Electoral Integrity Project

5-9th July 2021 — Lisbon Virtual Workshop

Delivering Trusted Elections: New Challenges in Electoral Integrity

Enhancing the Security of Electronic Pollbooks is Essential for Election Integrity

David Levine, Alliance for Securing Democracy
Edward Perez, OSET Institute

Abstract

Democracies around the world are struggling to combat multiple challenges that threaten public confidence in electoral integrity. These threats include both cybersecurity operations and disinformation campaigns. In the election security context, while much of the attention has been paid to voting system vulnerabilities, electronic pollbooks ("e-pollbooks") represent a frequently overlooked election infrastructure asset. E-pollbooks are used in a growing number of countries to validate the eligibility of voters at polling locations and document the issuance of ballots. To properly function, many e-pollbooks need to update information across numerous devices and/or locations. These data exchanges, which can happen with or without wireless communications, add risks to election security. In a worst-case scenario, malicious actors could access e-pollbooks and alter or delete voter registration data, thereby disrupting voting and causing long lines, or even leading to a full-scale meltdown, with voters and election officials alike desperately trying to make sense of a chaotic situation. This paper offers guidance for how to use e-pollbooks in a more secure and effective manner. It includes information on implementing cybersecurity best practices for e-pollbooks, tailoring poll worker training to address procedures for e-pollbook failures, and ensuring that necessary materials are available to continue voting even if the e-pollbooks become inoperable. It also includes recommendations for identifying potential vulnerabilities in e-pollbooks through the procurement process.

Keywords

Election integrity, election security, election interference, electronic pollbooks, elections

Table of Contents

I: Introduction

Democracies around the globe are currently struggling to respond to multiple challenges that pose threats to public confidence in the legitimacy of election outcomes. Recent research and reporting have illustrated efforts to undermine democratic processes in Australia,[1] North and South America, Europe, Africa, and Asia.[2] These threats include cybersecurity operations[3] as well as disinformation campaigns.[4] More specifically, election interference typically takes one of two forms. The first is influence campaigns designed to affect "hearts and minds."[5] This includes overt and covert efforts to manipulate voter preferences and turnout through the dissemination of information.[6] The second form targets election infrastructure. This form targets the technical aspects of the election, such as voter registration, the casting and counting of ballots, and the reporting of results, and can have a more direct impact on the electoral outcome.[7] Both types of activities are also sometimes done in conjunction with one another to undermine confidence in the integrity of an election more broadly.[8]

In the election-security context, much attention has been paid to voting systems, because they capture and count the voters' ballot choices that ultimately generate the results. Like any technology, voting systems have vulnerabilities, and these vulnerabilities have been documented

---

1 Paul Karp, "Russian Twitter Trolls stoking anti-Islamic sentiment in Australia, experts warn," The Guardian (online, 20 November 2018), https://www.theguardian.com/australia-news/2018/nov/20/russian-twitter-trolls-stoking-anti-islamic-sentiment-in-australia-experts-warn

2 Qi Cheng et. al, "Hacking Democracy: Cybersecurity and Global Election Interference," Henry M. Jackson School of International Studies, University of Washington, Seattle (2018), https://jsis.washington.edu/news/hacking-democracy/

3 van der Staak and Wolf, "Cybersecurity in Elections," Institute for Democracy and Electoral Assistance (2019), https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

4 Bandeira, et. al., "Disinformation in Democracies: Strengthening Digital Resilience in Latin America," The Atlantic Council (2019), https://www.atlanticcouncil.org/wp-content/uploads/2019/09/Disinformation-in-Democracies.pdf

5 "Prepare for the Worst and Fight for the Best: A Citizen's Guide to 2020 Electoral Interference," Just Security (2020), https://www.justsecurity.org/72491/prepare-for-the-worst-and-fight-for-the-best-a-citizens-guide-to-2020-electoral-interference/

6 Dawood, "Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats," Election Law Journal, Vol. 20. No. 1 (2021), https://www.liebertpub.com/doi/pdf/10.1089/elj.2020.0652c

7 "Prepare for the Worst and Fight for the Best: A Citizen's Guide to 2020 Electoral Interference," Just Security (2020), https://www.justsecurity.org/72491/prepare-for-the-worst-and-fight-for-the-best-a-citizens-guide-to-2020-electoral-interference/ See also National Intelligence Council, Intelligence Community Assessment, "Foreign Threats to the 2020 US Federal Elections" (2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

8 Dawood, "Combatting Foreign Election Interference: Canada's Electoral Ecosystem: Approach to Disinformation and Cyber Threats, "Election law Journal, Vol. 20. No. 1 (2021), https://www.liebertpub.com/doi/pdf/10.1089/elj.2020.0652c

extensively.[9] In contrast, much less attention has been paid to electronic pollbooks (e-pollbooks), which are used to validate the eligibility of voters at polling locations and document the issuance of ballots (sometimes referred to as "posting" voters). While e-pollbooks do not record voter choices or tabulate election results, they are vulnerable to cybersecurity and disinformation attacks that can disrupt the voting process and/or undermine public confidence in the election, more generally. Furthermore, unlike voting technology, which is typically physically isolated and not connected to other networked infrastructure, e-pollbooks are often connected to cloud-based networks, which provide additional avenues for compromises and malfeasance. Even without changing votes, an attacker who interferes with electronic pollbooks could undermine confidence in an election in a variety of ways.

Furthermore, fewer uniform standards exist for the use of e-pollbooks in comparison to voting systems. For example, in the United States, although there is a federal testing and certification program for voting systems based on voluntary national guidelines,[10] no such program currently exists for the testing and certification of e-pollbooks.

