MUNICIPAL SECURITY ASSESSMENT REPORT

Risks and mitigations of voting technology use in Ontario's municipal elections

Prof. Nicole Goodman, Noah Nickel, Carlie Pagliacci, and Jared Boles

Brock University

James Brunet

Carleton University

Prof. Aleksander Essex

Western University

March 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report presents the findings of a security assessment of election technologies used in Ontario municipal elections. The study examines municipal practices related to electronic tabulators, online voting, and electronic poll books (e-poll books). Its objective is to identify security gaps and provide practical recommendations to strengthen the integrity, transparency, and resilience of Ontario's local elections.

Nine municipalities participated in the project through discovery sessions, surveys, and document sharing. Each municipality received an assessment tailored to up to three self-identified areas of need. Across the nine cities, common areas of focus included Logic and Accuracy (L&A) testing, authentication practices, system reliability, recruitment and training, and broader governance.

Key findings and recommendations are as follows:

1. Strengthen and Publicize Logic & Accuracy Testing

We recommend publishing detailed procedures allowing candidate observation, testing all ballot configurations (including overvotes and multi-member contests), and ensuring distinct vote totals during testing to detect configuration errors. While L&A testing is necessary, it is not sufficient to catch all failure modes (e.g., hacking). Municipalities should adopt Risk-Limiting Audits when legislative changes permit.

2. Improve Online Voting Authentication and Verifiability

Using date of birth as an authentication factor presents security and ballot secrecy risks. We recommend replacing it with stronger multi-step credentialing and improving the security of the voter information letters. Municipalities should also move toward end-to-end (E2E) verifiable online voting systems and seek independent technical evaluations of vendor claims. Standards from the Digital Governance Standards Institute (CAN/DGSI 111-1) should inform procurement and oversight.

3. Increase E-Poll Book Resilience

E-poll book outages have disrupted voting in past elections. We recommend that municipalities implement paper backups and manual training, deploy redundant Internet connections and hardware, and procure service guarantees from vendors to ensure continuity in the event of power or service failures.

4. Enhance Recruitment, Training, and Governance

Elections depend on well-trained staff. Regarding recruitment and training we recommend that municipalities conduct technical and situational screening, provide hands-on training, and offer competitive compensation. On governance, we recommend greater transparency, incident tracking, iterative technology adoption, and legislative updates to clarify rules for remote electronic voting and verification.

Note: *A full list of the recommendations is provided at the end of the report. While the above items capture some top recommendations, the full list is more detailed.*

NOTE TO THE READER

This report was compiled to summarize the results of Security Assessments conducted with nine Ontario municipalities. The purpose of these assessments was to help improve processes and procedures related to the use of election technologies in local elections and to mitigate the potential for technical issues. The research also identifies best practices in the areas of election worker recruitment and training, as well as election night reporting. It is our hope that the translating general, non-municipality-specific insights will benefit public and policy communities.

We would like to sincerely thank the nine municipalities for bravely taking part in this study. It is not easy to open your practices to scrutiny; however, each community did so with the shared aim of strengthening local election procedures and enhancing the integrity of their elections. This work would not have been possible without their commitment to safe and secure digital elections.

This research was supported by the Social Sciences and Humanities Research Council of Canada (Insight Development Grant #430-2022-01059) and Brock University.

All errors and omissions are our own.

HOW TO CITE THIS REPORT

Goodman, Nicole, Noah Nickel, Carlie Pagliacci, Jared Boles, James Brunet, and Aleksander Essex. 2026. *Municipal Security Assessment Report: Risks and Mitigations of Voting Technology Use in Ontario's Municipal Elections*. St. Catharines: Brock University.

1. INTRODUCTION

The use of technologies in municipal elections in Ontario has become widespread. Three popular technologies used in local races include e-poll books, electronic tabulators, and online voting.

The deployment of these election technologies has shown promise through increased voter participation, greater equity and inclusiveness in the voting process, shorter wait times, more efficient tabulation, and improved accessibility. On the other hand, their introduction has been accompanied by potential threats to security, voter fraud, and the possibility of compromised election outcomes.

The goal of this study is to identify ways to mitigate potential risks and issues in cyber elections. We accomplish this by examining election protocols and procedures in nine Ontario municipalities to identify risks and process gaps. We then suggest amendments or devise potential solutions to fill those gaps, making cyber elections in Ontario's municipalities safer.

1.1 Background

In 2023, Ontario municipalities received an email invitation to participate in a Social Sciences and Humanities Research Council of Canada funded research project hosted by a team of researchers at Brock and Western Universities. The goal of the project was to evaluate municipal processes for using election technology by providing post-election evaluations for tabulators, online voting, and e-poll books in up to three selected areas (e.g., Logic & Accuracy Testing). The specific areas assessed were chosen by each municipality according to where clerks identified the greatest need. Additional topics including election worker recruitment and training and election night reporting were added to the evaluations at the request of participating municipalities.

In total, nine municipalities across Ontario took part identifying the following areas of need:

Tabulators	Online Voting	E-Poll Books	Other
• Logic & Accuracy testing	• Logic & Accuracy testing • Authentication & DOB	• Gaps & Redundancies	• Election worker recruitment & training • Election night reporting

This report presents the aggregate results and best practices identified through this research. Specifically, it points to suggestions and recommendations to address current gaps in election technology implementation as well as other key areas of election administration. The report begins by providing historical context about the election technologies examined and definitions of them.

