Email and Internet Voting:

The Overlooked Threat to Election Security

By

Susan Greenhalgh
National Election Defense Coalition

Susannah Goodman
Common Cause Education Fund

Paul Rosenzweig
R Street Institute

Jeremy Epstein
ACM US Technology Policy Committee

Acknowledgements

The authors would like to thank Dr. James Hendler and Adam Eisgrau of ACM and its US Technology Policy Committee, Matt Bernhard, Duncan Buell, David Jefferson, Joe Kiniry, Lyell Read, and Dan Zimmerman. A special thank you goes to Joe Maschman, Common Cause legal fellow for his initial work. Common Cause and the National Election Defense Coalition would like to thank the Wallace Global Fund, the Rockefeller Brothers Fund, the Threshold Foundation, Philip and Janice Levin Foundation, and Marion Edey.

FOREWORD

In the armed services, our primary mission is to defend the United States. I served overseas and was assigned to intelligence and security posts in the Middle East and around the globe, where I was trained to think like an adversary, to look for vulnerabilities that I could exploit. Clearly, internet voting introduces that type of vulnerability. This report and a decade's worth of research conclude that we need to shut down this critical attack vector for our adversaries.

Men and women in uniform risk their lives every day to defend our democracy. In this growing cyberthreat environment, online voting endangers the very democracy they are charged with protecting. We owe our service personnel a means of voting in which they are assured that their votes cannot be compromised and used against the very democratic institutions they are sworn to protect.

-Retired Lt. Colonel Anthony Shaffer

Retired Lt. Col. Anthony Shaffer is a senior fellow with the London Center for Policy Research, national security expert, and recipient of the Bronze Star with 30 years of field and operational experience

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Over the past two years, revelations that our election systems have been targeted for cyberattack have roiled the United States. Leaders of our national security apparatus have repeatedly warned that our election infrastructure continues to be targeted for online attacks by foreign intelligence. As state election officials grapple with the looming threat of cyberattack on election technology, there is a significant vulnerability that has been roundly ignored: transmission of ballots over the internet, including by email, fax and web portal.

This report reviews the research that has been conducted by the federal government concluding that secure online voting is not yet feasible. We examine the insoluble security problems that are inherent to casting ballots online, including server penetration attacks, client-device malware, attacks to emailed and faxed ballots in transit, denial-of-service attacks, disruption attacks and the challenge to reliably authenticate voters.

The report foregrounds a serious, yet widely overlooked cybersecurity threat to state and county election infrastructure that receive ballots sent as attachments in the form of emails or digital faxes. In jurisdictions that receive ballots by PDF or JPEG attachment, election workers must routinely click on documents from unknown sources to process emailed or faxed ballots, exposing the computer receiving the ballots — and any other devices on the same network — to a host of cyberattacks that could be launched from a false ballot laden with malicious software. An infected false ballot would enter the server like any other ballot, but once opened, it would download malware that could give attackers backdoor access to the elections office's network.

A review of publications on security best practices from the U.S. Election Assistance Commission (EAC), the Department of Homeland Security (DHS) and the National Association of Election Officials found no published guidance regarding the security of emailed ballots or recommendations for securing a computer terminal receiving emailed ballots.

Findings:

- Federal government, military and private sector studies have examined the feasibility of internet-based voting and have concluded it is not secure and should not be used in U.S. government elections.
- Thirty-two states permit online voting for some subset of voters.
- In the 2016 general election, over 100,000 ballots were reported to have been cast online, according to data collected in the EAC's Election Administration and Voting Survey. The actual number is likely much higher.
- The federal agencies supporting states in improving their election security have not issued any warnings regarding the online return of voted ballots.
- Ballots returned online can be undetectably changed by a variety of cyberattacks, including via malware on a user's computer and server penetration attacks. The latter has been demonstrated live and in a "test" election.
- Internet voting expands the opportunity for an attacker to engage in damaging disruption and denial-of-service attacks, aimed at disabling the system, prohibiting voters from casting ballots, and undermining voter trust in the election.
- Receiving ballots as attachments can also expose a state or county election system to systemic election system attacks. Sophisticated attackers can spoof a legitimate voter's emails and use fake ballots to deliver malware that can be used to gain entry into county or state election infrastructure.
- New technologies, including blockchain, fail to resolve the insoluble security issues inherent with online voting. These issues include server penetration attacks, client-device malware, denial-of-service attacks and disruption attacks.

Conclusion

Until there is a major technological breakthrough in or fundamental change to the nature of the internet, the best method for securing elections is a tried-and-true one: mailed paper ballots. Paper ballots are not tamper-proof, but they are not vulnerable to the same wholesale fraud or manipulation associated with internet voting. Tampering with mailed paper ballots is a one-at-a-time attack. Infecting voters' computers with malware or infecting the computers in the elections office that handle and count ballots are both effective methods for large-scale corruption.

Military voters undoubtedly face greater obstacles in casting their ballots. They deserve any help the government can give them to participate in democracy equally with all other citizens. However, in this threat-filled environment, online voting endangers the very democracy the U.S. military is charged with protecting.

Considering current technology and current threats, postal return of a voted ballot is the most responsible option. States that permit online return of voted ballots should suspend the practice. Federal agencies such as DHS and EAC should acknowledge the vulnerabilities introduced by permitting online voting and recommend that states curtail all online ballot return. Until they do, the integrity of Americans' votes is at stake, and in many cases, the integrity of the election system is at risk.

Summary Recommendations

We recommend some basic precautions that election officials and voters should follow. [A comprehensive set of recommendations is at the end of this report.]

Recommendations for election administrators:

- Map the network to ensure that the computer used to receive emailed or digitally faxed ballots is *not* connected to or on the same network as the voting machine network, election management system (EMS) or voter registration system through the wired or wireless means.
- Scan all incoming email and digital attachments for malware. The mail program should be configured to verify that attachments are of the expected type and fall into the typical size range. **Important**: Scanning may find attachments for executable malware programs but may be unable to detect malware *inside* a PDF or JPEG file. Malware inside such files is much more complex.
- Ensure all ballots returned by electronic means are printed for counting and not electronically transmitted to the EMS for tallying.
- Provide all voters with information and options for mailing ballots back by postal mail.
- Ensure military voters are aware of the free expedited postal mail option available to them.

