Photo by Getty Images

 This article is provided for informational purposes only with permission of the Institute of Industrial and Systems Engineers from the August 2024 issue of ISE magazine, Copyright©2024. All rights reserved.

Securing democracy: Threat mitigations for the mail voting process

Continuous improvement, innovation can ensure ballots are cast, counted accurately

By Vanessa Gregorio, Natalie M. Scala and Josh Dehlinger

As a representative democracy, the United States depends on free and fair elections to ensure the will of the American people is heard in local, state and national governments. As a result, the security of U.S. elections is of vital national interest and has gained even more importance in light of the ever-expanding risk analysis landscape.

Modern developments in U.S. elections were implemented as a result of the controversy surrounding ballot counting procedures and dated technology during the 2001 presidential election and subsequent Bush v. Gore litigation. Following the election and Supreme Court proceedings, the Help America Vote Act (HAVA) was passed by Congress in 2002 to reform voting systems, creating federal standards for voting machines and ballot accessibility, as well as an agency, the Election Assistance Commission (EAC), to assist in implementing these standards.

The more recent threat of foreign interference introduced a greater consideration for cybersecurity within elections, this being discussed in detail within former special counsel Robert Mueller's probe and the Senate Intelligence Committee's bipartisan investigations on Russia's malicious involvement in the 2016 presidential election. In 2017, the U.S. Department of Homeland Security officially recognized election security as critical infrastructure, further signaling the need to improve protections for U.S. election processes.

More recently, concerns about the COVID-19 pandemic spurred states to expand mail voting during the 2020 primary and general elections (Scala et al., 2022). While changes were swiftly made, the 2020 general election was reported to be one of the most secure elections in U.S. history, having one of the highest participation rates within the last century. However, false claims that mail voting was fraudulent circulated during this period of time, despite there being no evidence to support this. Academic studies affirmed the security of mail voting, finding that it disincentivizes adversarial interference and increases voter access. Furthermore, mail voting has been used in some capacity in U.S. elections since the Civil War; it is not new. Even with these facts, disinformation/misinformation about mail voting continues to be spread.

Although it is established that mail voting is not synonymous with wide-scale fraud, it does not mean safeguards should not be in place. Elections staff – which includes public servant boards of elections employees and the nearly 1 million poll workers needed nationwide during a presidential election – must be ready to identify and mitigate possible adverse scenarios for both the in-person and mail voting processes during election season.

Scala, et al., in "Evaluating MailBased Security for Electoral Processes Using Attack Trees" (2022), discussed that the majority of mail voting threats are not related to voter fraud or external adversaries but instead come from insiders who genuinely try to participate in elections. It is possible that some insiders may have nefarious intent, but the vast majority of them are trustworthy and altruistic; however, the latter group may make mistakes during the voting process. This is because, compared to other methods of voting such as in-person, mail voting is unique in that the process does not involve voters and poll workers interacting in person and lasts over a period of time rather than a single day. If a voter happens to be confused about any of the steps involved in the mail voting process, they cannot ask poll workers for immediate, face-to-face assistance.

Additionally, sending a completed mail ballot package to a voter's local board of elections takes time. If there are errors in the mail ballot package, such as forgetting to

More voting security resources

- **U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency**: *cisa.gov/topics/election-security/protect2024*
- **FBI voter security**: *fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/election-crimes-and-security*
- **Ballotpedia**: *ballotpedia.org*

sign the ballot or applying correct labels to the envelope, fixing these issues during the ballot curing process – which varies by state – will also take time. When the distinct characteristics of mail voting are not accounted for when participating in the process, this may lead to an inability for voters to successfully submit their completed mail ballot package before the deadline.

Risk analysis in mail voting is important

For any organization, effective planning for and implementation of threat mitigations must adapt to the continuous evolution of technology and societal institutions. Using a combination of approaches, such as reactive (e.g., responding to problems after they happen), proactive (e.g., preventing problems before they happen) and predictive (e.g., tackling problems based on historical data and previous experiences) – not simply one or the other – provides a variety of options to prepare for adverse scenarios.

