with election administrators, legislators, and other elected officials at the local, state, and federal level to reform and improve our elections and election administration.

Every independent review has found that we currently lack the technology to make electronic ballot return secure from attack. In 2020 and again in 2024, four federal executive branch agencies --the Cybersecurity and Infrastructure Security Agency (part of the Department of Homeland Security or DHS), the Election Assistance Commission, the Federal Bureau of Investigation, and the National Institute of Standards and Technology (NIST)-- jointly released a report concluding that internet-based return of votes presents a "high risk" to United States elections and cannot be secured.[1] It noted that, with internet-based ballot return, hackers from anywhere in the world could engage in large-scale, high-volume tampering with ballots that could impact results and possibly the outcome of an election. Two of these agencies have opined repeatedly on the issue over the years. In 2022, NIST issued the report *Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities* and notably did not include internet-based ballot return among its recommendations because, as it concluded, "there remain significant security, privacy, and ballot secrecy challenges."[2] In 2016, through its Office of Cybersecurity and Communications, DHS

[1] CISA et al., *Risk Management for Electronic Ballot Delivery, Marking, and Return*, at 1 (May 8, 2020).

[2] Kerrianne Buchanan et al., *NIST Spec. Pub. No. 1273, Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities*, at 48, 51 (Mar. 23, 2022).

stated that "online voting, especially online voting in large scale, introduces great risk into the election system by threatening voters' expectations of confidentiality, accountability and security of their votes and provides an avenue for malicious actors to manipulate the voting results."[3]

These agencies are not the only independent experts to opine on the issue. The Department of Defense has stated it "does not advocate for the electronic transmission of any voted ballot, whether it be by fax, email or via the Internet."[4] The United States Select Senate Committee on Intelligence concluded in a 2020 report that "States should resist pushes for online voting," because "no system of online voting has yet established itself as secure."[5] And a Working Group from the Center for Security in Politics at the University of California, Berkeley formed to determine "the feasibility of technical and implementation standards that would enable safe and secure digital remote ballot marking and return of these ballots" instead concluded "the current cybersecurity environment and state of technology makes it infeasible for the Working Group to draft responsible standards to support the use of internet ballot return in U.S. public elections at this time."[6]

Importantly, the consensus on the security challenges should be viewed within the current risk landscape. For at least a decade, our foreign adversaries—including Russia, China, and Iran—have launched cyberattacks targeting the United States' digital election infrastructure. They have done so in the 2016, 2018, 2020, 2022, and 2024 federal elections, with the goal of undermining confidence in our elections. At the same time, federal agencies have cut back on cyber and other election security support for local election offices.[7] Additionally, there is an active movement within the United States to undermine confidence in our elections, and we should not give it more oxygen through use of an untested and unproven technology for which there are currently no federal security standards.[8] Within this context, it is unwise for Maryland to adopt the use of electronic ballot return.

Of course, there are voters who face unique challenges casting their ballots and it is important to address those challenges -- but not with solutions that may put the security of their votes at risk or open them to challenge. There are many existing alternatives for casting ballots to electronic

---

[3] Sarah Horwitz, *More than 30 states offer online voting, but experts warn it isn't secure*, WASH. POST (May 17, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/.

[4] Greg Gordon, *As states warm to online voting, experts warn of trouble ahead*, MCCLATCHY WASHINGTON BUREAU (Apr. 16, 2015).

[5] See S. Rep. No. 116-290, at 61-62 (2020).

[6] R. Michael Alvarez et al., *Working Group Statement on Developing Standards for Internet Ballot Return*, CTR. FOR SEC. IN POL.,UNIV. OF CAL.,BERKELEY, at 2 (Dec. 2022).

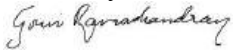
[7] Lawrence Norden, How the Federal Government Is Undermining Election Security, BRENNAN CENTER FOR JUSTICE (April 14, 2025).

[8] The Briefing, *Brennan Center Live:The Campaign to Undermine the Mid-terms* (YouTube, September 18, 2025).

ballot return, which is unproven and untested.[9] We are happy to explore those alternatives with you.