This paper examines e-pollbook risks and explores ways to prevent, detect, and recover from e-pollbook attacks that could otherwise potentially undermine public confidence in the legitimacy of election outcomes.

- Section II provides a more detailed introduction to electronic pollbooks and how they function;
- Section III outlines the security risks associated with their use;
- Section IV addresses technical measures to mitigate security risks;
- Section V addresses operational practices to mitigate security risks; and
- Section VI addresses best practices for training and polling place operations.

II. E-Pollbooks: An Overview

What Are E-Pollbooks?

E-pollbooks are electronic versions of voter registries that contain a list of eligible voters in the relevant jurisdiction.[11] This includes the hardware and/or software that allow election officials to review and maintain voter information for an election.[12]

---

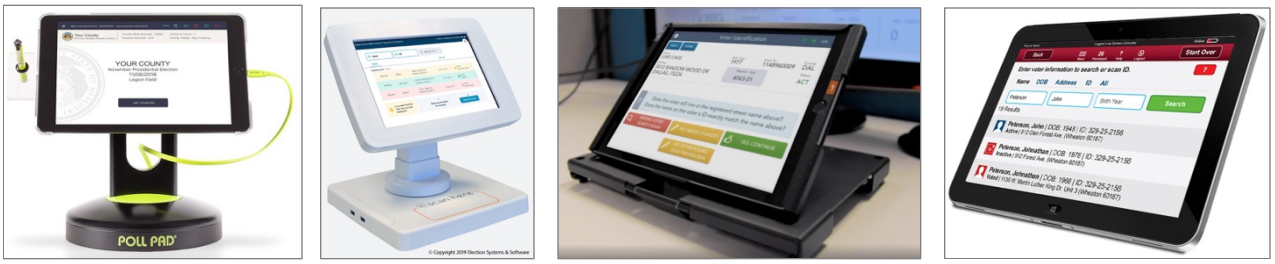
9 "Securing The Vote," The National Academies of Sciences, Engineering, and Medicine (2018), https://www.nationalacademies.org/news/2018/09/securing-the-vote-new-report

10 U.S. Election Assistance Commission, "Voluntary Voting System Guidelines," https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

11 "The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration" (2014), https://www.eac.gov/sites/default/files/eac_assets/1/6/Amer-Voting-Exper-final-draft-01-09-14-508.pdf

12 Verified Voting, "Electronic Poll Book Use in the United States," https://verifiedvoting.org/wp-content/uploads/2020/08/Verified-Voting-Electronic-Poll-Book-Use-in-the-United-States-20200831.pdf

Electronic pollbooks are often, but not always,[13] proprietary software installed on commercial-off-the-shelf devices such as electronic tablets or laptop computers.[14]



Knowink PollPad | ES&S ExpressPoll | Tenex PrecinctCentral | Robis AskEd

Figure 1. Representative Sample – Popular E-Pollbooks in the U.S.

Generally, polling officials use e-pollbooks to verify a voter's eligibility to cast a ballot and check in the voter at a polling place before voting. E-pollbooks enable polling officials to look up voters and verify their qualifying personal information (such as their address and date of birth). They also generally allow the voter to sign his/her name before the voter is "posted." In some places, e-pollbooks can export information that allows electronic voting machines to display the proper digital ballot style to a voter (although they are physically separated by an "air gap").[15] In other places, e-pollbooks provide an additional safeguard against double voting by offering real-time updates about voter participation throughout an election. [16]

E-pollbooks can facilitate the check-in and verification of voters at polling places, and when used properly, they can help reduce voting wait times.[17] According to the International Institute for Democracy and Electoral Assistance (IDEA), at least 42 countries throughout the world use e-pollbooks to identify voters at polling stations.[18] Thirty-two countries use e-pollbooks that are

---

13 In the US, in some individual states, such as the Commonwealth of Virginia and the States of Michigan and Colorado, for example, the state elections division has developed its own computer software to support verification of voter eligibility during check-in at polling places. In those states, the software is installed on COTS laptop computers. See Verified Voting, "In-House Electronic Poll Books," https://verifiedvoting.org/election-system/in-house-electronic-poll-books/

14 "A Handbook for Elections Infrastructure Security," Center for Internet Security (2018), p. 19, https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

15 An "air gap" is a network security measure to ensure that sensitive computing components (like voting systems) are physically isolated from other networks.

16 See, for example, safeguards against "multiple voting" in OSCE Office for Democratic Institutions and Human Rights, "Romania Presidential Election ODIHR Needs Assessment Mission Report" (2019), https://www.osce.org/files/f/documents/2/9/426629_0.pdf

17 See, for example, "Electronic lists – the roll of the future?" p. 8, in Annual Report of the Australian Electoral Commission, https://annualreport.aec.gov.au/2013/contents/files/aec-annual-report-12-13.pdf

18 International IDEA, "Is Technology Used for Identifying Voters at Polling Stations (Electronic Poll Books)?," https://www.idea.int/data-tools/question-view/740

offline and only access registration data in the polling station, while ten countries use e-pollbooks connected to a central voter registration database via the Internet.

Furthermore, in the United States, roughly 75 percent of registered voters lived in jurisdictions that used e-pollbooks in 2020.[19]

The primary input to e-pollbooks is information contained in the voter registration database.[20] Voter registration databases are systems designed to ensure the accuracy and integrity of voter registration records maintained by election management bodies. They house data associated with a district's eligible voters and support critical functions of an election management body—from determining voter eligibility to maintaining voting district data to producing voter rolls for pollbooks. They too have vulnerabilities that, if successfully exploited, can lead to voter registration data being deleted or altered. However, if proper cybersecurity practices are observed,[21] illicit efforts to alter voter data can be mitigated, and voters can learn of changes to records—at the latest when they attempt to vote, and hopefully sooner.