Recommendations for voters:

- Voters who receive blank ballots in the mail are encouraged to mark the ballots and mail them back.
- Voters who receive blank ballots by email are encouraged to print out the ballot and mark it by hand if possible. If marking the ballot using a computer, print out the final version and carefully review the choices before mailing it back.
- Send the ballot back by postal mail. Military personnel in army, fleet or diplomatic post office (APO/FPO/DPO) locations can return absentee ballots via Priority Mail Express using the free Express Mail Label 11-DOD.

After the 2018 general election, states that permit online return of voted ballots should eliminate the practice. This will require legislative action in most states. While imposing a quarantine on incoming ballots is helpful, that will by no means stop a sophisticated attacker from attempting to use ballots in a spear phishing attack or corrupting ballots in transit. Additionally, federal agencies charged with assisting states in strengthening their election security should exercise leadership and publish warnings regarding the online return of voted ballots.

INTRODUCTION

Over the past two years, the United States has been roiled by revelations that our election systems have been the target of nation-state-sponsored cyberattacks. There has been an unprecedented level of attention paid to the security of U.S. election infrastructure. Leaders of our national security apparatus have repeatedly warned that our election infrastructure continues to be targeted for online attacks by foreign intelligence.[1] As state election officials grapple with the looming threat of cyberattack on election technology, there is a significant vulnerability that has been roundly ignored: transmission of ballots over the internet, including by email and fax. In discussions regarding the integrity of our election system, it has been frequently stated that voting equipment would be difficult to hack because voting machines themselves are not connected to the internet. Though this claim is, in itself is incorrect,[2] it completely disregards the fact that thousands of ballots are routinely cast over the internet.

BACKGROUND

Internet Voting Persists in the U.S. Despite Research and Warnings

Casting ballots over the internet is recognized as an action especially vulnerable to cyberattacks. Because election laws in the U.S. call for secret ballots, there is no mechanism to check a ballot cast online to be sure it was not manipulated. Therefore, online voting is particularly susceptible to undetectable hacking. Yet, as we receive regular warnings that our elections are the target of foreign adversaries, 32 states allow some subset of voters to return ballots by email,[3] fax or internet portal. For most states this is allowed only for military and overseas voters. However, in Alaska, all voters may vote absentee, and all absentee voters may return ballots electronically[4] by fax.[5] In Hawaii, permanent absentee voters who do not receive a mailed ballot within five days of the election are permitted to return the ballot electronically, via email.[6] In Utah, overseas and military voters as well as voters with disabilities may return ballots electronically.[7]

Online voting has persisted despite ample research and widespread agreement that it is not possible to reliably authenticate voters and securely transmit ballots over the internet. For years, experts in the private sector, government and military have studied the feasibility of internet-based voting. The consistent conclusion is unqualified: it is impossible to ensure that votes cast through the internet cannot be cast fraudulently, undetectably manipulated or simply deleted. Below is a timeline of such research:

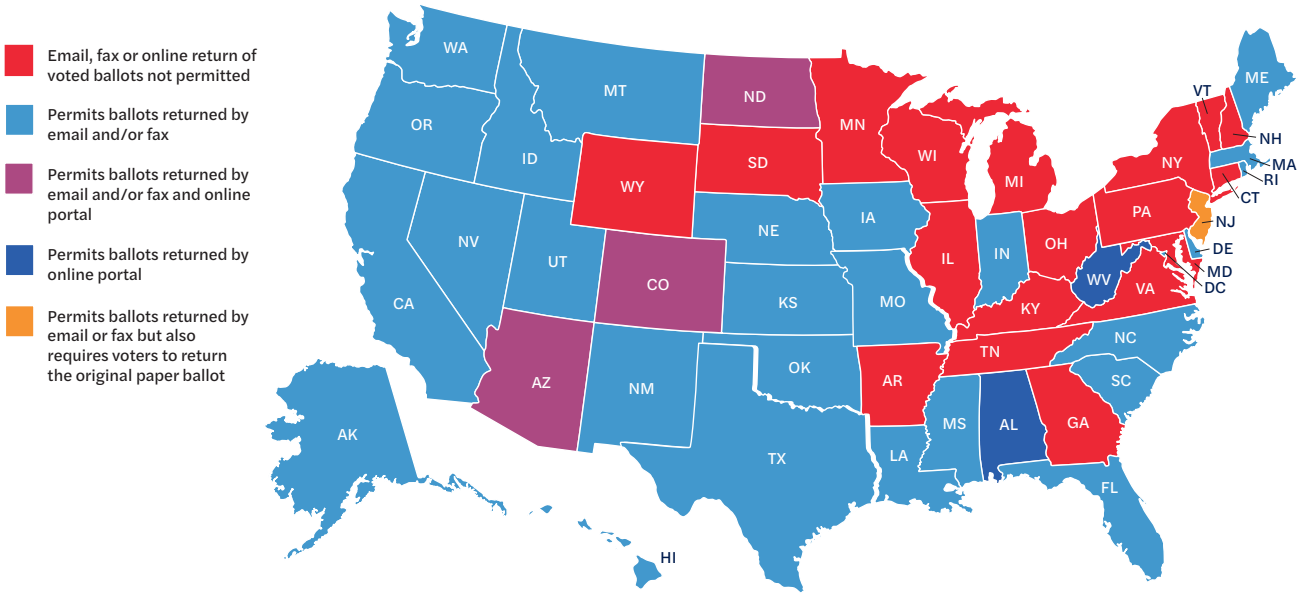
- In 2002, recognizing that military and overseas voters face unusual challenges in voting, Congress aimed to address those difficulties. It directed the Department of Defense (DOD) to develop an online ballot return system for military and overseas voters.
- In 2004, Deputy Secretary of Defense Paul Wolfowitz canceled a DOD online voting pilot program because security reviews warned that it's not possible to ensure that ballots sent over the internet would be legitimate.[8]
- In 2005, Congress tasked the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST) with studying online and email ballot return and developing standards for a secure, remote electronic absentee voting system. The research, conducted over several years, has been documented in multiple reports. NIST identified several obstacles to reliably authenticating voters' identities and transmitting ballots securely that cannot yet be reasonably overcome. In 2011, NIST issued a summary of its research and a statement concluding that secure electronic ballot transmission was not yet feasible.[9]
- In response to NIST's research, in the 2015 National Defense Authorization Act, Congress repealed its 2002 directive to DOD to create an online voting system for overseas and military voters.[10]
- In 2008, 32 respected computer scientists issued a cautionary statement that "serious, potentially insurmountable" challenges stood in the way of creating a safe internet-based voting system.[11]

- In 2015, the Pentagon affirmed that the DOD "does not advocate for the electronic transmission of any voted ballot, whether it be by fax, email or via the Internet."[12]
- In 2016, an official with the Office of Cybersecurity and Communications in the Department of Homeland Security (DHS) stated: "We believe 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."[13]
- In 2018, the National Academies of Sciences, Engineering, and Medicine released a report, "Securing the Vote: Protecting American Democracy," concluding "***At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place***, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet."[14]

These conclusions were not formed hastily. They were reached after years of research, funded by tens of millions of dollars from the federal government and the private sector.