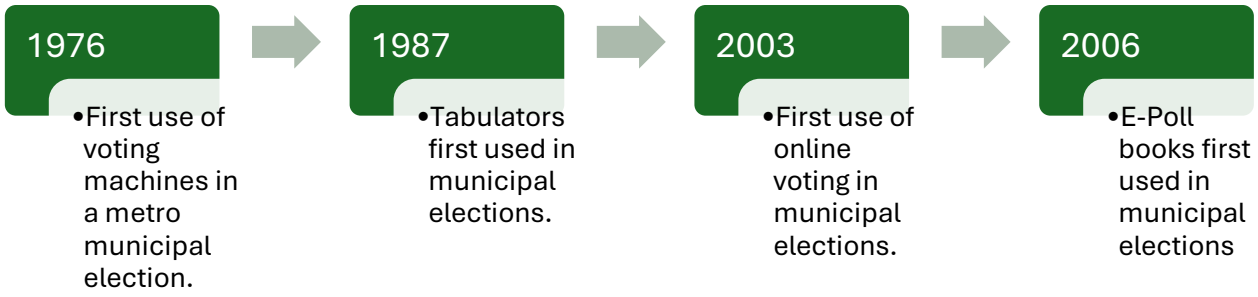
Note: *Cryptographic Secret-sharing Systems and Memory Card & Result Certification were also addressed but the analysis is not generic enough to include in this report.*

2. REPORT OVERVIEW

This report is intended to provide a concise overview of generic key findings to benefit public and policy communities. It is organized into the following sections: municipal history and context, definitions of key election technologies (e-poll books, tabulators, and online voting), approach and data, findings and recommendations for each technology area, and general recommendations at the municipal, provincial, and national levels in Canada.

3. MUNICIPAL HISTORY & CONTEXT

The use of election technology in Ontario municipalities has evolved over several decades. Voting machines were first used in the 1970s, electronic tabulators appeared in the late 1980s, and online voting was first deployed in 2003 by 12 municipalities.



3.1 Context: E-Poll Books

E-poll books were first used in Ontario municipal elections in the early 2000s.

Definition: An electronic device running a software application that manages the list of approved voters for a given electoral region. Polling staff use the poll book data to look up and validate the eligibility of individuals who come to vote.

Two Major Deployment Models

Standalone: When the e-poll books are not Internet/network connected. This means that voter revisions and registration cannot be done on election day, and location-specific voting is required.

Networked: When the e-poll books are Internet/network connected. This allows revisions and registration on election day and voting anywhere.

Benefits

E-poll books can improve the voter validation process, reduce manual errors in voter strike-off, speed up the voting process, and can be used to provide real-time voter turnout data to candidates.

Drawbacks

E-poll books can pose threats to election security and integrity, including through physical manipulation of the e-poll book, flaws in hardware and/or software configuration, supply chain issues, and vulnerabilities in Internet communication infrastructure.

Source: Canadian Centre for Cyber Security, 2022

3.2 Context: Tabulators

Tabulators were first used in Ontario municipal elections in the late 1980s.

Definition: A device that reads, interprets and counts votes on paper ballots by detecting marks made by voters in designated areas using digital image processing technology.

Benefits

Tabulators can increase the speed of tallying votes and releasing results, reduce the risk of human ballot-counting errors, and reduce the number of spoiled ballots due to over-, under-, or otherwise incorrect or unclear voting. The addition of tabulator audio, touch, and sip-and-puff mechanisms can enable electors with disabilities to cast a ballot.

Drawbacks

Tabulators can pose threats to election security and integrity, particularly if they are not functioning properly. Extensive logic and accuracy testing is required to ensure that all tabulators are operating as intended before deployment in an election.

Source: City of Windsor, 2023; Goodman, 2010; Digital Governance Standards Institute, 2023b; Walker et al., 2022.

3.3 Context: Online Voting

Online voting was first used in the 2003 Ontario local elections by twelve municipalities.

Definition: The process of casting a ballot via an Internet connection. It includes any and all systems in which obtaining the ballot, casting or counting ballots relies on an Internet connection.

Types of Online Voting

Uncontrolled Online Voting: A voter can cast their vote outside of an official voting location without election staff present or having verified their identity in person, and on their own device.

Controlled Online Voting: The voter must cast their ballot at an in-person voting location using a provided device, and their identity must be verified in person.

Benefits

Online voting can increase convenience and accessibility, enhance voter privacy, increase turnout, reduce spoiled ballots, improve tabulation and result release, and lead to long-term reductions in administrative costs.

Drawbacks

Online voting can disenfranchise digitally illiterate voters if no other channels are offered and can raise issues of ballot secrecy, coercion, fraud, and vote buying. Likewise, online voting can reduce the capacity to authenticate and may lack publicly auditable results. Finally, the voting mode can introduce numerous security and integrity concerns.

Source: Goodman, 2017; Goodman et al., 2024; Cardillo et al., 2019; Klassen at al., 2025.

4. APPROACH & DATA

4.1 Approach

The project took a community-based approach to the research that positioned municipalities as active partners throughout the project. Our approach emphasized collaboration, shared decision-making, and mutual learning. Municipal clerks and staff helped shape the assessment focus areas, identified local priorities, and provided contextual knowledge that was important for both the assessments and the interpretation of findings. Engaging municipalities in project design, data collection, and the discussion of results helped to ensure that the research is reflective of local needs, context, and administrative expertise and supports findings that can have direct, actionable benefits for municipalities. This collaborative approach to research helps build trust, strengthens the relevance of study recommendations, and supports capacity-building for future election planning and technology use.

4.2 Data Collection

Municipal clerks across the province of Ontario were invited to take part in the study via email. Emails were sent to individuals designated as the clerk or deputy clerk (one per municipality) based on a list obtained from the Association of Municipal Clerks and Treasurers of Ontario. Ideal municipal partners were those focused on improving election processes and security, or those who did not have the resources or capacity to facilitate their own system review and could thus benefit from a no-cost custom evaluation. While the initial plan was to work with six to eight cities, nine municipalities were a good fit for the research and agreed to take part. Each participating municipality received an individually curated report based on up to three identified areas of need. Generally, evaluations were based upon a combination of technological reviews (e.g., system tests, verification, authentication, etc.) and process reviews (e.g., Logic & Accuracy testing, and other procedures).