For these reasons, we respectfully urge you to reject House Bill 1066, which would allow electronic ballot return in municipal elections. We appreciate your leadership and commitment to ensuring both accessibility and security in our elections.

Sincerely,



Gowri Ramachandran
Director of Elections and Security, Elections & Government
Brennan Center for Justice at NYU School of Law

[9] Verified Voting, *Casting Votes Safely: Examining Internet Voting's Dangers and Highlighting Safer Alternatives (October 2023).*

RISK MANAGEMENT FOR ELECTRONIC BALLOT DELIVERY, MARKING, AND RETURN

INTRODUCTION

Some voters face challenges voting in-person and by mail. State and local election officials in many states use email, fax, web portals, and/or web-based applications to facilitate voting remotely for groups like military and overseas voters and voters with specific needs.

The Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) assess that the risks vary for electronic ballot delivery, marking, and return. While there are effective risk management controls to enable electronic ballot delivery and marking, we recommend paper ballot return as electronic ballot return technologies are high-risk even with controls in place. Recognizing that some election officials are mandated by state law to employ this high-risk process, its use should be limited to voters who have no other means to return their ballot and have it counted. Notably, we assess that electronic delivery of ballots to voters for return by mail is less vulnerable to systemic disruption.

In this document, we identify risks and considerations for election administrators seeking to use electronic ballot delivery, electronic ballot marking, and/or electronic return of marked ballots. The cybersecurity characteristics of these remote voting solutions are further explored in NISTIR 7551: A Threat Analysis on UOCAVA Voting Systems.

RISK OVERVIEW

	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
Technology Overview	Digital copy of blank ballot provided to voter	Making voter selections on digital ballot through the electronic interface	Electronic transmission of voted ballot
Risk Assessment	Low	Moderate	High
Identified Risks	Electronic ballot delivery faces security risks to the integrity and availability of a single voter's unmarked ballot	Electronic ballot marking faces security risks to the integrity and availability of a single voter's ballot	Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results and, can occur at scale

All states use **electronic ballot delivery** to transmit a digital copy of an unmarked ballot to the intended voter to mark, in compliance with the Military and Overseas Voters Empowerment Act (MOVE). These ballot delivery systems are exposed to typical information security risks of internet-connected systems. The most severe risks to electronic ballot delivery systems are those that would impact the integrity and/or availability of the ballots, such as altering or removing ballot choices. These risks can be reduced and managed through use of appropriate security controls. Additionally, some electronic ballot delivery systems perform functions to verify a voter's identity before presenting them their assigned ballot. The identification process can use personal identifying information, such as name and driver's license number, or biometrics. When this verification is improperly configured, remote electronic ballot delivery systems can present additional privacy risks—like the loss or theft of the voter's personal and/or biometric identity information. These risks may be managed through configuration management and appropriate security controls.

Electronic ballot marking allows voters to mark their ballots outside of a voting center or polling place. Typically, this describes the electronic marking of a digital copy of the blank ballot using the electronic interface. The marked ballot is then returned to the appropriate official. Risks to electronic ballot marking are best managed through the production of an auditable record, meaning the voted ballot is printed and verified by the voter before being routed to the appropriate official. This auditable record is an important compensating control for detecting a compromise of security in remote voting.

Electronic ballot return, the digital return of a voted ballot by the voter, creates significant security risks to the confidentiality of ballot and voter data (e.g., voter privacy and ballot secrecy), integrity of the voted ballot, and availability of the system. We view electronic ballot return as high risk.

Securing the return of voted ballots via the internet while ensuring ballot integrity and maintaining voter privacy is difficult, if not impossible, at this time. As the National Academies of Science, Engineering, and Medicine write in Securing the Vote: Protecting American Democracy (2018), "We do not, at present, have the technology to offer a secure method to support internet voting. It is certainly possible that individuals will be able to vote via the internet in the future, but technical concerns preclude the possibility of doing so securely at present." If election officials choose or are mandated by state law to employ this high-risk process, its use should be limited to voters who have no other means to return their ballot and have it counted. Further, election officials should have a mechanism for voters to check the status of their ballot, as required for provisional ballots and military and overseas voters by the Help America Vote Act and the MOVE Act, respectively.