In response to threats of Russian interference in its 2017 presidential election, France suspended all online voting for its citizens living abroad.[15] In the U.S., there has been worryingly little acknowledgment — or even understanding — of the threat posed by casting ballots over the internet.

Only two states have addressed the high vulnerability of online ballot transmission in light of the current nation-state threats we face. Alaska's lieutenant governor discontinued the use of an online ballot transmission system in 2018, which facilitated and encouraged online ballot transmission.[16] However, it is important to note that even though the web portal was discontinued, voters may still return ballots electronically in Alaska by fax.[17] Washington's secretary of state issued an emergency rule rescinding permission for voters other than military and overseas voters to return ballots over the internet. This action reversed regulations issued by Washington's secretary of state that allowed **all** voters to return ballots by email or fax. The secretary acted just as "white hat" hackers demonstrated ways to hack an emailed ballot at the August DEF CON hackers conference in Las Vegas.[18] In both Alaska and Washington, the chief election officers used legal authority to implement these changes which were important but limited in scope. These states and most others will require further action by their legislatures to discontinue all online voting.



Reported Number of Ballots Received Through Electronic Means

We are unable to accurately quantify the number of ballots that are cast online because this data is not collected consistently or uniformly by the states and counties. In many states the method of ballot return is not recorded at all. The EAC included a question requesting this data in its 2016 Election Administration and Voting Survey (EAVS),[19] however the data set is incomplete because many counties and states did not respond to the question. The EAC did not publish the responses in the survey report,[20] instead the data from the jurisdictions that did respond were given to the Federal Voting Assistance Program which posted it online.[21]

We aggregated the data reported by the counties to the EAVS and posted by FVAP and found that around 100,000 ballots were *reported* to be received via the internet in the 2016 elections.[22] [See Appendix] However, we expect this number to be profoundly underreported. Sixteen states, (Delaware, Florida, Iowa, Idaho, Kansas, Massachusetts, Missouri, Mississippi, New Jersey, New Mexico, North Carolina, Oklahoma, Oregon, Rhode Island, South Carolina, and Utah) all allow online return of voted ballots either through digital fax, email or online portal but none of their counties responded to the question. In other states, such as Arizona and Texas, where some counties did provide a response many others did not, suggesting the total number of ballots returned electronically for the whole state may be higher. Moreover, in our review, we discovered errors in the reporting.[23] Notwithstanding errors in reporting and incompleteness, the data available points to at a minimum, approximately 100,000 ballots returned by online methods in the 2016 general election.

Given the Risks, Why Online Voting?

The ample evidence that ballots cast over the internet could be cast fraudulently or be undetectably altered begs the question: Why did states pass legislation and adopt regulations to permit a highly insecure voting process?

When considering why so many states currently permit online voting, it is important to take into account historical context and the role of the DOD and its FVAP. Most states that permit electronic ballot return began to do so in the late 20th century or the first decade of the 2000s. At that time, the risks of hacking were not as commonplace as they are today, and cybercrime and identity theft were much less mature. Thus, there was less awareness of the prospect of online attacks.

During this period, the DOD pursued a congressionally mandated online voting project for military and overseas voters. Expecting that the Pentagon would offer a secure and trustworthy electronic absentee voting option for military voters, states passed laws allowing ballots to be returned electronically so they could eventually opt into the Pentagon's system once it was available. As previously discussed, the DOD online voting project was scrapped and indefinitely postponed in 2004 because of security concerns, yet states continued to change their laws.

In reviewing states' actions, it is also essential to examine the role the FVAP played as states adopted policies to permit voting by email. The FVAP is a tiny agency housed within the DOD and tasked with administering federal laws regarding military and overseas voters. Operating under the undersecretary for personnel and readiness, the FVAP has admitted it urged states to explore email voting from 1990 to 2009, even as computer security experts warned of the grave security risks inherent in transmitting ballots by email.[24] The FVAP's former director stated he continued to promote email and fax return of voted ballots to state officials until mid-2010, when he realized it was far less secure than other voting methods.[25]

The FVAP's influence could be seen years after it claimed it had reversed course, through the DOD State Liaison Office. The State Liaison Office works with state policymakers to promote reforms on issues that impact military personnel and their families, including voting.[26] By DOD directive, the office must consult with the FVAP for "legislative and other policy matters involving voting assistance and elections."[27] As recently as 2015, a representative from the State Liaison Office testified before a Washington State legislative committee in support of a bill to expand online voting to all voters, stating that the Pentagon supported the policy.[28] When contacted by a reporter, Pentagon spokesman Lt. Cmdr. Nathan Christensen said the Defense Department "does not advocate for the electronic transmission of any voted ballot, whether it be by fax, email or via the Internet,"[29] suggesting that the State Liaison Office continued the FVAP's promotion of online voting in contravention of DOD policy.

RISKS OF ONLINE VOTING

Online voting introduces multiple risks not just to the security of the ballots cast online, but also to the integrity of the overall election system. Adopting features such as blockchain or encryption does not resolve many of the fundamental security risks inherent to online voting.