Choosing not to do anything to counteract risks could lead to disrupted operations, a damaged reputation or harm against the organization's stakeholders. Organizations therefore should take great care in conducting risk analysis research in order to eliminate these potential costs.

In the case of mail voting, ensuring the process is kept secure has more implications than ensuring ballots are counted correctly. Having effective and trustworthy elections is essential for the U.S. to maintain democratic legitimacy. Voting processes must be accessible to all eligible voters, especially those who belong to groups that have been historically suppressed within elections. That said, there is currently a lack of research on how to calculate risk reduction for mail voting threats, not because mail voting is novel but since it had been underutilized on a wider level until the COVID-19 pandemic.

Poll worker training must be improved for all types of voting methods so that those who administer elections know how to deal with the possibility of threats against each of these processes. This is especially true for mail voting, which does not have detailed training or manuals in many districts across the U.S. Therefore, it is of utmost importance to begin formal research into this relatively new subject.

Properly assessing how to mitigate risks within the mail voting process first requires identifying threats within the mail voting process. Various sources can be used to build a list of threats, such as news articles on recent events and academic literature. Aside from publications, eliciting information from elections staff and experts familiar with the mail voting process can also be valuable.

Researchers should try to consider every aspect of what could logically go wrong. Examples of already existing research include the EAC's Election Operations Assessment (2009), which constructed attack trees that outlined threats for several voting methods, including mail voting; and Scala, et al., (2022), which added new threats to the Election Operation Assessment's mail voting attack tree, accounting for changes in the risk environment since the original assessment was made.

After identifying threats, the next step is to make a list of mitigations to counteract them. Threats and mitigations should be mapped to each other. A threat may have multiple mitigations that can prevent or reduce its consequences, and a mitigation could prevent or reduce the consequences of multiple threats. Ensuring there is a direct relation between threats and mitigations is important; if a list of mitigations is made without accounting for what adverse scenarios they are subverting, this might make it so that some or none of the mitigations are effective.

Making a complete analysis requires the defense in-depth strategy, or using multiple approaches. For instance, a Delphi panel may be conducted. This is an approach where researchers gather a group of subject matter experts to anonymously submit their thoughts and opinions on effective mitigations for mail voting threats. Researchers compile all inputs and present them to participants for feedback and further conversation. This approach lessens the likelihood of power dynamics and biases arising within the group and having participants' responses being diluted, which could happen during real-time discussions.

Although it is established that mail voting is not synonymous with wide-scale fraud, it does not mean safeguards should not be in place. Elections staff – which includes public servant boards of elections employees and the nearly 1 million poll workers needed nationwide during a presidential election – must be ready to identify and mitigate possible adverse scenarios for both the in-person and mail voting processes during election season.

Researchers must also take care in the design and conduct of the panel, as the parameters for achieving consensus may be subjective and could take an extended period of time. In previous work, we used Delphi panels to review and discuss mitigations against the spread of election disinformation/misinformation.

Researchers may also consider allocating resources based on which mail voting risks are of most concern. Our work in Scala, et al., ("A Process Map and Risk Assessment for Mail-based Voting," 2021 IISE Annual Conference &

Expo proceedings) and in 2022 begins accomplishing this by evaluating the likelihood and riskiness of mail voting threats and recommends general mitigations against the most and least likely threat scenarios to take place. The Cybersecurity and Infrastructure Security Agency (CISA) provides further guidance on performing systemic risk reduction.

Risk analyses should not be a one-time occasion. While organizations should aim to be complete when evaluating risk, they should not assume their research is perfect and does not need to be improved. Lists of threats and mitigations should be continuously reviewed since every industry experiences change with the passage of time. Even if these lists do not need to be modified, it is always a good practice to verify their accuracy.

With all of this in mind, we attempt to address the gaps in risk reduction analysis for mail voting by creating a table of mitigations for mail voting threats.