The primary output from e-pollbooks is a record of issuing a ballot to the voter (also known as "posting" the voter). In some cases, posting the voter prompts the e-pollbook to print ballot style information that can be used to activate the vote capture device in the voting system. Again, this is typically facilitated across an "air gap" that keeps e-pollbook check-in components separate from the voting system itself. For example, upon posting a voter, an e-pollbook may print a barcode containing a particular precinct ballot style but no other personally identifiable voter information. The barcode can then be scanned on a separate voting machine to activate the correct digital ballot for that voter. This process may reduce the possibility that polling officials provide voters with the wrong ballot.

According to Verified Voting, e-pollbooks' "dynamic functionality and capacity to hold data from entire jurisdictions give electronic pollbooks some advantages over paper poll books."[22] For example, e-pollbooks may allow poll workers to access a jurisdiction's entire voter registry with a continuous connection, enabling workers to make real-time updates and, in jurisdictions with more than one polling place, to assist voters who may not be at their correct polling place.[23] E-pollbooks can also be used by polling officials in "super precincts" (also called "vote centers"), polling places that combine multiple precincts to allow voters to choose at which location to vote, and other non-neighborhood voting locations to determine if a voter has already voted

---

19 Verified Voting, "Electronic Poll Book Use in the United States," https://verifiedvoting.org/wp-content/uploads/2020/08/Verified-Voting-Electronic-Poll-Book-Use-in-the-United-States-20200831.pdf

20 See "Voter Registration Databases and e-Pollbooks" in "The State and Local Election Cybersecurity Playbook," The Belfer Center for Science and International Affairs, Harvard Kennedy School (2018), https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#voterreg

See also "A Handbook for Elections Infrastructure Security," Center for Internet Security (2018), p. 18, https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

21 See, for example, University of Pittsburgh, Institute for Cyber Law, Policy and Security, "The Blue Ribbon Commission on Pennsylvania's Election Security: Study and Recommendations" (2019), https://www.cyber.pitt.edu/sites/default/files/final_full_pittcyber_pas_election_security_report.pdf

22 Verified Voting, "Electronic Poll Book Use in the United States," https://verifiedvoting.org/wp-content/uploads/2020/08/Verified-Voting-Electronic-Poll-Book-Use-in-the-United-States-20200831.pdf

23 Ibid.

elsewhere in the jurisdiction. And in places that allow for same-day voter registration, e-pollbooks can even be used to register voters. [24]

The functionality of e-pollbooks can vary widely between jurisdictions. [25] For example, not all e-pollbooks are deployed to have real-time connections to cloud servers that hold the voter registration database; instead, in some locations, e-pollbooks are deployed in "standalone" fashion, so that the devices in any given polling place access their voter registration data locally, and the devices are not exchanging data with anything else. In other places, e-pollbook devices have peer-to-peer communication only, allowing pollbooks to communicate and sync with each other in the same facility, so that multiple check-in stations can be available in one polling location even though none are communicating to a central database in the cloud.

What Makes E-Pollbooks Popular?

In 2014, the U.S. Presidential Commission on Election Administration (PCEA) recommended that election officials adopt e-pollbooks to check in voters at polling places,[26] citing several perceived benefits that have also been cited in other countries,[27] including the following:

1. **Electronic pollbooks can facilitate more effective support for voters and potentially better voting experiences.** The PCEA notes that paper pollbooks only contain the names of voters eligible to vote in a specific precinct. "If the voter is in line for the wrong precinct or in the wrong polling place and reaches the front of the line, the election worker with the paper pollbook cannot resolve the issue. Thus, the voter must be removed from the line until the issue is resolved—often by contacting the central election office, which may be busy addressing a number of other issues. Even in the best of circumstances, the voter is inconvenienced, and the capacity of the central election office is taxed."[28] In contrast to paper pollbooks, e-pollbooks often allow poll workers to not only confirm that a voter is in the wrong polling place, but to direct him/her to the correct location.
2. **E-pollbooks benefit poll workers.** E-pollbooks can help reduce poll worker errors frequently associated with paper-based voter check-in processes. According to the PCEA, "Poll workers sometimes fail to check-in voters, distribute the wrong ballots, or send voters

---

24 Ibid.

25 For a more detailed list of functions typically available on e-pollbooks, see "What Can E-Poll Books Do?," National Conference of State Legislatures, https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

26 "The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration" (2014), https://www.eac.gov/sites/default/files/eac_assets/1/6/Amer-Voting-Exper-final-draft-01-09-14-508.pdf

27 See, for example, OSCE Office for Democratic Institutions and Human Rights, "Norway: Parliamentary Elections OSCE/ODIHR Election Expert Team Report, p. 6, "Electronic Administration" (2017), https://www.osce.org/files/f/documents/3/a/360336.pdf

28 See p. 44, "The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration" (2014), https://www.eac.gov/sites/default/files/eac_assets/1/6/Amer-Voting-Exper-final-draft-01-09-14-508.pdf

to the wrong polling place."[29] E-pollbooks can help address each of these issues by automating these processes and notifying poll workers if they have not been completed. E-pollbooks can also help gather data on polling place wait times and traffic since they often keep track of when a voter arrives and checks in.[30] Election officials can review this data to help determine how many voting systems, e-pollbooks, and workers they will need to staff similar future elections.