Ballot Integrity

Risks to Emailed Ballots in Transit

Ballots sent online can be manipulated undetectably at different points in the journey from the voter's computer to the county election office. The most common forms of online ballot return (email and fax) are susceptible to manipulation at multiple points during transmission.[30] A ballot transmitted by email or fax moves through networks of routers and forwarding agents until it arrives at its final destination.[31] It is impossible to guarantee the security of this entire infrastructure, given that it extends worldwide. At any link in the chain, someone who controls a router or forwarding agent could detect which messages are being directed toward the email server of an American elections office. It would not be difficult to create an automated process for discarding ballots with undesired votes and replacing them with forgeries.[32] In this process, the sender's original message and any other attachments, such as a voter's declaration and signature, could be maintained, producing a forged ballot that would appear perfectly authentic to any unsuspecting election official.[33] This process would not require extensive processing time and could be accomplished with a delay as brief as a fraction of a second.[34] At the August 2018 DEF CON hackers conference, researchers showed the ease with which an in-flight emailed ballot can be manipulated undetectably.[35]

Malware on the Voter's Computer or Device

Ballots also can be compromised by malware before they even leave voters' personal computers. Computers and devices are under constant attack from a host of viruses, Trojan horses, spyware and malware.[36] Any ballot cast online is vulnerable to malware that could be used to spy on the voter's selections and/or manipulate vote choices. Even if the ballot is sent through an encrypted web portal or blockchain transmission system, it is still vulnerable because malware on a voter's computer can modify a marked ballot *before* it enters the encrypted system or blockchain. It is estimated that as many as one in three computers is already infected with malware that could be leveraged to tamper with ballots.[37] Attackers wishing to manipulate ballots would not have to infect computers with a new malware. They could simply "rent," on the black market, computers already infected with malware and customize the malware to modify ballots. Just as Microsoft, Apple or Symantec can send updates to their software products remotely, a malicious attacker can remotely update malware on infected computers, customizing it to recognize and replace ballots or modify votes.[38] This manipulation would affect only the ballot image being returned to the elections office. On the computer screen, the voter would see the correct ballot image with the voter's choices, making such an attack undetectable. Researchers warn the potential to exploit a large number of already infected computers means such client-side attacks can have large-scale impact.[39]

Voter Authentication

Reliably authenticating voters casting ballots over the internet remains an unsolved online voting problem.[40] Online voting introduces the possibility that attackers could steal voters' authentication credentials, such as pins or passwords. Such attacks could be automated, allowing a computerized program to cast a large number of fraudulent ballots.[41] Other options, such as biometrics or facial recognition software, remain inadequate. Election officials do not have access to the biometric databases needed to authenticate voters. Facial recognition software has high error rates and has been shown to fail disproportionally with faces of citizens who are minorities.[42]

Server Penetration Attacks

An online voting system could also be attacked through directly penetrating the county election server or network components. An attacker could infect elements of the county's network with malware designed to replace

legitimate ballot images with a ballot image reflecting the attacker's choices. Even if election workers discovered malware on election systems before Election Day, election officials would have no way to identify the affected ballots from legitimate ones.[43] This sort of attack was successfully demonstrated on an encrypted online voting system in 2010, when Washington, D.C., attempted a pilot program for an online ballot return system. D.C.'s Board of Elections (BOE) created an evaluation version, encouraging members of the public to test the system's security and ease of use. The BOE was forced to cancel the program's rollout after a team of security researchers at the University of Michigan was able to penetrate the system, gain access to all ballots and replace them with doctored ones.[44]

Election Results Cannot Be Audited with Current Online Systems

Regardless of the method of meddling, one damning final vulnerability stands: there is no effective means to detect interference in the process or audit for it after the fact. To county election officials receiving ballots transmitted online, an authentic ballot looks identical to a fake. Because the ballots are transmitted electronically, there is no way to know that the manipulated message that arrives is identical to the one sent by a voter. There is no torn envelope or scratched-out marking. Even if officials became aware of an attack, it would be impossible to determine which specific ballots were targeted and manipulated. Even reassuring the public against *rumors* of ballot-tampering would prove impossible. There is no way to confidently certify the integrity of the voting system, which would inevitably affect voters' views of its legitimacy.

Election Offices Face Systemic Risk by Receiving Emailed and Faxed Ballots

Emailed Ballots Provide an Opportunity to Infect Entire Systems with Malware

By far the most common form of online voting in the U.S. is email voting. Receiving voted ballots by email introduces severe threats to the integrity of a state or county's election infrastructure that extend beyond the integrity of an individual's ballot. Transmitting emailed ballots to a county or state elections office could become the tip of the spear in an attack on the larger county election infrastructure, affecting everything from voter rolls to the operating systems of electronic voting machines.

Ballots and other documentation used to verify the voter's eligibility are typically attached to the email as a PDF or JPEG file. It is well-known that both PDF[45] and JPEG[46] files can be used to deliver malware or other cyberattacks, which is why security best practices regularly warn against opening email attachments from unknown sources. But for jurisdictions that receive ballots by email, election workers must routinely click on attached documents from unknown sources to process emailed ballots, exposing the computer receiving the ballots — and any other devices on the same network — to a host of cyberattacks. The infected false ballot would enter the server like any other ballot, but once opened, it would download malware that could give attackers backdoor access to the elections office's network.[47]

If the county or state device receiving ballots is not properly isolated, malware transmitted by PDF attachment could potentially serve as a vector to infect electronic voting machines or ballot scanners used statewide, even when those machines are not themselves connected to the internet. Before voting machines or scanners can be used, "ballot definition files" must be created on another computer to tell the machines which candidates should appear on the ballot or how to count marks on a paper ballot.[48] Those files must then be transferred to the voting machines or scanners through a cartridge or memory card. It is alarmingly possible to infect voting machines through these cards. In 2007, a Princeton University team successfully created self-replicating code that spread from machine to machine via administrator cards, altering vote counts.[49] In a mock election between George Washington and Benedict Arnold conducted on an infected machine, every voter chose Washington and confirmed the selection, but the vote tallies nevertheless reported a victory for Arnold.[50] Many other methods of affecting elections through malware in email attachments are equally feasible.

This is, right now, the worst-case scenario for an email-based voting system:

An election official receives a new ballot submission, with the ballot attached as a PDF file, on a computer terminal with direct or indirect networking to other computers in the jurisdiction. The email address appears to be a .mil

address, indicating a military voter. The message and attachment are opened, and the ballot is received with the others. Unbeknownst to the election official, the PDF has installed a dangerous program designed to spread to other computers within the network. Days later, when another official prepares ballot definition files for the state's voting machines or scanners, the hidden program copies malicious code onto the memory card. The malware is installed on every voting machine or scanner in the state, surreptitiously changing vote totals. Even after a voter sees his or her choice confirmed on the voting machine screen or marked on the paper, the final results reflect a totally different choice.