Three phases of data collection informed the project. In the first phase, each municipality participated in a 90-minute Discovery Session to discuss the election technologies or election aspect(s) along four key themes: (1) their municipal experience, (2) concerns and gaps related to election technology implementation, (3) internal and external accountability measures, and (4) opportunities for guidance and solutions to promote safe digital elections in the municipal sector. At the end of the session, municipalities were asked to identify their areas of need. Eight municipalities chose three areas of need, while one community selected two topics.

In the second phase of data collection, municipalities were asked to provide relevant documents and information related to their processes and procedures for deploying election technologies. Obtaining this information was essential since knowing what was being done allowed us to identify gaps and areas for improvement.

Finally, to obtain more granular data regarding specific protocols and procedures, in the third phase of data collection municipalities took part in a short 10-minute survey. Questions focused on specifics relating to processes and testing of election technologies and were not opinion-based. Follow-ups were conducted as needed to verify information or clarify questions.

Once complete, the research team drew upon the Discovery Session and any follow-ups, document provision, and survey responses to identify gaps and suggest modifications to address them. The substance of these high-level findings is outlined in the remainder of this report.

The project was approved by Brock University's Research Ethics Board, and a Research and Access Agreement was signed between each municipality and Brock University.

5. LOGIC & ACCURACY TESTING FOR TABULATORS

5.1 What is Logic & Accuracy Testing (L&A)?

Before an official election is held, a mock election is run with the equipment a municipality intends to use. This mock election allows for the testing of a variety of ballots to be cast in this mock election to test if the tabulators are functioning correctly. Common checks include:

- Testing overvoted ballots to confirm that the tabulator correctly rejects them when they have too many selections.
- Testing undervoted ballots to verify that the tabulator accepts ballots with fewer than the maximum selections.
- Casting valid votes for each candidate to ensure the tabulator accurately records and tallies every selection.

5.2 Why is L&A Important?

L&A testing is an essential exercise for detecting a variety of common tabulator failure modes. Specifically, L&A testing can:

- Reveal tabulators that are broken or otherwise non-functional before they are deployed on election day.
- Detect misconfigured election definitions in which ballot data has been incorrectly loaded onto the tabulator.
- Uncover configuration errors and discrepancies with the Election Management System (EMS) software used to consolidate and report results.
- Identify incorrectly set overvote thresholds, which can cause a tabulator to accept or reject an incorrect number of selections.

LA testing is an important exercise for demonstrating intended behaviour and outcomes. It also helps to build public confidence in election technology.

Note: *L&A cannot reliably protect against malicious modification of the tabulator software (hacking).*

5.3 Overview of L&A Practices for Tabulators

We recommend adhering to the following best practices for tabulators and ensuring that processes meet as many of these guidelines as possible:

- L&A procedures should be made available to the public through a document posted on the municipal website.

- L&A procedures should permit candidates and their appointed representatives to be present to scrutinize the testing process.
- All tabulators, including reserve units, should be tested to ensure that every device intended for election use functions correctly.
- Overvoted ballots should be tested to confirm that the tabulator properly rejects overvoted ballots.
- Overvote testing should be performed especially for multi-member contests, where the allowed number of selections varies (e.g., allowing up to *three* choices).
- Memory cards should be loaded into the Election Management System (EMS) during testing to verify that the results aggregation process functions as expected.
- Unpredictable testing should be included, using randomly marked ballots to detect unintentional or intentional misconfigurations in the ballot definition file.
- All candidates should receive at least one valid vote during testing to confirm that each option is recorded correctly.
- No two candidates should receive the same number of votes during testing to detect configurations that may swap results between candidates.

5.4 Recommendations

LT.1 Make L&A procedures publicly available

We recommend that detailed L&A procedures are made available in a publicly accessible document on the municipal website.

Making such procedures publicly available is identified as a best practice to improve transparency of the electoral process. It allows interested individuals, experts, and advocacy groups to review and potentially suggest improvements. It can also help build trust and confidence among select members of the electorate.

LT.2 Make L&A process open to scrutineers

We recommend that L&A testing dates are announced to candidates well in advance and that candidates and their representatives are invited to observe the testing.

Making such procedures publicly accessible is a best practice to improve transparency of the electoral process. It plays an important role in cultivating trust and confidence among candidates.

LT.3 Test for overvotes, including in multi-member contests

We recommend overvote testing. We also recommend that the test deck for each contest include one ballot with the maximum allowable number of selections and a second ballot with selections exceeding the maximum allowable. For example, in a regional councillor vote where voters are expected to choose up to 3 of 6 candidates, a test deck should include a ballot with 3 selections and a ballot with 4 selections.

Following this process enables election administrators to detect misconfigurations where the overvote threshold for a multi-member contest is set incorrectly.

LT.4 Load tabulator memory cards into Election Management System (EMS)

If election night procedures include loading memory cards into an election management system, which consolidates the result from multiple tabulators, we recommend testing this stage during your municipality's L&A testing process.

Loading tabulator memory cards into the EMS as part of L&A testing can identify issues with the EMS in advance of election day. It can also identify scenarios where election definitions are configured incorrectly.

LT.5 Add unpredictable testing

We recommend that officials mark some ballots with a source of randomness as part of testing (this could include a coin toss, dice roll, etc.) In addition, we recommend that some public observers be allowed to arbitrarily mark and cast ballots. Adopting these recommendations helps administrators detect cases where a person has unintentionally or intentionally misconfigured a tabulator in a way that regular procedures may not detect.

LT.6 Test deck with all candidates receiving at least one valid vote

We recommend that all possible ballot choices receive at least one valid vote during testing.

LT.7 Test deck with no two candidates receiving the same vote total

We recommend that no two choices on a ballot receive the same number of votes. Enacting this recommendation helps election administrators to detect misconfigurations in the election definition tabulator that would 'swap' the results for two candidates. Undertaking this practice promotes result accuracy and election integrity.