RISK COMPARISON – ELECTRONIC AND MAILED BALLOT RETURN

Some risks of electronic ballot return have a physical analogue to the return mailing of ballots. However, electronic systems present far greater risk to impact a significant number of ballots in seconds.

- **Scale –** While mailing of ballots could be vulnerable to localized exploitation, electronic return of ballots could be manipulated at scale. For mailed ballots, an adversary could theoretically gain physical access to a mailed ballot, change the contents, and reinsert it into the mail. This physical man-in-the-middle (MITM) attack is limited to low-volume attacks and mitigated by proper chain of custody procedures by election officials. In comparison, an electronic MITM attack could be conducted from anywhere in world, at high volumes, and could compromise ballot confidentiality, ballot integrity, and/or stop ballot availability.
- **Bring Your Own Device –** Unlike traditional voting systems, electronic ballot delivery and return systems require a voter to use their own personal devices such as a cell phone, computer, or tablet to access the ballot. A voter's personal device may not have the necessary safeguards in place. As a result, votes cast through "bring your own device" voting systems may appear intact upon submission despite tampering as a result of an attack on the personal device rather than on the ballot submission application itself. Voters using personal devices increase the potential for an electronic ballot delivery and return system to be exposed to security threats.
- **Voter Privacy –** Electronic ballot return brings significant risk to voter privacy. Unlike traditional vote by mail where there is separation between the voter's information and their ballot, many remote voting systems link the two processes together digitally. This makes it difficult to implement strong controls that preserve the privacy of the voter while keeping the system accessible.

TECHNICAL CONSIDERATIONS FOR ELECTRONIC BALLOT RETURN

Some voters, due to specific needs or remote locations, may not be able to print, sign, and mail in a ballot without significant difficulty. While we assess electronic ballot return to be high risk, some jurisdictions already use electronic ballot return systems, and others may decide to assume the risk.

While risk management activities should lower risk, election officials, network defenders, and the public may all have different perspectives on what level of risk is acceptable for the systems used to administer an election. For those jurisdictions that have accepted the high risk of electronic ballot return, the following guidance identifies cybersecurity best practices for internet- and network-connected election infrastructure. The information provided should be considered a starting point and is not a comprehensive list of defensive cybersecurity actions. Even with these technical security considerations, electronic ballot return remains a high-risk activity. Refer to applicable standards, best practices, and guidance on secure system development, acquisition, and usage.

GENERAL

- All election systems and technology should be completely separated from systems that are not required for the implementation or use of that specific system.
- Any ballots received electronically should be printed or remade as a paper record.
- Election officials should implement processes to separate the ballot from the voter's information in a manner that maintains the secrecy of the ballot.

- If the system attempts to verify the voter's identity through digital signature, biometric capture, or other method, assess whether an attacker could use this to violate ballot secrecy.
- The auditability of the results should not rely solely on the data stored digitally within the system.
- Best practices for securing voter registration data should be used to protect the personal identifying information that is stored in the voter registration database and used to authenticate voters.
- Removable storage media (e.g., USB drives, compact flash cards) used to handle sensitive election data should be obtained from a trusted source and erased before being used. To the extent practical, removable storage media should be new.
- Follow the domain security best practices issued by the Federal Government available at https://home.dotgov.gov/management/security-best-practices/

FAX

Facsimile (fax) machines are often used by local election offices and voters. While this may be a convenient tool for distributing or receiving ballots, policy makers should be aware of the risks and challenges associated with fax. Fax has no security protections unless sent over a secured phone line and is generally not considered suitable for sensitive communications. Faxes may be viewed or intercepted by malicious actors with access to phone lines. Furthermore, multipurpose fax machines with networked communications capability can be leveraged by cyber actors to compromise other machines on the network. We recommend election officials using fax machines implement the following best practices.