*Unless the state has paper ballots that the voter has marked themselves for **all** votes cast, and the paper ballots are used to manually audit each election contest to a high degree of statistical confidence, this change in the final results could not be detected and thwarted. Without fanfare, one email has swung an election.*

To protect other elements of the county or state election system from potential cyberattacks that could be delivered by email attachments posing as ballots, **elections offices must employ strict protocols to isolate and quarantine the computer used to receive emailed ballots.** However, there is no evidence to suggest this is commonplace.

A review of publications on security best practices from the EAC, DHS and the National Association of Election Officials found no published guidance regarding the security of emailed ballots or recommendations for securing the computer terminal receiving emailed ballots. (We provide some basic recommendations at the end of this report and urge election administrators to seek guidance for securing these devices from their state chief information officers, the National Guard, DHS, the Elections Infrastructure Information Sharing and Analysis Center, Center for Internet Security and other resources.)

Denial-of-Service Attacks

Receipt of email ballots could also expose the elections office to denial-of-service attacks, in which a server is flooded with so many requests that it is too overloaded to handle traffic from legitimate users. Overwhelmed, the server is effectively crashed. A botnet — a group of infected computers that are controlled by one source — could do this from remote overseas locations beyond the reach of U.S. law enforcement, preventing voters from casting ballots for hours or days.[51] Denial of service can also occur from nonmalignant circumstances. Days before the 2012 election, New Jersey permitted citizens displaced by Superstorm Sandy to vote by email[52] with little advance preparation. There was no malicious attack; however, the volume of emails crashed servers, clogged email inboxes and prevented other voters from voting,[53] essentially generating a denial of service.

Disruption Attacks

Warnings from the U.S. intelligence community have emphasized that our adversaries are also seeking simply to disrupt our elections in order to sow chaos and distrust in the system. Internet voting is exceptionally vulnerable to attacks meant to undermine confidence in the election. An attacker could breach a system just to delete all the votes that had been cast online and effectively discredit the election. Another increasingly common attack, ransomware, could be used to hold the ballots cast online to extort a payment, while corroding confidence in the election. Most disruption attacks will not be mitigated with blockchain or encryption and could effectively decimate the public's trust in an election outcome.

Any combination of the vulnerabilities of online voting could be exploited — or all of them. There could be multiple, simultaneous attacks. The attackers need not even be aware of each other. With so many avenues of attack and insufficient defenses available, the only responsible course today is not to rely on online voting at all.

IS NEW TECHNOLOGY THE ANSWER?

Blockchain Voting

Resistant to the idea of abandoning internet-based voting, some activists and election officials have explored emerging security technologies as a way to overcome current vulnerabilities. Start-ups have introduced online voting systems based on blockchain technology, improperly claiming it solves the security problems of online voting. A blockchain is a public ledger that is shared electronically with a number of users, with every transaction between them recorded as an unchangeable "block."[54] No one person can alter the code. When each new block is entered, the entire chain is updated by consensus and is identical for all users.[55]

Blockchain is no magic bullet. **It fails to address many of the fundamental and universal security challenges inherent to online voting, such as voter authentication, client-side malware attacks, denial-of-service attacks, server penetrations and disruption attacks**. Furthermore, blockchain systems are vulnerable to "collusion" attacks. In such attacks, if the participants in the blockchain colluded to control the ballot set, they could agree to rig the election by substituting a set of fraudulent ballots stored on the blockchain. Moreover, the participants do not have to wittingly agree to tamper with the ballots. If the individual participants' servers are hacked by nation-states or criminal organizations, they could be infected with malware created to coordinate with the other infected participants' servers to manipulate the ballot set.[56]

End-to-End Verifiable Systems

Cryptographers have identified "end-to-end (E2E) verifiability" as a method to provide auditable online voting.[57] End-to-end verifiability utilizes cryptographic methods to allow the voter to verify that the ballot was recorded and counted accurately and would also allow third parties to check the election results to confirm they are correct. End-to-end verifiability addresses the possibility of undetectable hacking. The results can be reliably audited for correctness, not just by election officials or vendors but by individuals or independent organizations, such as media outlets, political parties or nongovernmental organizations.

End-to-end verifiable online voting systems however, do not address the unresolved problems of voter authentication or denial-of-service attacks. Like all online voting systems, E2E systems are vulnerable to malware, which can be used to spy on the voter's selections and compromise ballot secrecy.[58] The system would not prevent or be able to detect fraudulent votes from also being inserted into the vote tally.[59] Additionally, it is difficult to provide a way to allow the voter to verify how s/he voted without also making it possible for the voter to prove to a third party how her vote was cast, which introduces the risk of vote selling or coercion. E2E verification could not prevent a disruption attack that deletes all ballots. Indeed, voters seeking to confirm their votes could find their ballots were not cast, and the attack could very effectively sow distrust among voters.

Finally, E2E voting systems are complex and notoriously difficult to use; a significant drawback is that voters may inadvertently disenfranchise themselves by not following the system directions correctly.[60]

E2E online voting warrants further research. It offers a way to audit an election and detect possible vote tampering, but it still includes many significant unresolved security issues. Leading researchers in E2E have explicitly warned that E2E online voting should not yet be deployed in public elections until the security issues have been resolved.[61] These researchers estimate those solutions could be several decades away. Election officials and the public should also be aware that some commercially available online voting systems are being marketed as E2E; however, these systems do not provide actual end-to-end verifiability.

CONCLUSION

Paper Ballots: Today, the Answer Is Low Tech

Until there is a major technological breakthrough in or fundamental change to the nature of the internet, the best method for secure elections is a tried-and-true one: paper ballots. Paper ballots aren't tamper-proof, but they are not vulnerable to the same sort of wholesale fraud or manipulation associated with email voting. No malware can change the mark made on a piece of paper. Moreover, tampering with a mailed paper ballot requires physical access to the ballot itself, whereas emailed ballots can be manipulated by a hostile foreign government, crime syndicate, terrorist organization, hacktivist group or partisan criminal from anywhere in the world. Further, tampering with mailed paper ballots is a one-at-a-time corruption. Even if one ballot is stolen in the mail, it is impossible to create an automated system that intercepts all of them. In contrast, as the old adage goes, to really foul things up, you need a computer. Infecting the computers that handle the ballots and tabulation permits large-scale corruption.