6. LOGIC & ACCURACY TESTING FOR ONLINE VOTING

6.1 What is L&A Testing for Online Voting?

Before an election, a mock election is held using the municipality's online voting system. This requires the creation of test voters and voting PINs, which are used to cast a variety of ballots in the mock election to test if the system is working correctly, including ensuring that:

- Overvoted ballots are tested to verify that the online voting system correctly prevents voters from selecting more candidates than allowed.
- Undervoted ballots are tested to confirm that the system properly accepts ballots with fewer than the maximum selections.
- Valid votes for different candidates are cast to ensure the online voting system accurately records and tallies each selection.

Why is L&A Testing for Online Voting Important?

L&A testing is an essential exercise for detecting a variety of common online voting failures. Specifically, it helps to:

- Identify misconfigured online elections, where ballot options or contest settings have been set up incorrectly.
- Detect incorrectly set overvote thresholds that allow voters to select too many or too few candidates.
- Reveal missing candidates from the ballot, which can necessitate a costly new election if not caught in advance.

Note: *L&A cannot protect against malicious modification of the online voting system.*

6.2 Overview of L&A Best Practices for Online Voting

We recommend adhering to the following best practices for testing online voting systems and ensuring processes meet all, or as many of these standards as possible:

- Formal L&A procedures should be documented to encourage consistency and enable periodic review.
- L&A procedures for online voting should be made publicly available on the municipal website to improve transparency.
- The L&A process for online voting should allow candidates and their representatives to scrutinize the test.

- All possible ballot configurations should be tested, including undervotes, overvotes, and declined ballots for each contest. Because online voting is digital (unlike the manual process of marking paper ballots), comprehensive test suites can be efficiently automated.
- The overvote threshold for multi-member contests should be verified by casting ballots for at least the maximum allowed selections.
- A process should be in place to ensure that all eligible candidates appear on the ballot, with testing conducted *after* the final registration deadline.
- Testing should confirm that multiple voting is prevented, ensuring that the same credentials cannot be used to cast more than one ballot (unless specifically allowed as part of a coercion mitigation strategy, such as in Estonia).
- An administrator should attempt to log in with the oldest and youngest possible voter ages to verify that age-based eligibility restrictions function correctly.
- The election administrator's web portal should be tested thoroughly, including opening and closing the mock election, generating reports, and tabulating votes.

6.3 Recommendations

LO.1 State L&A procedures in a document

Maintaining formal online voting L&A procedures in a document promotes consistency of procedures across elections and allows for periodic review and updating.

LO.2 Make L&A procedures publicly available

We recommend that online voting L&A procedures are made available in a publicly accessible document on the municipal website.

Making such procedures publicly available is a best practice to improve transparency of the election process. It allows interested individuals, experts, and advocacy groups to review and potentially suggest improvements. It can also support trust and confidence among electors.

LO.3 Make L&A testing open to scrutineers

We recommend that online voting L&A testing dates are announced to candidates well in advance and that candidates and their representatives are invited to observe the testing.

Making such procedures publicly accessible is identified as a best practice to improve transparency of the electoral process. It can also foster trust and confidence among candidates.

LO.4 Test all possible ballots

Online voting L&A procedures should test undervotes for each contest, overvotes for each contest, and declined ballots. This helps to verify that the voting system is working as expected.

LO.5 Test overvotes in multi-member contests

For each contest, we recommend that a vote is cast with the maximum allowable number of selections and a second ballot with one extra selection.

For example, for a Regional Councillor vote where voters are expected to choose up to 3 of 6 candidates, a ballot with 3 selections and a ballot with 4 selections should be tested.

Following this process will enable election administrators to detect misconfigurations where the overvote threshold for a multi-member contest is set incorrectly.

LO.6 Ensuring that all candidates are on the ballot

It is critical that online voting L&A testing occurs after the last day to withdraw from or register for the election. L&A testing should include checking each ballot face to ensure all eligible candidates are present.

This is a crucial step – not having this as a formal procedure can lead to missing candidate names on the ballot, which could require a new election.

LO.7 Testing login with oldest/youngest possible voter ages

We recommend that during online voting L&A testing, Test Voters are created with a variety of birth dates, including the youngest age eligible to vote, the oldest possible age of a voter, and the oldest ineligible voter (e.g., someone who is 17).

It should be verified that ineligible voters are prevented from voting and that eligible voters are able to cast their ballots.

This is important to verify that the restrictions put in place by the online voting systems are correct. During our Discovery Sessions, one municipal official noted that an elderly voter was prevented from voting because their age was considered “invalid” by the online voting system (the vendor had arbitrarily implemented a maximum valid age).

LO.8 Ensure multiple voting is prevented

We recommend that election administrators test whether a vote can be cast with the same Test Voter's credentials multiple times to prevent the possibility of multiple votes.

This helps to verify that the voting system is working as expected. It also allows administrators to see whether voters receive a clear error message informing them of next steps. This is helpful in cases where a vote is cast on behalf of a voter without their consent.

LO.9 Test the administrative site

We recommend testing the administrative site for the online voting system thoroughly. This includes opening and closing the mock election, creating, and running reports, and tabulating the votes to verify that the mock election count is correct.

Conducting these tests can help administrators verify that the voting system is working as expected.

7. AUTHENTICATION & DATE OF BIRTH

7.1 Analysis

Date of birth is a popular login authenticator used by municipalities in Ontario. Its use, however, poses several risks:

1. **Re-identification:** In smaller municipalities, a date of birth can be unique to a voter. Our research shows that this can allow an online voting system to re-identify a voter with their vote, which can be a threat to ballot secrecy.
2. **Lack of secrecy:** Dates of birth are known to voters' household members and are not considered secret by all levels of government. For example, the Ontario COVID-19 vaccine passport QR code included the names and dates of birth of Ontario residents.
3. **Year of birth is easy to guess:** In the 2022 Ontario municipal election, one online voting vendor used year of birth as an authentication factor. Given enough attempts, it is plausible to simply guess a voter's year of birth.