- Use a no-frills fax machine; multipurpose fax machines typically have modems for external network communications. If you only have a multipurpose fax machine, turn off the Wi-Fi capability and do not plug it into the network—only connect it to the phone line.
- Check the configuration to make sure that the fax cannot print more pages than anticipated from a single fax or ballot package.
- Use a dedicated fax machine and fax line for the distribution and receipt of ballots. Do not make the phone number publicly available, and only provide it in the electronic ballot package for voters who have been authorized to vote using electronic return.
- Election officials should set up transmission reports when faxing a ballot package to the voter to verify that the ballot package was received by the fax machine it was sent to.
- Use a trusted fax machine that has been under your control. Ensure you have enough fax machines and phone lines to handle the anticipated volume.
- When a public switch telephone line (PSTN) fax machine is not available and internet Protocols are used to fax, treat these systems as internet-connected systems, not as a fax machine using telephone protocols.

EMAIL

Email is a nearly ubiquitous communications medium and is widely used by election offices and voters. While this may be a convenient tool for distributing or receiving ballots, policy makers and election officials should be aware of the risks and challenges associated with email. Email provides limited security protections and is generally not considered suitable for sensitive communications. Email may be viewed or tampered with at multiple places in the transmission

process, and emails can also be forged to appear as if they were sent from a different address. Furthermore, email is often used in cyberattacks on organizations, such as attackers sending messages with malicious links or attachments to infect computers with malware. This malware could spread to other machines on the network if strong network segmentation techniques are not used.

- Use a dedicated computer that is separated from the remainder of the election infrastructure to receive and process these ballots. For very small offices that may not have the resources to use a dedicated computer, a virtual machine should be installed to separate these devices.
- Patch and configure the computer—as well as document viewer software—against known vulnerabilities (e.g., disable active content, including JavaScript and macros.).
- If possible, implement the .gov top-level domain (TLD). The .gov TLD was established to identify U.S.-based government organizations on the internet.
- Use encryption where possible (e.g., implement STARTTLS on your email servers to create a secure connection, encrypt attached files, etc.)
- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to help identify phishing emails.
- Implement DMARC, DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) on emails to help authenticate emails sent to voters.
- Utilize anti-malware detection and encourage voters to as well. Make sure to update the anti-malware regularly.
- Implement multi-factor authentication (MFA) on any email system used by election officials.
- Follow best practices for generating and protecting passwords and other authentication credentials.
- Use a dedicated, shared email address for receiving ballots, such as Ballots@County.Gov. Implement naming conventions in subject lines that will help identify emails as legitimate (e.g., 2020 Presidential General). While a dedicated, shared email account is typically not a best practice, in this instance, it segregates potentially malicious attachments from the network.

WEB-BASED PORTALS, FILE SERVERS, AND APPLICATIONS

Websites may provide accessible and user-friendly methods for transmitting ballots and other election data. While web applications support stronger security mechanisms than email, they are still vulnerable to cyberattacks. Software vulnerabilities in web applications could allow attackers to modify, read, or delete sensitive information, or to gain access to other systems in the elections infrastructure. Sites that receive public input, such as web forms or uploaded files, may be particularly vulnerable to such attacks and should be used only after careful consideration of the risks, mitigations, and security/software engineering practices that went into that software.

- Avoid using knowledge-based authentication (e.g., address, driver's license number, social security number). To the extent practical, implement MFA for employees and voters and mandate MFA for all system administrators and other technical staff (including contractors).
- Patch and configure computers as well as document viewer software against known vulnerabilities (i.e., disable active content, including JavaScript and macros.).

- If possible, implement the .gov top-level domain (TLD). The .gov TLD was established to identify US-based government organizations on the internet.
- Use secure coding practices (e.g., sanitized inputs, parameter checking) for web applications.
- Encrypt traffic using Hypertext Transfer Protocol Secure (HTTPS) supporting Transport Layer Security (TLS) version 1.2. If you use a file server, ensure it uses a secure file transfer protocol, such as SFTP or FTPS.
- Ensure you have the bandwidth/capacity to handle the anticipated volume of traffic.
- Obtain outside cybersecurity assessments, such as CISA vulnerability scanning and remote penetration testing.
- Develop a vulnerability management program (VMP). This allows well-meaning cybersecurity researchers to find and disclose vulnerabilities privately to an election official, giving the election official time to implement upgrades and patches before disclosing the information publicly.
- Place the application on a network that is continuously monitored, such as the network with a web application firewall, an Albert sensor, or an intrusion detection and prevention system.
- Carefully vet any third-party companies or contractors obtaining system access to perform security assessments or regular maintenance.
- Inform voters to only download the application from the trusted mobile application store.
- Encourage voters to use a trusted network and not an open Wi-Fi network.