Military voters undoubtedly face greater obstacles in casting their ballots. They deserve any help the government can give them to participate in democracy equally with all other citizens. However, in this threat environment, online voting endangers the very democracy the U.S. military is charged with protecting. Considering current technology and current threats, postal return of a voted ballot is the most responsible option. In this threat environment, states that permit online return of voted ballots should eliminate the practice. Until they do, the integrity of Americans' votes is at stake, and in many cases, the integrity of the election system is at risk.

RECOMMENDATIONS

In most states, it will be impossible to amend statutes or policies permitting online ballot return in the near term. Nevertheless, voters should be made aware of the acute security risks as well as systemic risks, and encouraged to vote by paper ballots whenever possible. States that permit online ballot return should consider amending their laws to prohibit online ballot return as soon as possible.

While online ballot return is inherently very risky, election officials are urged to take certain precautions to reduce exposure to cyberattacks.

Recommendations for Election Officials Processing Emailed or Faxed Ballots

Election officials are encouraged to:

- Ensure that military voters know they can use free, trackable, expedited postal mail return. Postal labels for free and expedited postal mail return can be obtained for military personnel at FVAP.gov. The Military Postal Service Agency reports that the average transit time for expedited postal mail return is four days.
- Map the network and ensure that the computer used to receive emailed or digitally faxed ballots is *not* connected to or on the same network as the voting machine network, election management system (EMS) or voter registration system through wired or wireless means and that the wireless capability is disabled.[62]
- Scan all incoming email and digital faxes for malware; the mail program should be configured to verify that attachments are of the expected type and fall into the typical size range.[63]
  - Important: Scanning may find attachments for executable malware programs but may be unable to detect malware *inside* a PDF or JPEG file. Malware inside such files is much more complex.
- Ensure that ballots returned by email are printed for counting, not electronically transmitted to the EMS for counting.
- Ensure that the printer used to print email ballots is used only for this purpose, and no media that is connected to that printer (USB, networks, computers) should be plugged into anything else.

- Hand-count emailed ballots rather than copying the votes onto optical scan ballots.
- If the ballot was marked on an electronic ballot marking device that produced a barcode of vote choices, we recommend election officials manually remake the ballots directly from the voters' choices marked on the ballot, rather than electronically remaking the ballot from a barcode. (If remaking the ballot, the original should be retained, used to audit remade ballots for accuracy and used in case of recounts.)
- If the 2-D barcode is used to remake the ballot for scanning, election officials are urged to check the remade ballot's printed choices carefully against the original voter-marked choices to ensure all the voter's selections were captured correctly.

Recommendations for States Offering Web-Portals for Ballot Return

- Election officials are urged to ensure that military voters know they can use free, trackable, expedited postal mail return. Postal labels for free and expedited postal mail return can be obtained for military personnel at FVAP.gov.
  - The Military Postal Service Agency reports that the average transit time for expedited postal mail return is four days.
- Map the network and ensure that the server hosting the web-portal is *not* connected to or on the same network as the voting machine network or election management system.
- Do not connect the web-based ballot return system directly to the voter registration database or ballot file database. Create a static copy of the voter registration database and ballot file database to interact with the web-based ballot return system.

Recommendations for Voters

- All voters are urged to protect the integrity and privacy of their votes by hand-marking paper ballots if possible and returning them by postal mail rather attempting to return them via online portal or by email or fax.
- Voters using electronic ballot delivery systems are encouraged to print the blank ballots and mark them by hand. If voters choose to use online ballot marking features, they should be encouraged to print the ballot and *carefully review the entire ballot* to be sure it has been marked correctly.
- Military personnel in Army, Fleet or Diplomatic Post Office (APO/FPO/DPO) locations can return absentee ballots via Priority Mail Express using the Express Mail Label 11-DOD. "Waiver of Signature" and "Guaranteed by End of Day" endorsements are printed on the label, so ballots sent with it are delivered on the day they arrive at the destination post office. According to FVAP:
  - The Military Postal Service Agency distributes the labels overseas and pays for the postage.
  - The Priority Mail Express ballot label is only for absentee ballots mailed from military post offices overseas.
  - The label may be used on any size ballot envelope. It always goes in the upper right corner.[64]
    - Voters can keep part of the tracking label and use the tracking number to track their ballots.
  - At the International Sorting Center (ISC), absentee ballots receive special handling including accelerated sortation, special tray identification and priority transportation.
  - Overseas U.S. military and civilian citizens will be returning their absentee ballots either via the military or diplomatic postal service (APO/FPO/DPO) or via the international mail system.
  - The ballots will arrive by international transportation at one of the U.S. Postal Service's gateway offices for customs clearance and initial processing at select designated offices (International Sorting Center/Processing and Distribution Center)
  - At these facilities, the mail is processed by postal automation equipment in an initial domestic primary sort for distribution throughout the United States.

NOTES

1 "Press Briefing by Press Secretary Sarah Sanders and National Security Officials" (August 2, 2018), https://www.whitehouse.gov/briefings-statements/press-briefing-press-secretary-sarah-sanders-national-security-officials-08022018/.

2 *See* Kim Zetter, "The Myth of the Hacker-Proof Voting Machine, *The New York Times Magazine* (February 21, 2018).

3 Caitriona Fitzgerald, Susannah Goodman, and Pamela Smith, "The Secret Ballot at Risk: Recommendations for Protecting Democracy," *Common Cause/Electronic Privacy Information Center/Verified Voting* (2016), http://www.secretballotatrisk.org/Secret-Ballot-At-Risk.pdf.

4 Alaska Stat. § 15.20.910 (2016), available at http://law. justia.com/codes/alaska/2016/title-15/chapter-15.20/ article-05/section-15.20.910/.

5 *See "By-Fax Ballot Delivery"* http://www.elections.alaska.gov/Core/votingbyfax.php

6 Hawaii House Bill 1654 (2016), available at http:// www.capitol.hawaii.gov/session2016/bills/HB1654_ SD2_.htm; National Conference of State Legislatures, "Electronic Transmission of Ballots."