7.2 Recommendations

AD.1 Replace date of birth as a credential

Using a date of birth as a credential provides minimal protection to voters and creates a ballot secrecy risk.

One possible improvement is to implement a 2-step voting process where voters first register to receive a ballot and then receive credentials to vote via email. With this approach, a voter's access to their email address is used as part of authentication.

This mitigates some risks compared to relying upon date of birth for authentication, however, it is important to ensure that the registration step does not allow for easy impersonation.

AD.2 Work toward a national or provincial digital identity card

One solution to this issue is a national or provincial digital identity card. Canadians could use this card to access government services and e-voting, similar to Estonia's system.

This can greatly reduce authentication risks that exist in Ontario's local elections. However, we recognize introducing digital identity card could introduce cyber, privacy, data, and political problems of its own.

7.3 Voter Information Letter

We recommend that document security considerations be taken for Voter Information Letters (VIL). Specifically, credentials on the VIL should not be readable through envelopes. Our research found that some municipalities did not take these precautions.

We also recommend that the VIL clearly explain how to connect securely to the online voting system. In particular, the VIL should direct voters to type “https://” before entering the voting portal URL. Not doing so could make voters vulnerable to network-based attacks.

Once a voter has connected to the voting website, they should be directed by the VIL to check their browser URL bar to ensure they are connected to the online voting portal (e.g., https://elections.municipalnamevotes.ca).

8. E-POLL BOOK GAPS & REDUNDANCIES

8.1 Best Practices for E-Poll Books

We recommend adhering to the following best practices for e-poll book use:

- E-poll books should be resilient to power outages, using devices with working batteries or uninterruptible power supplies.
- E-poll books should be resilient to service outages and tested to ensure functionality is maintained even when the central service is temporarily unavailable.
- A paper alternative to e-poll books should exist at each polling location to ensure voting can continue during outages.
- Staff should be trained on the paper alternative so they can seamlessly switch to manual processes if the digital system fails.
- A backup Internet connection should be available at every voting location to ensure redundancy if the primary connection fails.
- Diversification of backup Internet providers should exist, ensuring that primary and backup connections use different service providers and connection types.
- Redundant e-poll book hardware should be available at each voting location to ensure voting can proceed in the event of device failure.
- The software installed on the e-poll book should be verified by the municipality to ensure it has not been tampered with or misconfigured.

8.2 Recommendations

EP.1 Ensure a backup to e-poll books is made available

We recommend that a backup to e-poll books, such as a paper option, be available at polling locations in the event of a service outage. In the 2022 Ontario municipal elections some municipalities were forced to turn away voters because of e-poll book service outages.

Enacting this recommendation will allow staff to ensure that voting continues even in cases of outages to power, the Internet, or the e-poll book service.

EP.2 Ensure staff at each voting location are trained on a paper alternative

Staff must be prepared to strike-off voters on paper, process changes of registration on paper, and, in some elections, provide candidates and their representatives with paper copies of strike-off lists.

Enacting this recommendation can reduce risks from untrained staff quickly switching from a digital e-poll book system to a paper strike-off system.

EP.3 Provide backup Internet connections and diversification of providers

We recommend that voting locations have both primary and backup Internet connections. Optimally, a backup Internet connection should have a different connection type than the primary Internet connection (e.g., if the primary Internet connection is fiber, the backup could be DSL or 5G), and have a different Internet Service Provider (ISP).

Redundant Internet can allow voting to proceed in case of outages. Requiring multiple connection types protects against outages inherent to that connection type (e.g., a lawnmower running over a cable outside the voting location). Likewise, requiring multiple Internet Service Providers protects against ISP-specific outages (e.g., the 2022 Rogers Communications outage).

EP.4 Make redundant e-poll book hardware available

We recommend that redundant e-poll book hardware be available at all voting locations. This may simply involve having additional laptops on hand that are pre-configured with the e-poll book software.

Redundant e-poll book hardware can allow voting to proceed in cases of hardware failure.

EP.5 Ensure e-poll book service is resilient to power outages

We recommend that e-poll book hardware be resilient to power outages. This is achievable by using laptops with working batteries or using uninterruptible power supply (UPS) products.

It is also important to ensure that network equipment can continue to function during a power outage. Having a redundant Internet connection through a battery-powered mobile hotspot is one strategy.

The use of hardware and networking equipment that is resilient to power outages can allow voting to proceed for some time during a power outage, giving staff time to plan alternatives before batteries run out.

EP.6 Ensure e-poll book services are resilient to service outages

We recommend that the e-poll book service be resilient to service outages (e.g., if an outage occurs with VoterView).

We assess the risk of e-poll book outages to be high given the occurrence of numerous outages in past elections and by-elections and outages.

We recommend that cities use an e-poll book system that is resilient to service outages to ensure that, in the event of an outage, voter registrations can still be updated and voters can still be struck off. When service is restored, changes in voter status should be automatically communicated to the e-poll book service, which can highlight any discrepancies (e.g., where a voter voted twice in their ward during the outage).

EP.7 Obtain availability guarantees from e-poll book providers

We recommend that municipalities ensure that the e-poll book service provider offers a high availability guarantee in their service agreement. A common availability guarantee is 99.999% uptime (or less than 1 second of downtime per 24-hour period).

Availability guarantees are a common indemnification in the IT industry and provide recourse to municipalities if availability issues occur.

8.3 DGSI Online Voting Standard

The Digital Governance Standard Institute published a voluntary standard for online voting systems (**CAN/DGSI 111-1**) in December 2024.

We recommend that municipalities consult the standard when drafting their RFPs. This recommendation is echoed in the broader recommendations at the end of this report.