RESOURCES

- CISA services can be located in the CISA Election Infrastructure Security Resource Guide. All services can be requested at cisaservicedesk@cisa.dhs.gov.
- Become an EI-ISAC Member by going to https://www.cisecurity.org/ei-isac/.
- CISA's Binding Operational Directive (BOD)18-01 addresses enhancing email and web security.
- NIST Activities on UOCAVA Voting
- NIST special publication (SP) 800-177 provides recommendations and guidelines for enhancing trust in email.
- NIST SP 800-52r2 provides guidelines for selection, configuration, and use of TLS.
- FBI's Protected Voices initiative provides information and guidance on cybersecurity and foreign influence topics.
- The EAC's Election Security Preparedness webpage collects multiple resources that can assist election administrators.
- For more information about how election jurisdictions in the United States vote remotely, please see Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes.

APPENDIX: DETAILED RISK MAPPING

TECHNOLOGY	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
RISK: Exploitation of software flaws in election infrastructure			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	High
Web	High	High	High
RISK: Unauthorized modification(s) to blank ballots			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	N/A
Web	Low	Moderate	N/A
RISK: Loss of voted ballot integrity			
Fax	N/A	N/A	High
Email	N/A	N/A	High
Web	N/A	N/A	High
Risk: Loss of ballot secrecy			
Fax	N/A	N/A	Moderate
Email	N/A	N/A	High
Web	N/A	N/A	High
RISK: Unauthorized individual participates in voting channel			
Fax	Moderate	N/A	High
Email	Low	Low	High
Web	Low	Moderate	High

TECHNOLOGY	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
Risk: Broken Chain of Custody			
Fax	Low	N/A	Moderate
Email	Moderate	Moderate	High
Web	Low	Moderate	Moderate
RISK: Unable to access system or obtain ballot			
Fax	Low	N/A	Moderate
Email	Moderate	Moderate	High
Web	Moderate	High	High

Internet voting is insecure and should not be used in public elections

January 16, 2026

https://blog.citp.princeton.edu/2026/01/16/internet-voting-is-insecure-and-should-not-be-used-in-public-elections/

Signed by a group of 21 computer scientists expert in election security

Executive summary

Scientists have understood for many years that internet voting is insecure and that there is no known or foreseeable technology that can make it secure. Still, vendors of internet voting keep claiming that, somehow, their new system is different, or the insecurity doesn't matter. Bradley Tusk and his Mobile Voting Foundation keep touting internet voting to journalists and election administrators; this whole effort is misleading and dangerous.

Part I. All internet voting systems are insecure. The insecurity is worse than a well-run conventional paper ballot system, because a very small number of people may have the power to change any (or all) votes that go through the system, without detection. This insecurity has been known for years; every internet voting system yet proposed suffers from it, for basic reasons that cannot be fixed with existing technology.

Part II. Internet voting systems known as "End-to-End Verifiable Internet Voting" are also insecure, in their own special ways.

Part III. Recently, Tusk announced an E2E-VIV system called "VoteSecure." It suffers from all the same insecurities. Even its developers admit that in their development documents. Furthermore, VoteSecure isn't a complete, usable product, it's just a "cryptographic core" that someone might someday incorporate into a usable product.

Conclusion. Recent announcements by Bradley Tusks's Mobile Voting Foundation suggest that the development of VoteSecure somehow makes internet voting safe and appropriate for use in public elections. This is untrue and dangerous. All deployed Internet voting systems are unsafe, VoteSecure is unsafe and isn't even a deployed voting system, and there is no known (or foreseeable) technology that can make Internet voting safe.