7 Utah Code § 20A-16-404, available at https://le.utah. gov/xcode/Title20A/Chapter16/20A-16-S404. html?v=-C20A-16-S404_1800010118000101; National Conference of State Legislatures, "Electronic Transmission of Ballots"

8 Jim Garamone, "Pentagon Decides Against Internet Voting This Year," *Armed Forces Press Services* (February 6, 2004), http://archive.defense.gov/news/newsarticle.aspx?id=27362.

9 *See* "NIST Activities on UOCAVA Voting," *NIST Information Technology Laboratory* (August 25, 2016), https://www.nist.gov/itl/voting/nist-activities-uocava-voting.

10 "Voting Demonstration Project Repealed," *U.S. Vote Foundation*, https://www.usvotefoundation.org/blog/domestic-voting/voting-demonstration-project-repealed.

11 "Computer Technologists' Statement on Internet Voting," *Verified Voting* (2008), http://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf.

12 Greg Gordon, "As States Warm to Online Voting, Experts Warn of Trouble Ahead," *McClatchy DC* (April 16, 2015), http://www.mcclatchydc.com/news/politics-government/election/article24783181.html.

13 Sari Horwitz, "More Than 30 States Offer Online Voting, but Experts Warn It Isn't Secure," *The Washington Post* (May 17, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/morethan-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/.

14 Andrew Appel, "Securing the Vote — National Academies Report," *Freedom to Tinker (2018),* https://freedom-to-tinker.com/2018/09/11/securing-the-vote-national-academies-report/.

15 "France Drops Electronic Voting for Citizens Living Abroad Over Cyber Security Fears," *Reuters* (March 6, 2017), https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233.

16 Mary Stimton, "Threat of Cyber Attack Prompts Change in Alaska Primary," *KTVA* (August 5, 2018), http://www.ktva.com/story/38816657/threat-of-cyber-attack-prompts-change-in-alaska-primary.

17 *See "By-Fax Ballot Delivery"* http://www.elections.alaska.gov/Core/votingbyfax.php

18 Tim Johnson, Greg Gordon, and Christine Condon, "Can Hackers Tamper With Your Vote? Researchers Show It's Possible in Nearly 30 States," *McClatchy News* (August 14, 2018), https://www.mcclatchydc.com/news/nation-world/national/national-security/article216610445.html.

19 *See question B27 https://www.eac.gov/assets/1/28/2016_EAVS_Instrument.pdf*

20 "Election Administration and Voting Survey Report," *U.S. Election Assistance Commission* (2016), https://www.eac.gov/assets/1/6/2016_EAVS_Comprehensive_Report.pdf.

21 "FVAP Reports and Surveys," https://www.fvap.gov/uploads/FVAP/Surveys/PEV81601_State_Jurisdiction_Final_V2.xlsx.

22 Washington state counties did not answer the question in its EAVS response, but the secretary of state published the number of ballots returned online in 2016. This value was included in the total.

23 Four states (Arkansas, Michigan, New Hampshire and Vermont) reported ballots returned electronically, though they prohibit the practice. Representatives from the Arkansas, Michigan, New Hampshire and Vermont state elections offices advised that the data was reported in error and we did not include it. Emails are on file with National Election Defense Coalition.

24 Greg Gordon, "Pentagon Unit Pushed Email Voting for Troops Despite Security Concerns," *McClatchy News* (November 4, 2012).

25 Ibid.

26 "Department of Defense State Liaison Office," *USA4 Military Families,* http://www.ncsl.org/documents/environ/DSLO-mission2013.pdf.

27 "Department of Defense Instruction," Number 1000.04, *Department of Defense* (September 13, 2012), http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/100004p.pdf?ver=2017-12-01-105434-817.

28 Gordon, *supra* note 9.

29 Ibid.

30 The security considerations for ballots returned by fax are nearly identical to email voting, sharing a similar security profile. *See* David

Jefferson, "What About Email and Fax?" *VerifiedVoting.org,* https://www.verifiedvoting.org/resources/internet-voting/email-fax/.

31 Andrew Regensheid and Geoff Beier, "Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters," *U.S. Department of Commerce, National Institute of Standards and Technology (September 2011),* http://nist.gov/itl/vote/upload/nistir7711-Sept2011.pdf.

32 Andrew Regenscheid and Nelson Hastings, "A Threat Analysis of UOCAVA Voting Systems," NIST IR 7551, *U.S. Department of Commerce, National Institute of Standards and Technology* (December 2008), http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf.

33 Johnson et al., *supra* note 14

34 Jefferson, *supra* note 26

35 Johnson et al., *supra* note 14

36 Danny Palmer, "What is malware? Everything you need to know about viruses, trojans and malicious software," *ZDnet* (May 30, 2018)

37 John P. Mello, "Report: Malware Poisons One Third of World's Computers," *TechWorldNews* (July 9, 2014).

38 Nelson Hastings, Rene Peralta, Stephan Popovenuic, and Andrew Regenscheid, "Security Considerations for Remote Electronic UOCAVA Voting," NIST IR 7770, *U.S. Department of Commerce, National Institute of Standards and Technology* (February 2011).

39 Ibid.

40 See *supra* note 6

41 Jefferson, *supra* note 26

42 Steve Lohr, "Facial Recognition Is Accurate, If You're a White Guy," *The New York Times* (February 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

43 See Hastings et al., *supra* note 34

44 J. Alex Halderman, "Hacking the D.C. Internet Voting Pilot," *Freedom to Tinker* (October 5, 2010), https://freedom-to-tinker.com/2010/10/05/hacking-dc-internet-voting-pilot/.

45 Karthik Selvaraj and Nino Fred Gutierrez, "The Rise of PDF Malware," *Symantec Security Response* (2010), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_rise_of_pdf_malware.pdf.

46 Swati Khandelwal, "How to Hack a Computer Using Just an Image," *The Hacker News* (June 1, 2015).

47 Joel Yonts, "PDF Malware Overview," *Sans Institute* (July 19, 2010), https://www.sans.org/security-resources/malwarefaq/pdf-overview.