8.4 Drafting with Other Municipalities

Some municipalities that participated in this study drafted joint RFPs with neighbouring communities or shared information through Election Working Groups. Co-writing RFPs allows municipalities to develop more robust RFP requirements in consultation with domain experts.

We recommend that municipalities leverage horizontal collaboration and explore partnering with other local governments to jointly draft RFPs for online voting systems.

9. ELECTION WORKER RECRUITMENT & TRAINING

9.1 Promotion

Social media is considered a best practice for promoting job opportunities and recruiting election workers. It may be particularly effective at reaching younger demographics, who are often more technologically savvy. However, platform usage patterns often differ across demographic groups, including by age and race and ethnicity.

For example, Facebook is more popular among older demographics. As a result, it may attract older users and not reach younger ones. Additionally, research finds that LinkedIn is most commonly used by white males between the ages of 30 and 49. Similarly, Facebook is most commonly used by black females ages 30 to 49, and Instagram most commonly used by Hispanic females ages 18 to 29 (Pew Research, 2021). Thus, when advertising, municipalities should be mindful of variation in social media use across platforms.

We recommend using multiple social media platforms to reach different demographics.

Promoting job opportunities through local universities and colleges (if possible) can encourage student engagement. This may include in-person job promotions, posters, emails, or announcements about the upcoming election.

Election recruitment can often be made more obvious on municipal websites during the recruitment period. For example, some municipal websites have a job board that is not easily accessible to those who are unfamiliar with the site. We recommend posting the job openings on the website homepage to ensure easier access.

9.2 What to Look for When Recruiting

We recommend assessing the following skills and qualities during recruitment for election workers:

- Strong literacy skills, as election work involves reading and interpreting detailed procedures and documentation.
- Strong interpersonal skills to promote professional interactions with voters and resolution of any issues at the polls.
- Patience, as election workers may encounter long lines, confused voters, and repetitive questions throughout the day.
- The ability to perform repetitive tasks since much election work involves consistent, methodical actions over a prolonged period.
- Analytical skills to identify irregularities, troubleshoot issues, and ensure accuracy in ballot handling and voter validation.

- Attention to detail to ensure correct processing of voter information, management of ballots, and following precise procedures.
- The ability to follow directions to promote adherence to established protocols and maintain the integrity of the election process.
- The ability to work long days since election days typically requires staff to be present from early morning through late evening.
- Technological literacy, measured by familiarity, experience, and willingness to navigate digital tools if technology is being used in the election process.
- The ability to learn quickly and adapt to new systems, procedures, and unexpected situations that may arise on election day.

To assess certain skills, **asking potential employees situational questions can help recruiters determine which role a candidate is best suited for or whether they are compatible with election-related roles**.

For example, recruiters may wish to try a role-playing scenario in which they act as an irate voter experiencing difficulties at the polls. This can enable the recruiter to assess how the candidate performs under pressure and how they apply their problem-solving and interpersonal skills to the role.

A technical test is also recommended to assess a candidate's familiarity and comfort with technology. Including this kind of assessment highlights the importance of workers being comfortable in their roles.

9.3 Tips for Training

Training must involve instruction regarding typical manual election procedures and expectations, and training on the types of technologies being used (e.g., e-poll books, tabulators).
Hands-on training which includes employees learning how to use the technologies in real-time may help mitigate confusion on election day.
Providing staff with a "cheat sheet" that outlines commonly identified issues can help to defuse incidents (e.g., "Is the tabulator plugged in?")
Conducting several test-runs for each employee and the technologies they will be using at the polls can help employees feel more comfortable in their roles (practice makes perfect).
Offering additional training and practice time for those who need it. This may look like an additional training session for those who report lower digital literacy skills.

Consider conducting training in smaller groups based on responsibilities (e.g., DROs as a group), as some employees will have more complex and specific responsibilities than others.
Having documented processes and procedures related to training promotes consistency and reliability of the training. Making these publicly available, as echoed elsewhere in the report, is also suggested.

9.4 Compensation

Compensation is an important incentive for recruiting and retaining temporary election staff.

We recommend that compensation be generous and competitive.

We include some examples of compensation and a compensation range based on a review of municipal compensation:

If financially feasible, **we recommend that municipalities offer compensation at the upper end of the range to recruit and retain staff.**

9.5 Recruitment & Training Takeaways

We recommend adhering to the following best practices for the recruitment and training of election staff:

- Use a variety of social media platforms to target desired demographics, such as Facebook to reach older populations and Instagram to engage younger audiences.
- Advertise job openings prominently on municipal websites, such as featuring them on the homepage during the recruitment period.
- Conduct technical and situational testing during the recruitment period to assess each candidate's compatibility with the specific roles they may fill.
- Compensate generously and competitively to attract qualified applicants and retain experienced election staff across election cycles.

10. BROADER RECOMMENDATIONS

10.1 Recommendations: General

RG.1 Enhance transparency of policies and procedures

We encourage municipalities (and all EMBs using election technologies in Canada) to enhance transparency of the policies, procedures, and protections related to election technologies. This includes publicly posting documentation regarding L&A processes for online voting and tabulators and/or security assessments such as online voting penetration testing on the government website. For e-poll books it may look like posting administrative guidelines for use.

Likewise, we recommend publicly disclosing election post-mortems and reports.

RG.2 Review current procedures against provincial standards

If relevant, we recommend reviewing current procedures against provincial standards. Conducting a top-to-bottom review of any tabulator and e-poll book procedures (testing, setup, operation, closing) against the Canadian Digital Governance Standards Institute Standards for Vote Tabulators (CAN DGSI 119-1) and Electronic Poll Books (DGSI 119-2).

If relevant, we recommend reviewing the Canadian Digital Governance Standards Institute Standard for Online Voting (CAN DGSI 111-1).