3. **E-pollbooks can help save money by reducing printing costs.** While the initial purchase of e-pollbooks is often a significant up-front capital expenditure, using them for an extended period of time can reduce costs. Rather than generating thousands of pages of paper voter rolls for each election, electronic pollbooks can simply be reprogrammed before each election.[31] Such savings can subsequently be put towards securing other parts of the election process.

III. E-Pollbook Security Risks

In addition to their potential benefits, the use of e-pollbooks also introduces additional security risks. Because there is a lack of uniform standards for their use, there is relatively little regulation and oversight over how they should be safely operated. Additionally, the network-connected infrastructure associated with e-pollbooks introduces new avenues for potential hacking or operational issues that could impact the voting experience and, more broadly, public confidence in elections.[32]

Even though e-pollbooks are growing in popularity, standards for their security, reliability, and usability remain inconsistent, especially in comparison to voting systems. In the United States, for example, there is no national federal testing and certification program for e-pollbooks. Only a handful of states have their own certification programs to ensure that their e-pollbooks meet their own functionality and design requirements,[33] and many jurisdictions do not regulate or conduct oversight on their e-pollbooks.

Furthermore, unlike most voting systems, which are "air gapped" and not connected to the Internet or other networks, e-pollbooks use technology that enables them to communicate with voter registration databases in cloud-based servers or with other e-pollbook devices in the same polling location—either via a physical connection or a wireless network. These connections introduce vulnerabilities associated with remote hacking or network failure.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) in its "Election Infrastructure Cyber Risk Assessment,"

---

29 Ibid.

30 Ibid.

31 Ibid.

32 Kim Zetter, "The election security hole everyone ignores," POLITICO (August 2020), https://www.politico.com/news/2020/08/31/election-security-hole-406471

33 National Conference of State Legislatures, "Electronic Poll Books," https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

> *The scale of a cyber-attack on election infrastructure has the potential to be more widespread if an attack compromises networked infrastructure. For example, electronic pollbooks in some jurisdictions are networked together across the jurisdiction to facilitate vote center operation, whereas electronic pollbooks in other jurisdictions are non-networked. A cyber-attack on an individual non-networked pollbook has less chance to spread if the machine remains isolated from a network. An integrity attack on a networked e-pollbook has the potential to affect an entire jurisdiction, while an integrity attack on a local, non-networked pollbook can be isolated to that particular voting location.*[34]

If a sophisticated adversary exploits the network connections that e-pollbooks depend upon and gains access to the connected devices and components, the attacker could disrupt voting through a variety of actions. For example, the Center for Internet Security (CIS) identifies the following electronic pollbook security risks:[35]

- **Alteration of data**. The integrity of voter registration data can be compromised. For example, if an attacker successfully accesses an electronic pollbook through a wireless network connection, data could be altered to remove a voter's registration record or to make it appear as if the voter has already voted even if he/she has not.
- **Availability**. By modifying voter registration records, disrupting e-pollbook connectivity, or disabling ("crashing") poll books altogether, an attacker could bring the voting check-in process to a standstill in polling stations. Many citizens could be forced to wait much longer to vote, confusion could quickly spread about what was occurring, and some voters' faith in the election process could be undermined.
- **Ballot activation**. As noted earlier, in some jurisdictions, e-pollbooks are used to facilitate ballot activation on (separate) electronic voting machines. For example, e-pollbooks can generate QR codes with anonymous ballot styles that can be scanned by voting machines, or they can be used to encode "smart cards" that polling officials use to activate digital ballots on marking devices. According to investigative journalist Kim Zetter, "A hacker could potentially cause an e-pollbook to embed malicious commands in the voter access card, barcode or QR code that some of those devices use to convey instructions to the voting machines."[36]
- **Voter privacy**. Although practices and restrictions vary across different jurisdictions, e-pollbooks may store non-public, personally identifiable information (PII) such as voters' dates of birth, identification numbers, addresses, and other sensitive information. An unauthorized party could gain access to, and possibly expose, this confidential information.

---

34 "Election Infrastructure Cyber Risk Assessment," U.S. Cybersecurity and Infrastructure Security Agency (July 2020), https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf

35 "A Handbook for Elections Infrastructure Security," Center for Internet Security (2018), p. 19, https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

36 Kim Zetter, "The election security hole everyone ignores," POLITICO (August 2020), https://www.politico.com/news/2020/08/31/election-security-hole-406471

These threats are not theoretical. During the 2016 U.S. presidential election, many voters went to vote in several North Carolina precincts only to discover that the e-pollbooks had inaccurate information in them, such as notations showing that voters had already voted when they had not.[37] Investigators later discovered that the vendor that had provided those poll books had been the target of a Russian cyberattack, though it remains unclear whether the two incidents were linked.[38]

Electronic pollbooks can also significantly disrupt the voting process if they experience technology failures. For example, after experiencing problems uploading all of its early in-person voting into its e-pollbooks early on Election Day, the Franklin County, Ohio Board of Elections decided to switch to using its backup paper pollbooks for the 2020 presidential election.[39] Franklin County wanted to ensure that voters would not be able to vote twice without being detected, and it could not confirm that its e-pollbooks had all of the county's early in-person voting information on them. Problems with e-pollbooks also contributed to voting delays in 2020 in several other states, including Georgia, Ohio, Nevada, and Texas.[40]

Finally, contingency plans for responding to e-pollbook interruptions have shortcomings as well.[41] In many jurisdictions, if a voter's eligibility cannot be validated due to e-pollbook disruptions, the voter is issued a "conditional" ballot. This allows the voter to vote—***however***, the vote is only counted upon a post-election verification of the voter's registration status. In the United States, these conditional ballots are commonly known as "provisional" ballots. The issuance of large numbers of conditional or provisional ballots has downsides. They require more time for election officials to process after the election, before results can be certified; they are sometimes rejected at a high rate; and, particularly for voters who are self-assured about the status of their registration, being issued only a "conditional" ballot can undermine their confidence that their ballot will be counted as cast.