Addressing risks with mitigations

Our proposed table of mail voting threat mitigations relies on the work done in Scala, et al., (2022) and C. Haseltine, S. Wang, and L.A. Albert, "Dynamic Cyber-Physical System Security Planning Using Attack Graphs," (IISE Annual Conference & Expo 2022). As mentioned, Scala, et al., (2022) is an extension of the Election Operations Assessment that updated the EAC's original mail voting Attack tree and calculated risk for the updated Attack tree. Haseltine, et al., uses the mail voting threats from the updated attack tree to begin making a set of mitigations for mail voting threats. This research only maps its mitigations to the updated

Figure 1

Mail-in ballot solutions

The various mitigations to address risks involved in remote and absentee voting.

Mitigation	Description	Threats
M1: Encourage voter registration in local districts*	Increases voter participation. Registration, especially ahead of time, increases the likelihood of mail ballots arriving on time.	N/A
M2: Verify the mailing address and contact information*	Ensures that the mail ballot reaches the correct person when sent.	- Mail ballot is sent to the incorrect voter - Mail ballot is registered to a deceased voter or a voter who moved recently and a third party poses as the voter to submit a vote
M3: Send a notification via text, email, or voice alert via BallotTrax/ BallotScout*	A poll worker should notify the voter if their mail ballot package is/becomes invalid. This must be followed by a replacement ballot package request from the voter.	- Mail ballot becomes lost or stolen - Mail ballot is tampered with or damaged - Voter incorrectly completed mail ballot package
M4: Replacement ballot package request*	After being notified that their mail ballot package is or became invalid, the voter should request another mail ballot.	- Voter notices they did not receive a mail ballot or received a false mail ballot - Voter is informed that the mail ballot package they submitted is invalid
M5: Notify voter to send the ballot back before the deadline*	A poll worker should notify the voter to return a completed mail ballot before the deadline. This may take place after a voter receives their first or replacement mail ballot package.	- Ballot arrival is delayed due to the voter not being aware of the deadline - Ballot arrival is delayed due to supply chain issues (applicable to first and replacement mail ballot packages)
M6: In-person absentee voting*	A voter may choose to return their mail ballot to their local polling place rather than through the mail. Allows a completed mail ballot package to arrive on time.	- Ballot arrival is delayed due to the voter not being aware of the deadline - Ballot arrival is delayed due to supply chain issues (applicable to first and replacement mail ballot packages) - Challenges against a completed mail ballot package (i.e., signature, address, package preparation)
M7: Drop the ballot at drop boxes*	A voter may choose to return their mail ballot to a drop box within their region rather than through the mail. Allows completed mail ballot package to arrive on time.	- Ballot arrival is delayed due to the voter not being aware of the deadline - Ballot arrival is delayed due to supply chain issues (applicable to first and replacement mail ballot packages)
M8: Monitor election staff misbehavior*	Discourages bad behavior from malicious actors. If an adverse event takes place at ballot storage areas or election offices, poll workers can take action against it.	- Malicious actors volunteer as poll workers and conspire to interfere with the mail voting process - Editing, stealing, or destroying completed mail ballot packages after they arrive at election offices - Ballot stuffing
M9: Provide sufficient and comprehensive election staff training*	Poll workers should receive training on mail voting procedures and how to mitigate risks that could arise within the mail voting process.	- Handling delays or mistakes - Mail voting process procedures are misinterpreted by poll workers - Acceptance of completed mail ballot packages with forged signatures or faulty registrations - Rejection of completed mail ballot packages that have been prepared correctly - Offering inaccurate information to voters - Ballot scanners are hacked
M10: Video monitoring*	Discourages bad behavior from malicious actors. If an adverse event takes place at ballot storage areas or election offices, there will be video evidence.	- Damaging or destroying drop boxes - Gaining access to mail ballots within warehouses or election offices - Editing, stealing, or destroying completed mail ballot packages within storage areas - Ballot stuffing - Malicious actors volunteer as poll workers and conspire to interfere with the mail voting process - Editing, stealing, or destroying completed mail ballot packages after they arrive at election offices
M11: Ballot design*	Mail ballots with clear and easily understandable instructions and design will ensure that voters are able to correctly complete their mail ballot package. Multiple formats should be available to accommodate voters with disabilities or voters who speak/understand other languages than English.	- Mail ballot has confusing, misleading, or incorrect instructions - Mail ballot has confusing, misleading, or incorrect design - Voter completes mail ballot package incorrectly or does not vote because of poor instructions or design
M12: Enhanced IT resources*	Decreases the likelihood of system outages and digital attacks.	- Ballot scanner is hacked into and votes are denied or altered - Network shuts down and prevents voters and election officials from accessing resources
M13: Storage security	Limit access to ballot storage areas to a small number of trusted election staff. Ballot storage areas should have daily checks done by elections staff members and be securely locked.	- Damaging or destroying drop boxes or mail boxes - Gaining access to mail ballots within warehouses or election offices - Editing, stealing, or destroying completed mail ballot packages within storage areas - Ballot stuffing within storage areas
M14: Equipment security	Implement physical security mechanisms (locks, tape) onto equipment to dissuade tampering when equipment is not in use. Restrict Internet access within the area when equipment is in use. Equipment should be as updated as possible, and election staff may want to keep backup machines or parts on hand in case of equipment failure.	- Ballot scanner is hacked into and votes are denied or altered - Ballot scanner is tampered with, damaged, or destroyed
M15: Voter roll upkeep	Voter rolls must be checked and updated regularly for outdated or inaccurate registrations. Standardize methodology for cleaning voter rolls so that registrations are correctly being marked as outdated or inaccurate. Notify voters if their registration needs to be updated.	- Mail ballot is sent to the incorrect voter - Mail ballot is registered to a deceased voter or a voter who moved recently and a third party poses as the voter to submit a vote - Voter is unaware that their registration was removed from their region's voter roll and must register again
M16: Enhance voter education	Resources on how to vote by mail and deadlines should be easily accessible (i.e., through the voter's local Board of Elections website) and understandable (written in clear language). Voters should be able to contact elections staff about questions they may have.	- Malicious actor attempts to vote using a peer's mail ballot - Voter believes election misinformation that is unintentionally or deliberately spread - Voter does not understand how to correctly prepare and submit their mail ballot package - Voter is convinced or bribed to vote for certain candidates / issues or to not vote - Voter is unaware of ID requirements within their region - Ballot arrival is delayed due to the voter not being aware of the deadline