RG.3 Establish cyber incident response plans

Since municipalities typically rely on third-party vendors for the use of technologies in the election process, cybersecurity incident response planning must account for the division of responsibilities between the municipality and its vendors.

Municipalities should ensure that contracts clearly specify the vendor's responsibilities for detecting, reporting, and mitigating cybersecurity incidents. At the same time, municipalities need their own parallel response plans detailing extending voting hours, communicating with the public and candidates, and escalating to provincial or federal agencies like the Canadian Centre for Cyber Security, if needed. The plan should establish clear points of contact and define how coordination between the municipality and vendor will function during the election period. Contracts should require that the municipality receive detailed findings from any post-incident reviews conducted by the vendor.

RG.4 Work toward establishing a centralized incident tracking body

To date a number of incidents have occurred across a range of election technologies in Canada, yet records of such events are difficult to find or are often without detail. We recommend that a central association or body keep a record of such incidents to track any gaps that exist across election technologies. This could be an association such as the Association of Municipal Managers, Clerks and Treasurers of Ontario (AMCTO), the Association of Municipalities of Ontario (AMO), or an ongoing research project

RG.5 Improve vendor vetting and procurement

Municipalities should establish rigorous vetting processes to evaluate a vendor's security practices, organizational stability, and track record across other jurisdictions. Contracts should include provisions for independent third-party security audits of vendor systems, and vulnerability disclosure policies that obligate the vendor to promptly report any security issues discovered before, during, or after an election. Municipalities should also seek transparency into the vendor's supply chain, including subcontractors, cloud hosting providers, and third-party software components.

RG.6 Take an iterative approach to technology adoption

We recommend taking an iterative approach to the adoption of election technologies. This means taking slow, small steps to implementation. Trialing technologies in pilots such as by-elections, in a particular ward, or in advanced polls is considered a best practice.

10.2 Recommendations: Tabulators

RT.1 Conduct Risk-Limiting Audits

When and if legislation permits, we recommend conducting Risk-Limiting Audits (RLAs). RLAs are the gold standard for verifying election results counted by automated tabulators. They can identify issues beyond what is detected by Logic & Accuracy testing such as when tabulator software has been compromised.

The RLA process involves undertaking a manual hand count of randomly selected ballots after the election is over. Georgia, Virginia, California, and other U.S. states regularly conduct RLAs.

Our understanding is that changes to the Municipal Elections Act (MEA) would be required for municipalities to conduct an RLA. We strongly recommend this practice in addition to L&A testing when and if it becomes a possibility.

10.3 Recommendations: Online Voting

RO.1 Move towards verifiable systems

While verifiability is a desirable quality of an online voting system, not all verifiability is equal. Individual verifiability (which allows voters to confirm that their ballots are cast as intended) adds a dimension of verification but does not ensure that the election result is correct.

Universal or end-to-end verifiability (E2E) (which allows voters and administrators to ensure that all ballots are counted as cast) is needed to verify the accuracy of the count. This latter type of verifiability is considered the gold standard, and we encourage municipalities to work towards this.

We recommend that all municipalities deploying or considering implementing, online voting move towards using verifiable systems whose outcomes are supported by evidence. For some municipalities this may look like implementing a cryptographic E2E verifiable system in the next election, however, for others it may first involve a trial of individual verifiability to move in that direction.

Technological claims around verifiability can be difficult for municipalities to internally assess. We recommend having an external independent party with specific knowledge of online voting evaluate vendor claims. If cost is an issue, this assessment could be undertaken as a group (for example, prospective municipalities could meet as part of a working group).

RO.2 Facilitate public demo/practice voting and set clear rules

We recommend ensuring that stakeholders (candidates and the public) can practice voting in the online system as part of a public demonstration or on a website prior to the election.

We recommend ensuring that each municipality has clear rules about the parameters of the online vote. This includes rules regarding which ballots are accepted, the criteria under which a new ballot could be issued, and the process for managing a dispute.

RO.3 Review recount and scrutineering procedures for adherence with MEA principles

Municipalities should carefully examine how (or whether) their recount and scrutineering procedures provide meaningful assurances consistent with the MEA ‘certainty’ principle. For example, do vendor-mediated digital recounts re-running the same software on the same data provide scrutineers with similar assurances compared to recounting physical paper ballots?

Municipalities should review whether their current frameworks for recounts and scrutineering, which were intended for paper ballots, are adequate for digital elections, and whether the

absence of an independent, human-auditable record constitutes a due-process concern for candidates challenging close results.

RO.4 Review ballot secrecy guarantees for adherence with MEA principles

We recommend that municipalities more precisely explore how ballot secrecy should be defined under the MEA, and whether the vendor's system meets this standard. Municipalities should assess whether the vendor has the technological capability to directly or indirectly recover voter identities and their associated ballot selections given their privileged access to the system's code, logs and data.

10.4 Recommendations: Election Recruitment

RR.1 Improve recruitment and compensation

Some municipalities have experienced difficulties recruiting and retaining election staff who can support the use of technologies in elections. We recommend increasing compensation where possible to better attract talent and undertaking technical and situational screening of candidates prior to hiring.

In terms of recruitment of election staff, different platforms, and modes of communication appeal to different demographic groups. Municipalities should keep this in mind when beginning recruitment efforts.

We recommend having job postings stand out (through placement, graphics, etc.) on municipal websites during the recruitment period.

10.5 Recommendations: Provincial

RP.1 Amend the Municipal Elections Act

We recommend changes to the MEA and corresponding municipal by-laws to include rules for unsupervised voting (e.g., online and telephone voting). This could include procedures for determining the validity of a remote electronic vote, parameters for conducting remote electronic voting, and destroying data.

In future, the province could consider requiring compliance with online voting standards by including it in legislation or regulations.

We further recommend the amendment of legislation to clarify the role of observers in the use of all election technologies, including those used for voting and supporting the election (e.g., e-poll books).