Amplifying the Risks: Misinformation and Disinformation

Deploying complex election technologies prone to human error, cyberattacks, and technical failures creates a fertile environment for the dissemination of false or misleading information. Whether spread intentionally or based on honest misunderstandings of common election

---

37 Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied to Voting Day Disruptions," NPR (August 2017), https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions

38 Kim Zetter, "How close did Russia really come to hacking the 2016 election?" POLITICO (December 2019), https://www.politico.com/states/florida/story/2019/12/26/politico-magazine-how-close-did-russia-really-come-to-hacking-the-2016-election-1237544

39 Khaleda Rahman, "Franklin County, Ohio Switches to Paper Pollbooks After Technical Difficulties with Voting Data," Newsweek (November 2020), https://www.newsweek.com/franklin-county-ohio-switches-paper-pollbooks-technical-issues-1544410

40 Kartikay Mehrota and Margaret Newkirk, "Voter Check-In Systems Slow Down Voting and Results Across U.S.," Bloomberg (November 2020), https://www.bloomberg.com/news/articles/2020-11-04/voter-check-in-systems-cause-sprawling-voting-and-results-delays

41 See, for example, University of Pittsburgh, Institute for Cyber Law, Policy and Security, "The Blue Ribbon Commission on Pennsylvania's Election Security: Study and Recommendations" (2019), https://www.cyber.pitt.edu/sites/default/files/final_full_pittcyber_pas_election_security_report.pdf

processes, false information can spread quickly and undermine public confidence in the election. Election processes associated with voter registration and e-pollbooks are not immune to this risk.[42]

A particularly worrisome phenomenon is "disinformation aggregation" — the ability of disinformation actors to aggregate *true* reports of typical dysfunction (for example, a power outage that impacts polling place operations), *spurious* similar reports, *speculative* "suspected malfeasance" reports by real people, and *intentionally fabricated* similar reports. The artful combination of just enough factual information to make something seem plausible, in conjunction with false or misleading information, is a toxic mix—with the capacity to go viral through social media. Here are some examples of what these tactics might look like:[43]

- Disinformation actors deface official election office websites (for example, "#RIGGED") and claim that voter registration data has been altered.
- Disinformation actors characterize election officials' inability to reliably update voter registration information after an early voting period as a voter suppression tactic that exclusively affects registered voters affiliated with one or more specific political parties.
- If e-pollbooks "freeze" due to configuration issues or lack of pre-election testing, causing long lines, disinformation actors conduct a social media campaign with a fabricated story that independent attacks have been made against actual state and local government networks.

These examples illustrate how real issues in a complex operating environment can be used as a basis to disseminate false information that undermines confidence in elections. Because e-pollbooks are subject to genuine disruptions and operational problems due to configuration issues and a vulnerable network environment, it is imperative that technical measures be applied to mitigate security risks and help ensure the reliable operation of e-pollbooks so that their deployment does not become fertile ground for disinformation tactics.

IV. Technical Measures to Mitigate E-Pollbook Security Risks

Election management bodies that use e-pollbooks should implement cyber- and physical security best practices to mitigate risks associated with their use. As a practical matter, most of these risks stem from network connections and/or data transmission with voter registration (VR) databases or other devices; loading VR data onto e-pollbook devices as part of pre-election configuration procedures (either through wired or wireless connections, or through the use of USB devices and other removable media); and physical security considerations.

---

42 See, for example, "Public Service Announcement: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections," U.S. Cybersecurity and Infrastructure Security Agency (September 2020), https://www.cisa.gov/sites/default/files/publications/PSA_voter_registration_data_508pobs.pdf

43 OSET Institute, Inc., TrustTheVote® Project, "Murphy's Guide to the 2020 Election," https://trustthevote.org/murphysguidetothe2020election/

Below is a compendium of some of the most important practices that election officials should consider to mitigate e-pollbook risks, as identified by the Center for Internet Security (CIS).[44]

Network Infrastructure Security

- **Assess connections to other internal systems.** It is critical to understand where voter registration data is stored and who has access to it. Are there other internal systems that the VR system can connect to? Other internal systems may be owned or operated by organizations or authorities other than the elections division. It is best to segregate VR data from non-election supporting systems.
- **Avoid wireless connectivity.** If possible, connectivity to wireless networks should be limited or eliminated altogether. If wireless connections are implemented, ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.
- **Restrict connections to authorized IP addresses only.** Through whitelisting, system administrators can regulate which IP addresses can access electronic pollbooks. Security settings must prevent other devices from detecting and connecting to networks in polling places.
- **Close unused ports and services.** Ensure that only required ports are open on the system through regular port scans.
- **Restrict devices on the network.** Build an inventory of authorized e-pollbook devices.
- **Monitor the network.** Implement network intrusion detection and monitoring systems, and regularly scan the network to ensure that only authorized devices are connected.
- **Regularly maintain the network and apply necessary security patches.**
- **Reduce administrative access.** Limit the number of individuals with administrative access to the platform and remove any default credentials.
- **Protect sensitive data.** Voter registration files should be encrypted and protected while in transit, in use, and at rest.
- **Isolate e-pollbooks from voting system components.** E-pollbook components and the networks they rely on should never be directly connected to any components of the voting system.