Chart created by the authors (mitigations adapted from Haseltine, et al., are denoted with an asterisk).

attack tree's insider threats. We map the mitigations in Haseltine, et al., as well as four additional, original mitigations to all threats in the updated attack tree.

Our table (Figure 1, Page 31) has three columns: the name of the mitigation, a description of the mitigation and a simplified list of mail voting threats the mitigation could counter. Mitigations adapted from Haseltine, et al., are denoted with an asterisk. These generally focus on ensuring a completed mail ballot package will arrive at a voter's local board of elections office on time, as time limitations are a central point in that research.

Other mitigations are concerned with insider threats and cybersecurity. To account for further issues we found important within the sphere of mail voting, our additional four mitigations consider improving the physical security of election infrastructure and better equipping voters with knowledge on voting procedures.

We add storage security (M13) because ballots could be tampered with when left within storage areas if security infrastructure and measures are not sufficient. For mail voting, ballot storage areas do not only include areas within a board of elections office; mailboxes and drop boxes count as well. We also suggest physical protections for voting equipment in equipment security (M14) to complement enhanced IT resources (M12), as both physical and cybersecurity are necessary for ballot scanners. Voter roll upkeep (M15) supplements verify the mailing address and contact information (M2).

Criticism about voter roll purges – deleting registrations of eligible voters, particularly from marginalized populations – have created a need to reexamine how voter rolls should be maintained and updated. With voting disinformation/misinformation becoming a growing problem, enhance voter education (M16) combats this by providing voters with resources to help them vote. This will lessen the likelihood of voters making mistakes and give them a greater sense of trust in elections staff if they know they are able to rely on them for assistance.

These mitigations, and future lists of such, should not be taken as static resources; rather, they should be modified to suit a district's unique needs. Elections in the U.S. are not federalized, so each locality is affected by varying legislation (e.g., not all states allow no-excuse mail ballots)

IISE ANNUAL CONFERENCE & EXPO 2025

Authors can submit conference findings

This article was based on a presentation by the authors at the IISE Annual Conference & Expo 2024 in Montreal. Conference presenters are invited to share their work in *ISE* magazine. Learn how to submit an article for consideration at *iise.org/ISEmagazine/guidelines* or contact Managing Editor Keith Albertson at kalbertson@iise.org.

and may also have different degrees of access to election-related resources (e.g., some districts might have older voting machines).