48 Andrew Appel, "Which voting machines can be hacked through the Internet?" *Freedom-to-Tinker, Sept. 20, 2016,* https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/

49 Ariel J. Feldman, J. Alex Halderman, Ed Felten, "Security Analysis of the Diebold AccuvoteOTS Voting Machine," *USENIX* https://www.usenix.org/legacy/event/evt07/tech/full_papers/feldman/feldman_html/index.html

50 Ibid.

51 Regenscheid, et al., *supra* note 28

52 "Directive Regarding Email Voting and Mail-In Ballots for Displaced Voters," *The State of New Jersey* (2012), https://nj.gov/state/elections/2012-results/directive-email-voting.pdf.

53 Ted Sherman, "Emergency Voting Measures During Hurricane Sandy Violated N.J. Law, Inviting Fraud, Study Finds," *NJ Advance Media* (October 24, 2014).

54 Lucas Mearian, "What Is Blockchain? The Most Disruptive Tech in Decades," *ComputerWorld* (January 18, 2018), https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html.

55 Ibid.

56 David Jefferson, "The Myth of Secure Blockchain Voting," *Verified Voting.* https://www.verifiedvoting.org/jefferson_themythof_secure_blockchainvoting/

57 "The Future of Voting, End-to-end Verifiable Internet Voting," *U.S. Vote Foundation*, https://www.usvotefoundation.org/e2e-viv/summary.

58 Ibid.

59 Ibid.

60 Claudia Z. Acemyan, Philip Kortum, Michael D. Byrne, and Dan S. Wallach, "Useability of Voter-Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Pret-a-Voter, and Scantegrity II, *Rice University,* https://www.usenix.org/node/185518

61 See *supra* note 53

62 See *supra* note 27

63 See *supra* note 27

64 "Military — APO/FPO/DPO Returning Absentee Ballots," *United State Postal Service*, https://about.usps.com/postal-bulletin/2016/pb22443/html/cover_018.htm

APPENDIX

Combined Totals for Ballots Received by Email and Ballots Received by Fax

Alabama	1016
Alaska	5057
Arizona	8830
California	17038
Colorado	13172
District of Columbia	2913
Hawaii	226
Indiana	6681
Louisiana	576
Maine	5826
Montana	3047
Nebraska	315
Nevada	4633
North Dakota	1156
Texas	10,686
Washington*	17418
West Virginia	488
Total	99078

Source: U.S. Election Administration and Voting Survey (EAVS) https://www.fvap.gov/uploads/FVAP/Surveys/PEV81601_State_Jurisdiction_Final_V2.xlsx (PEV8 Jurisdictions Not Imputed -Column AU and Column AT)

* Washington counties did not respond to the EAVS, but the number of ballots returned electronically has been reported by the Washington Secretary of State here: Election Reconciliation Reports.

In states that allow electronic return of marked ballots, we summed the numbers reported by each county. Officials from Arkansas, Michigan, New Hampshire and Vermont, which do not allow electronic return of marked ballots, advised the data for their states had been put into the survey incorrectly, and those values were excluded.

ABOUT THE ORGANIZATIONS

ACM US Technology Policy Committee

The Association for Computing Machinery is the longest-established society of practicing computing professionals of all kinds in the world. With more than 50,000 members in the United States and over 100,000 globally it also is the world's largest. ACM is non-profit, non-political, and non-lobbying. The ACM US Technology Policy Committee is charged by ACM with providing policy and law makers throughout government with expert, neutral, timely, and substantive input on computing technology and the issues to which it gives rise.

Common Cause Education Fund

The Common Cause Education Fund is the research and public education affiliate of Common Cause, founded by John Gardner in 1970, and one of the country's most effective organizations working to reduce the influence of special-interest money in politics, breaking down barriers to participation, ensuring transparency in government, and protecting the free flow of information. We work to create open, honest, and accountable government that serves the public interest; promotes equal rights, opportunity, and representation for all; and empowers all people to make their voices heard in the political process.

National Election Defense Coalition

The National Election Defense Coalition (NEDC) is a national non-partisan organization and network of recognized experts in cybersecurity and elections administration, bipartisan policymakers, and concerned citizens dedicated to promoting policies and practices to secure U.S. election systems. NEDC works to provide a bridge between cyber security experts, research and best practices that pertain to election systems, and the election administrators and policy makers responsible for selecting and managing election technology.

R Street Institute

R Street Institute is a nonprofit, nonpartisan, public policy research organization. Our mission is to engage in policy research and outreach to promote free markets and limited, effective government.

ABOUT THE AUTHORS

Jeremy Epstein

Jeremy Epstein is vice chair of the ACM US Technology Policy Committee (USTPC), and former chair of the voting subcommittee. He is as deputy division director for the Division of Computer and Network Systems at the National Science Foundation, where he oversees research on a wide range of scientific topics including cybersecurity. He's been a cybersecurity researcher for almost 30 years, focusing on voting & elections security for over a decade. Prior to joining NSF, he served at the Defense Advanced Research Projects Agency (DARPA) and SRI International, where he worked on cybersecurity topics.

Susannah Goodman

Susannah Goodman is the Director of the Election Security program at Common Cause. She works with national staff and Common Cause state offices to press for reforms that repair and strengthen our voting systems at both the state and federal level. She has testified before Congressional committees, appeared on national news television programs, and co- authored a number of reports on elections and voting. including Is America Ready to Vote? State Preparations for Voting Machine Problems in 2008, Voting in 2010: Ten Swing States, Counting Votes 2012: A State by State Guide to Election Preparedness and The Secret Ballot at Risk.

Susan Greenhalgh

Advocating for verifiable, auditable elections since 2004 Susan Greenhalgh is a recognized expert in election security policy. Over ten years ago Susan began studying the use of Internet voting in the U.S., examining the factors driving the expansion of online voting and closely reviewing the research into the security of online voting conducted in the U.S. and internationally. She has been invited to speak at conferences held by the MITRE Corporation, the National Conference of State Legislatures, the International Association of Government Officials, the Mid-West Election Officials Conference, the Election Verification Network and at the E-Vote-ID conference in Bregenz, Austria, among others.

Paul Rosenzweig

Paul Rosenzweig is a senior fellow of with the R Street Institute, where he works on legal and policy issues relating to cybersecurity, national security, and tech policy, including the intersection of privacy and security. In addition to his work at R Street, which he joined in November 2017, Paul continues to manage a small cybersecurity consulting company called Red Branch Consulting and to teach at the George Washington University School of Law. From 2005 to 2009, he was deputy assistant secretary for policy at the U.S. Department of Homeland Security.