Endpoint Security (The E-Pollbook Devices)

- **Restrict executable applications to only what is required.** CIS recommends that government jurisdictions work with their vendors to implement application whitelisting for e-pollbook devices. Whitelists allow the pollbooks to run only approved software and prevent execution of all other software.

---

44 Not an exhaustive list. For additional details, see pp. 36-55, "A Handbook for Elections Infrastructure Security," Center for Internet Security (2018), https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

- **Harden the operating system**. Jurisdictions should also work with their vendors to ensure that the base commercial-off-the-shelf (COTS) operating system (OS) has been "hardened" to minimize security vulnerabilities, disable any unneeded services, and install any applicable OS updates or security patches before each election to protect against known vulnerabilities.
- **If possible, implement e-pollbooks in "kiosk mode**." Kiosk-configured devices restrict the operating environment so that poll worker end-users can only access those software features needed to do their jobs. Access to any other software applications or utilities is restricted.
- **Seal exposed ports**. Place tamper-evident seals on any exposed ports on individual e-pollbook devices.
- **Employ user access controls**. Access to e-pollbook functions should be protected by strong passwords that are changed each election.
- **Validate data transferred between systems**. E-pollbooks should be implemented to use digital signatures and hashes to verify the integrity of data contained in voter roll files that are transferred, and to ensure data has not been maliciously altered or compromised.
- **Manage hardware inventory**. Ensure that all e-pollbook devices are documented and accounted for throughout their lifecycle. Any devices lost, decommissioned, returned, or otherwise disposed of must be permanently erased of any software and voter data. Documentation of "wiping" procedures should be retained for audit purposes.

Physical Security and Inventory

- **Restrict access to authorized personnel only**. Implement physical security protocols to ensure that only authorized personnel can access the elections division warehouse and polling places. Consider physical and/or electronic locks, surveillance video, personnel credentials, and tamper-evident seals.
- **Maintain strict chain-of-custody** with appropriate controls and documentation to track, control, and secure individual devices, and to document who accesses them.
- **Manage, track, and limit any data transfers using removable media**. If using flash memory devices such as USB devices to load or export data from e-pollbook devices (for example, instead of using network connections), create an inventory of approved, secure devices and track them. Only approved and managed USB devices with appropriate device encryption and device authentication should be used to transfer e-pollbook data, and they should be managed with chain-of-custody and administrative safeguards.

V. Enhancing Operational Security Associated with E-Pollbooks

In addition to employing best practices for cybersecurity, the reliability and security of e-pollbook operations requires accountability from vendors and rigorous contingency planning. Just like voting systems and any other technology, e-pollbooks have security vulnerabilities—and configuration mistakes can also leave e-pollbooks unnecessarily exposed to attackers. Accordingly, election officials and vendors must prepare for the unexpected. This should include working together to develop e-pollbook security plans and perform pre-election testing. Election officials should also deploy backup paper pollbooks and provisional ballot materials to help mitigate these risks.

Holding Vendors Accountable During Procurement and Implementation

Election officials need to actively engage technology vendors to ensure secure implementation of e-pollbooks and other network-connected infrastructure, including during the procurement process. Accepting vendor assurances that their products are "secure," or allowing vendors to define the requirements and features intended to achieve "security," is not sufficient; independent assessments are essential. According to Harvard University's Belfer Center for Science and International Affairs, "Performing a security risk assessment of vendors during the request for proposal (RFP) process can reveal vendor vulnerabilities and reduce future exposure to external attacks."[45] Such assessments should also occur on a regular, ongoing basis once the vendor is chosen to ensure continued compliance.[46]

In a similar vein, CIS recommends that vendors be subject to regular independent audits of security controls, with results made available to the elections office. CIS also recommends that vendors be required to provide documentation of their cybersecurity processes and protocols and a security plan as one of the contract deliverables. Such a plan should include answers to questions such as:

- How does the vendor protect its own facility, data center, and software?
- How does the vendor protect voter registration data that is provided to the vendor? Where is the data stored, and who has access to it? Is the data stored on privately controlled servers? Multiple servers?
- How does e-pollbook software and hardware protect against purposeful attacks such as hackers, malware, and viruses?
- How is sensitive elections-related data protected at rest, in transit, and while in use?
- How are information records responsibly destroyed?
- How does the usability of e-pollbook software and hardware reduce the likelihood of human error that could compromise security?

---

45 See "Appendix 1. Vendor Selection and Management," in ""The State and Local Election Cybersecurity Playbook," The Belfer Center for Science and International Affairs, Harvard Kennedy School (2018), https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#app1

46 Ibid.

- How do software and/or product features help to respond and protect data in the event that an e-pollbook is lost or stolen?
- What are the service level agreements (SLAs) that will be included in the contract?
- For how long will the vendor provide security updates to the implemented system?

In short, any contract with a vendor should include clearly defined security requirements, periodic audits based on these requirements, and documented incident response plans and processes.[47]

If devising requirements appears daunting, election officials may find it valuable to craft detailed questions for their prospective vendor based on a review of e-pollbook evaluation checklists obtained from elsewhere, in conjunction with their IT support team. Three resources are particularly valuable in this regard: 1) requests for proposal (RFPs) from other election jurisdictions; 2) checklists and testing protocols from certifying authorities that approve e-pollbooks for use; and 3) resources from other external entities with established expertise in enhancing the security of infrastructure like electronic pollbooks. While specific requirements vary from place to place, these resources can be helpful in clarifying common security standards and valuable or desirable functionality.[48]