Finally, we recommend that municipalities work with the province to implement a common (joint) system for voter registration. Voters would be better served by a joint municipal and provincial online portal to update their registration information. In many instances, it would improve security posture and lower cyber/privacy risk for a single provincial-level body to administer a common IT infrastructure for voter-facing data intake. This may make intuitive sense now that the province has taken over municipal voters' lists.

10.6 Recommendations: National

RN.1 Establish national coordination on election technologies

We recommend national-level involvement to coordinate and facilitate thought leadership and knowledge sharing on the topic of election technologies. Ideally this would take the form of an independent national agency the sets requirements, certification and testing programs for voting technology. However, in the interim, this might be undertaken by an existing agency (such as Democratic Institutions) as part of the government's broader initiative to tackle foreign interference.

11. CONCLUSION

Election technologies offer substantial benefits in accessibility, efficiency, and voter experience. However, they introduce important democratic, operational, and cybersecurity risks that require explicit technologies, actions, and processes to mitigate effectively.

The central conclusion of this report is that technological adoption in elections must be accompanied by technological, procedural and legislative provisions. These include:

- Transparent and rigorous testing to verify that all election technologies function as intended before deployment.
- Strong authentication and verifiability mechanisms to protect ballot secrecy and confirm the accuracy of election results.
- Operational resiliency planning to ensure continuity of voting in the event of power, service, or hardware failures.
- Well-trained personnel to operate election technologies effectively and respond to issues as they arise.
- Clear legislative authority and oversight to define the rules and accountability structures governing the use of election technologies.
- Inter-municipal, provincial, and national coordination to share best practices, track incidents, and build consistent standards and guidelines across jurisdictions.

By adopting the recommendations outlined in this report, Ontario municipalities can meaningfully improve the security posture, reliability, and public trust of technology-enabled elections while preserving the accessibility gains these systems provide.

REFERENCES

Canadian Centre for Cyber Security. (2022). *Security Considerations for electronic poll book systems* (ITSM.10.101). https://www.cyber.gc.ca/sites/default/files/cyber/2022-03/itsm10101-security-considerations-electronic-pollbooks-e.pdf

Cardillo, A., Akinyokun, N., & Essex, A. (2019). Online voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology?. In Krimmer, R., Volkamer, M., Cortier, V., Beckert, B., Küsters, R., Serdült, U., & Duenas-Cid, D. (eds) Electronic Voting. E-Vote-ID 2019. Lecture Notes in Computer Science, vol 11759. Springer, Cham. https://doi.org/10.1007/978-3-030-30625-0_5

City of Windsor. (n.d.). *Vote Tabulator*. https://www.citywindsor.ca/city-hall/municipal-election/voter-info/vote-tabulator

Digital Governance Standards Institute. (2023a). Election and Voting Technologies – Part 2: Electronic Poll Books (CAN/DGSI 119-2). https://dgc-cgn.org/product/dgsi-119-2/

Digital Governance Standards Institute. (2023b). Election and Voting Technologies – Part 1: Vote Tabulators (DGSI 119-1). https://dgc-cgn.org/product/dgsi-119-1/

Digital Governance Standards Institute. (2024). Online Voting – Part 1: Implementation of Online Voting in Canadian Elections (CAN/DGSI 111-1). https://dgc-cgn.org/product/can-dgsi-111-1/

Goodman, N., Hayes, H. A., McGregor, R. M., Pruysers, S., & Spicer, Z. (2024). *Voting Online: Technology and Democracy in Municipal Elections*. McGill-Queen's Press-MQUP.

Goodman, N. (2017). *Online Voting: A Path Forward for Federal Elections*. Privy Council Office. https://www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html

Goodman, N. (2010). *A Comparative Assessment of Electronic Voting*. Elections Canada. https://carleton.ca/canadaeurope/wp-content/uploads/AComparativeAssessmentofInternetVotingFINALFeb19-a-1.pdf

Klassen, E., Brunet, J., Goodman, N., Essex, A. (2026). *Credential Attacks in Ontario's Online Elections*. In Duenas-Cid, D., Roenne, P., Volkamer, M., Blom, M., Gaudry, P., Borucki, I., Loeber, L., & Debant, A. Electronic Voting. E-Vote-ID 2025. Lecture Notes in Computer Science, vol 16028. Springer, Cham. https://doi.org/10.1007/978-3-032-05036-6_9

Walker, J., Bajaj, N., Crimmins, B. L., & Halderman, J. A. J. (2022). *Logic and accuracy testing: A fifty-state review*. In Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) Electronic Voting. E-Vote-ID 2022. Lecture Notes in Computer Science, vol 13553. Springer, Cham. https://doi.org/10.1007/978-3-031-15911-4_10

AUTHOR INFORMATION

Prof. Nicole Goodman is an associate professor at **Brock University**. She is recognized internationally as a leading expert on electoral modernization.

Noah Nickel received both his B.A. in Political Science and M.A. in Canadian Politics from **Brock University,** where he studied municipal elections and electronic voting under the supervision of Dr. Nicole Goodman. He now works for an Ontario municipality in council and committee services.

Carlie Pagliacci graduated from **Brock University** with a Master of Arts in Political Science. Her research focused on democracy in the Middle East and North Africa. She currently works as a Museum Exhibit Designer.

Jared Boles is a Political Science graduate student at **Brock University**. Studying under the supervision of Dr. Nicole Goodman, Jared's research focuses on elections accessibility.

James Brunet is a lecturer (teaching stream) in the School of Information Technology at **Carleton University**. As part of his academic research, he has discovered several security vulnerabilities in Canadian online voting providers and performed a standards-based review of the use of online voting in Ontario.

Prof. Aleksander Essex is an associate professor of software engineering at **Western University** with a specialization in cybersecurity and applied cryptography. He runs Whisper Lab, the Western Information Security and Privacy Research Laboratory.