This means that different parts of the country are more prone to different threats compared to others. Therefore, before implementing any mitigations, districts must identify how impactful they are. They should look to past risk mitigation strategies put into place and pinpoint areas that need and do not need improvement, as well as whether new changes can be implemented.

Blindly deploying mitigations will lead to problems. For instance, if a district's voting manuals or procedures have not been updated, it may be best to invest more time and money into updating its training and policies. However, if the district decides to purchase more security cameras when it already has enough, this would be a waste of resources and, because it did not choose to improve its actual shortcomings, might result in more risks related to insufficient training and poor policies taking place.

Properly assessing how to mitigate risks within the mail voting process first requires identifying threats within the mail voting process. Various sources can be used to build a list of threats, such as news articles on recent events and academic literature. Aside from publications, eliciting information from elections staff and experts familiar with the mail voting process can also be valuable.

The evolving landscape of threats to elections, particularly concerning mail voting, underscores the critical importance of adaptive, informed and collaborative approaches to safeguard the democratic process. Research in this area, combined with the proposed table of mitigations, offers an initial framework to address the multifaceted challenges of mail voting security. Election officials, researchers and policymakers need to work in unison leveraging these insights to enhance the integrity of and trust in the electoral system.

Continuous improvement and innovation in election security practices is key moving forward through 2024 and beyond. It is essential to remember that the strength of democracy lies in the collective effort to ensure every vote is counted accurately, securely and transparently, thereby upholding the fundamental principles upon which the nation was built. ❖

Note: For a full list of references used by the authors for this article, see the *ISE* reference page, *iise.org/isemagazine/references*.

Vanessa Gregorio is a Towson University undergraduate student pursuing a bachelor's degree in business administration with a legal studies concentration. As a student researcher in the Empowering Secure Elections lab, she has assisted in creating an educational module for mail voting, collecting and analyzing survey data, and writing for various projects. During the past two summers, she interned for International Programs at Naval Air Systems Command.

Natalie M. Scala, Ph.D., is an Associate Professor and Director of the graduate programs in Supply Chain Management in the College of Business and Economics at Towson University as well as a Faculty Affiliate at the University of Maryland Applied Research Lab for Intelligence and Security. She earned Ph.D. and master's degrees in industrial engineering from the University of Pittsburgh. Her primary research is in decision analysis with specialization in military and security issues. Her expertise in elections security earned a University System of Maryland Board of Regents Award for Excellence in Public Service, the system's highest faculty honor. In conjunction with Anne Arundel County, Maryland, her work in cybersecurity and threat training for poll workers received a U.S. Elections Assistance Commission Clearinghouse Award for Outstanding Innovation in Election Cybersecurity and Technology. Scala frequently consults to government clients and has extensive professional experience, to include positions with the United States Department of Defense and the RAND Corporation. Her second book, a co-edited volume titled Mathematics in Cyber Research, *was released in 2022.*

Josh Dehlinger, Ph.D., is a Professor in the Department of Computer and Information Sciences and the Director of the undergraduate Computer Science program in the Fisher College of Science and Mathematics at Towson University. He earned his Ph.D. in computer science from Iowa State University in 2007 and served as a research scientist in the Department of Electrical and Computer Engineering at the University of Virginia in 2008. His research expertise lies, broadly, in software safety and reliability, election security, machine learning and software engineering. His recent research efforts have examined the cyber, physical and insider threats to voting processes, including mail voting, and developed training modules for election judges to empower them to identify and mitigate threats during an election. Some of this work, in partnership with the Anne Arundel County (Maryland) Board of Elections was recognized in 2020 with the U.S. Elections Assistance Commission Clearinghouse Award for Outstanding Innovation in Election Cybersecurity and Technology. He and Natalie M. Scala co- direct the Empowering Research Lab at Towson University.