One final consideration is essential in keeping vendors accountable and reducing risks associated with e-pollbook use: **pre-election testing** to ensure that the e-pollbooks are ready to use for Election Day. Pre-election stress and load testing must accurately reflect the volume of voter records, updates, and potential data transactions that could occur during peak times in polling places. In the absence of such realistic stress and load testing, e-pollbooks and/or the voter registration system may operate slowly in real-world conditions, or perhaps not at all (that is, the system may "crash" or "freeze"). Pre-election testing can also help identify any configuration or programming issues that diverge from the poll worker training, which could create confusion or inefficiency that leads to an Election Day fiasco.[49]

---

47 See "Contracting for systems or services" pp. 31-32 in "A Handbook for Elections Infrastructure Security," Center for Internet Security (2018), https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

48 For examples of state-specific testing protocols associated with e-pollbook use in the US, see Indiana (https://www.in.gov/sos/elections/voter-information/files/2019-EPB-Certification-Protocol_Signed.pdf), Ohio (https://www.ohiosos.gov/globalassets/elections/bvme/epollbooks/testlab.pdf), and Texas (https://www.sos.texas.gov/elections/forms/electronic-pollbook-technical-testing-matrix-101519.pdf)

49 See, for example, Kim Zetter, "L.A. County found the cause of its hourslong poll lines. It wasn't the new voting machines." POLITICO (June 2020), https://www.politico.com/news/2020/06/17/la-county-blames-voter-check-in-tablets-for-election-day-chaos-324894

Backups: Paper Pollbooks and Conditional Ballots

Because unanticipated errors and problems can arise with e-pollbooks, potentially leading to long lines or obstacles to continuous voting, election officials must expect the unexpected and prepare for contingencies.[50] Along with many U.S. election officials, the Brennan Center for Justice at New York University emphasizes that paper backups of e-pollbooks are an excellent resiliency measure in case e-pollbooks fail: "They allow poll workers to continue confirming voters' eligibility, diminish the potential for long lines, and may minimize the need to issue provisional [conditional] ballots."[51]

As noted earlier, if backup paper pollbooks are not available, it may be impossible for election officials to verify voter eligibility in the polling place. But even under such conditions, if a generous supply of provisional/conditional ballots and associated materials are available (such as privacy envelopes with instructions for voter attestations of eligibility), voting could continue even if the e-pollbook system is unavailable for use. The Brennan Center recommends having enough provisional ballot materials to account for two to three hours of peak voting activity as a backup measure.[52]

Finally, future developments in e-pollbook designs could also mitigate these risks. For example, if future e-pollbook devices could be capable of printing lists of voters who have already voted in polling places—even if the voter lookup feature malfunctions—this could still help to ensure that more voters can cast a regular (non-provisional/conditional) ballot,[53] even when the unexpected occurs.

VI: Training and Polling Place Operations

Because electronic pollbooks cannot be entirely secured against technology failures and cyberattacks, methodical training for poll workers is also an essential part of mitigating risks and vulnerabilities associated with e-pollbooks. In this section, we highlight three essential training needs: 1) ensuring that poll workers understand and are familiar with "normal" e-pollbook operations, as well as 2) explicitly training poll workers on how to address e-pollbook

---

50 See, for example, William Adler and David Levine, "Trusting the Vote: Establishing a Presidential Commission on Election Resilience and Trust," Center for Democracy and Technology and Alliance for Securing Democracy (February 2021), https://securingdemocracy.gmfus.org/wp-content/uploads/2021/01/Presidential-Commission-on-Election-Resilience-and-Trust.pdf

51 Edgardo Cortes, et. al., "Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials," Brennan Center for Justice (December 2019), https://www.brennancenter.org/our-work/policy-solutions/preparing-cyberattacks-and-technical-failures-guide-election-officials

52 Ibid.

53 See "How Can Pennsylvania Improve Contingency Planning" p.58 in University of Pittsburgh, Institute for Cyber Law, Policy and Security, "The Blue Ribbon Commission on Pennsylvania's Election Security: Study and Recommendations" (2019), https://www.cyber.pitt.edu/sites/default/files/final_full_pittcyber_pas_election_security_report.pdf

failures, with a particular eye toward 3) using backup paper pollbooks and/or provisional/ conditional ballots.

Provide Training for Basic E-Pollbook Operations

First, poll workers need a foundational understanding of the e-pollbooks. This includes an introduction to how the e-pollbook operates, procedures for how to network e-pollbooks if more than one e-pollbook device is being used in a polling place, and instructions for how to properly open the polls at the start of the day to support voter lookup functions. If more than one device is used, once the e-pollbooks are open, poll workers must learn how to check e-pollbooks to ensure that they are synchronized (that is that the vote totals at the bottom of the screen in one e-pollbook device match the vote totals of the other e-pollbooks in the polling place). And of course, in addition to setup operations, poll workers need to be trained on how to successfully complete some of the most frequently used Election Day procedures with the e-pollbook, such as searching for a voter by name or by address and assisting a voter if he/she cannot be found in the e-pollbook.

Provide Training for Addressing E-Pollbook Failures

Jurisdictions should evaluate their e-pollbook recovery procedures to ensure that they will be easy for poll workers to follow and will not introduce new obstacles to voters casting their ballots quickly, even when issues arise. This can be achieved by assessing poll workers periodically on their knowledge of the e-pollbooks' basic operations, and then walking through scenarios of what to do when e-pollbooks appear to experience technical issues.