Part I. All internet voting systems are insecure

Internet voting systems (including vote-by-smartphone) have three very serious weaknesses:

1. Malware on the voter's phone (or computer) can transmit different votes than the voter selected and reviewed. Voters use a variety of devices (Android, iPhone, Windows, Mac) which are constantly being attacked by malware.
2. Malware (or insiders) at the server can change votes. Internet servers are constantly being hacked from all over the world, often with serious results.
3. Malware at the county election office can change votes (in those systems where the internet ballots are printed in the county office for scanning). County election computers are not more secure than other government or commercial servers, which are regularly hacked with disastrous results.

Although conventional ballots (marked on paper with a pen) are not perfectly secure either, the problem with internet ballots is the ability for a single attacker (from anywhere in the world) to alter a very large number of ballots with a single scaled-up attack. That's much harder to do with hand-marked paper ballots; occasionally people try large-scale absentee ballot fraud, typically resulting in their being caught, prosecuted, and convicted.

Part II. E2E-VIV internet voting systems are also insecure

Years ago, the concept of "End-to-End Verifiable Internet Voting" (E2E-VIV) was proposed, which was supposed to remedy some of these weaknesses by allowing voters to check that their vote was recorded and counted correctly. Unfortunately, all E2E-VIV systems suffer from one or more of the following weaknesses:

1. Voters must rely on a computer app to do the checking, and the checking app (if infected by malware) could lie to them.
2. Voters should not be able to prove to anyone else how they voted – the technical term is "receipt-free" – otherwise an attacker could build an automated system of mass vote-buying via the internet. But receipt-free E2E-VIV systems are complicated and counterintuitive for people to use.
3. It's difficult to make an E2E-VIV checking app that's both trustworthy and receipt-free. The best solutions known allow checking only of votes that will be discarded, and casting of votes that haven't been checked; this is highly counterintuitive for most voters!
4. The checking app must be separate from the voting app, otherwise it doesn't add any malware-resistance at all. But human nature being what it is, only a tiny fraction of voters will do the extra steps to run the checking protocol. If hardly anyone uses the checker, then the checker is largely ineffective.

5. Even if some voters do run the checking app, if those voters detect that the system is cheating (which is the purpose of the checking app), there's no way the voters can prove that to election officials. That is, there is no "dispute resolution" protocol that could effectively work.

Thus, the problem with all known E2E-VIV systems proposed to date is that the "verification" part doesn't add any useful security: if a few percent of voters use the checking protocol and see that the system is sometimes cheating, the system can still steal the votes of all the voters that don't use the checking protocol. And you might think, "well, if some voters catch the system cheating, then election administrators can take appropriate action", but no appropriate action is possible: the election administrator can't cancel the election just because a few voters claim (without proof) that the system is cheating! That's what it means to have no dispute resolution protocol.

All of this is well understood in the scientific consensus. The insecurity of non-E2E-VIV systems has been documented for decades. For a survey of those results, see "Is Internet Voting Trustworthy? The Science and the Policy Battles". The lack of dispute resolution in E2E-VIV systems has been known for many years as well.

Part III. VoteSecure is insecure

Bradley Tusk's Mobile Voting Foundation contracted with the R&D company Free and Fair to develop internet voting software. Their press release of November 14, 2025 announced the release of an open-source "Software Development Kit" and claimed "This technology milestone means that secure and verifiable mobile voting is within reach."

After some computer scientists examined the open-source VoteSecure and described serious flaws in its security, Dr. Joe Kiniry and Dr. Daniel Zimmerman of Free and Fair responded. They say, in effect, that all the critiques are accurate, but they don't know a way to do any better: "We share many of [the critique's] core goals, including voter confidence, election integrity, and resistance to coercion. Where we differ is not so much in values as in assumptions about what is achievable—and meaningful—in unsupervised voting environments."