At minimum, the poll workers running their polling places must be trained on additional procedures and trouble-shooting solutions for less common Election Day occurrences, such as e-pollbook failures. For example, if an e-pollbook appears to be unresponsive to touch from the appropriate device (for example, a stylus designed for the e-pollbook) and there appears to be no activity on the screen, poll workers are often recommended to first wait 30-60 seconds, and then to reboot the e-pollbook if it remains frozen. If this issue occurs multiple times, the e-pollbook could be experiencing more significant issues, and there should be communication protocols in place to escalate this issue to the attention of individuals with more technical expertise, perhaps at the central elections office. Poll workers must also be trained in how to respond in case of a power outage at a polling place to ensure that e-pollbooks can continue to operate on backup battery power for a limited period of time. In general, the escalation protocols should clearly define when e-pollbooks should be removed from service and when the poll worker should shift to using paper backup pollbooks or provisional ballot materials, if they are available.

Provide Training on Backup Paper Pollbooks and Provisional/Conditional Ballots

It is common for election officials to spend the majority of poll worker training time on "normal" operations. With time a valuable resource and poll workers increasingly challenged to learn more and more technology and complex procedures, it is understandable if election officials focus on what is "basic" and expected. E-pollbook procedures are just one part of Election Day; assisting voters with the voting process itself is also a necessity, and it can be complex.

However, the need to train poll workers on the "exceptional" situation of how to recover from a possible standstill in the check-in process due to e-pollbook issues is critical. If poll workers do not know how to continue the voting process when e-pollbooks fail, there is a much greater likelihood that e-pollbook malfunctions lead to lengthy wait times, which could lead to some voters choosing not to vote. Accordingly, election officials **must** ensure that at least their leading poll workers are familiar and comfortable with all procedures for processing voters, including those for when the e-pollbooks unexpectedly become inoperable.

VII. Conclusion

As democracies increasingly confront autocratic efforts to undermine their democratic processes, it is essential that they do everything within their power to secure their election infrastructure, including their e-pollbooks. Electronic pollbooks can no longer remain an overlooked election cyber asset. Notwithstanding the many benefits and risks that must be balanced when choosing to deploy e-pollbooks, as well as the modest standards and regulation that currently govern their use, their popularity is growing. The global COVID-19 pandemic has created additional demands for new, more flexible voting methods (for example, more in-person early voting) in addition to traditional Election Day voting, and these newer approaches to voting rely heavily on the dynamic flexibility that e-pollbooks can provide.

Accordingly, enhancing the security of e-pollbooks is imperative. It is not necessary for bad-faith actors to change votes to undermine faith in elections; all that is required is to create chaos and doubt, and this paper illustrates how e-pollbooks are vulnerable to disruptions and data alterations that can serve this nefarious purpose. The bottom line: protecting the security and integrity of e-pollbooks is just as important as protecting the security and integrity of any piece of election infrastructure, including the voting machines that cast and count votes.[54]

[54] Unfortunately, e-pollbooks and voting machines share a noteworthy trait that imposes limitations on election officials' ability to bolster confidence in their use: both are based on proprietary "black box" software that resists public transparency. Publicly funded open-source election technology is an alternative approach that also merits consideration.

About the Authors

David Levine is the *Elections Integrity Fellow* at the **Alliance for Securing Democracy**, where he assesses vulnerabilities in electoral infrastructure, administration, and policies. David is also an advisory committee member for the Global Cyber Alliance's Cybersecurity Toolkit for Elections and an advisory council member for The Election Reformers Network, an organization dedicated to advancing nonpartisan reforms to address significant challenges in U.S. democracy. Previously, he worked as the Ada County, Idaho Elections Director, managing the administration of all federal, state, county, and local district elections. He received his JD from the Case Western School of Law, where he discovered his passion for election integrity, and he has observed elections overseas in several countries for the Organization for Security and Cooperation in Europe.

Edward ("**Eddie**") **Perez** is the *Global Director of Technology Development & Open Standards* at the **OSET Institute**. Eddie focuses on election administration, election technology, technology policy research, and government relations. Eddie is a veteran of the commercial election technology industry and formerly served as director of product management for one of the three major voting systems vendors in the U.S. He is also a media analyst on election systems and administration, including technology, security, and public policy issues, with regular contributions to NBC News, The Washington Post, The New York Times, The Associated Press, and POLITICO. He earned his Master's degree in Political Science from the University of California at Berkeley and his Bachelor's degree in Government from Georgetown University.

About the Organizations

alliance for securing democracy
G|M|F

The Alliance for Securing Democracy (ASD), a nonpartisan initiative housed at the German Marshall Fund of the United States, develops comprehensive strategies to deter, defend against, and raise the costs on autocratic efforts to undermine and interfere in democratic institutions. ASD has staff in Washington, D.C., and Brussels, bringing together experts on disinformation, malign finance, emerging technologies, elections integrity, economic coercion, and cybersecurity, as well as Russia, China, and the Middle East, to collaborate across traditional stovepipes and develop cross-cutting frameworks. ASD brings together a talented and diverse staff with expertise in government, foreign policy, politics, finance, media, and technology to provide quality research, policy recommendations, and analysis of the key issues and threats to our democracies.

OSET INSTITUTE

The Open Source Election Technology (**OSET**) **Institute** is a tax-exempt 501(c)(3) non-profit non-partisan election technology research, development, and education organization based in the Silicon Valley. A team of veteran technologists leads the Institute with extensive hardware, software, and systems design experience from well-known companies including Apple, Mozilla, Netscape, and Sun Microsystems. The Institute's mission is to make election technology more verifiable, accurate, secure, and transparent as a matter of national security in defense of democracy. The OSET Institute's TrustTheVote® Project is engaged in providing publicly available election administration technology to state and county governments. All work utilizes user-centered design principles and security-centric engineering practices and is based on open source principles to treat this critical government technology as an imperative public asset.