In particular,

- "We make no claim of receipt-freeness."
- "Of course, it may be possible for the voter to extract the randomizers from the voting client," meaning that voters would be able to prove how they voted, for example to someone on the internet who wanted to purchase votes at scale.
- "We agree that dispute resolution is essential to any *complete* voting system. We also agree that VoteSecure does not fully specify such a protocol." But really, the problem is much worse than this admission suggests. No one knows of a protocol

that could possibly work. So it's not a matter of dotting some i's and crossing some t's in their specification; it's a gaping hole (an unsolved, research-level problem).
- "Critique: Malware on the voter's device can compromise both voting and checking, rendering verification meaningless. Response: This critique is correct—and universal. There is no known technical solution that can fully protect an unsupervised endpoint from a sufficiently capable adversary."
- "VoteSecure does not claim to: Advance the state of the art in cryptographic voting protocols beyond existing E2E-VIV research; Eliminate coercion or vote selling in unsupervised elections; [or] Fully specify election administration, dispute resolution, or deployment processes. What VoteSecure aims to do is: Clearly define its threat model . . ."

In addition to the previously described flaws in the VoteSecure protocol, we note that its vote checking system is susceptible to mass automated vote-buying attacks[1]; and we have discovered a new flaw in the VoteSecure protocol that allows votes to be stolen[2]. *[click for details]*[1] This conclusion is based on a technical analysis. In the VoteSecure protocol, checking app can be run on a vote that is then cast; the checking app must be runnable on an alternate device than the voting app; that alternate device is likely a PC on which the user has control of installed software; user-installed software can extract decrypted randomizers; this allows the voter to participate in a mass vote-buying scheme. [2] "Clash attacks on the VoteSecure voting and verification process", by Vanessa Teague and Olivier Pereira, January 13, 2026.

Based on our own expertise test, and especially in light of the response from Free and Fair, we stand by the original analysis: Mobile Voting Project's vote-by-smartphone has critical security gaps.

Conclusion

It has been the scientific consensus for decades that internet voting is not securable by any known technology. Research on future technologies is certainly worth doing. However, the decades of work on E2E-VIV systems has yet to produce any solution, or even any hope of a solution, to the fundamental problems.

Therefore, when it comes to internet voting systems, election officials and journalists should be especially wary of "science by press release." Perhaps some day an internet voting solution will be proposed that can stand up to scientific investigation. The most reliable venue for assessing that is in peer-reviewed scientific articles. Reputable cybersecurity conferences and journals have published a lot of good science in this area. Press releases are not a reliable way to assess the trustworthiness of election systems.

Signed

(affiliations for for identification only and do not indicate institutional endorsement)

Andrew W. Appel, *Eugene Higgins Professor Emeritus of Computer Science, Princeton University*

Steven M. Bellovin, *Percy K. and Vida L.W. Hudson Professor Emeritus of Computer Science, Columbia University*

Duncan Buell, *Chair Emeritus — NCR Chair in Computer Science and Engineering, University of South Carolina*

Braden L. Crimmins, *PhD Student, Univ. of Michigan School of Engineering & Knight-Hennessy Scholar, Stanford Law*

Richard DeMillo, *Charlotte B and Roger C Warren Chair in Computing, Georgia Tech*

David L. Dill, *Donald E. Knuth Professor, Emeritus, in the School of Engineering, Stanford University*

Jeremy Epstein, *National Science Foundation (retired) and Georgia Institute of Technology*

Juan E. Gilbert, *Andrew Banks Family Preeminence Endowed Professor, Computer & Information Science, University of Florida*

J. Alex Halderman, *Bredt Family Professor of Computer Science & Engineering, University of Michigan*

David Jefferson, *Lawrence Livermore National Laboratory (retired)*

Douglas W. Jones, *Emeritus Associate Professor of Computer Science, University of Iowa*

Daniel Lopresti, *Professor of Computer Science and Engineering, Lehigh University*

Ronald L. Rivest, *Institute Professor, MIT*

Bruce Schneier, *Fellow and Lecturer at the Harvard Kennedy School, and at the Munk School at the University of Toronto*

Kevin Skoglund, *President and Chief Technologist, Citizens for Better Elections*

Barbara Simons, *IBM Research (retired)*

Michael A. Specter, *Assistant Professor, Georgia Tech*

Philip B. Stark, *Distinguished Professor, Department of Statistics, University of California*

Gary Tan, *Professor of Computer Science & Engineering, The Pennsylvania State University*

Vanessa Teague, *Thinking Cybersecurity Pty Ltd and the Australian National University*

Poorvi L. Vora, *Professor of Computer Science, George Washington University*