ALTERNATIVE VOTING TECHNOLOGIES REPORT

Appendix 5
Network Voting Business Case

Elections Ontario

Elections
Ontario

51 Rolark Drive
Toronto, Ontario
M1R 3B1

1.888.668.8683
TTY: 1.888.292.2312
info@elections.on.ca
elections.on.ca

ISSN 978-1-4606-2017-5 (PDF)

CONTENTS

EXECUTIVE SUMMARY

Background

Vision:

The *Election Act* requires Elections Ontario to review and report on alternative voting technologies by June 2013. As part of its strategy of innovation, Elections Ontario has determined that network voting technologies should be the focus of this review and if feasible that the evaluation be done during a by-election in 2012. The Business Case analyses the suitability of network voting technologies for the province of Ontario and assesses the feasibility of conducting a pilot within the given time constraint.

Opportunity:

Network voting is a means of both casting and counting votes electronically and is based on the transmission of ballots and votes via telephones, private computer networks, or the Internet. As it has in other jurisdictions, network voting could benefit Elections Ontario by making it easier to cast votes, and widening access for voters with disabilities via voting options beyond conventional paper ballots.

Purpose of this Business Case:

Driven by the Chief Electoral Officer's commitment to modernize the electoral process in Ontario, this investigation into network voting presents the benefits, assesses the risks, and estimates the costs of a network voting pilot.

Purpose of the Pilot:

In turn, the purpose of the pilot will be to evaluate the recommended solution's capacity to support Elections Ontario's principles. As the evaluation will take place in a by-election setting with real voters, the recommended approach must take into account the real risks and complexities of network voting.

Benefits:

The result of this effort, however, will be a set of measurable outcomes that will ensure that Elections Ontario's report to the legislature in 2013 is based on a comprehensive study during a binding election. The pilot would allow Elections Ontario to demonstrate the effectiveness of its risk management strategies, measure elector uptake and acceptance of network voting channels, and to assess the capacity of the technology to function at the scale of a general election.

Research indicates that a large proportion of the Ontario population views alternative voting favourably and this is mirrored in the recent movement towards Internet and telephone voting at the municipal level. These trends, combined with the high rate of access to the Internet in Ontario, create an opportunity to pilot network voting, evaluate it thoroughly in an election setting, and assess its suitability for use in a general election.

Constraints and Principles

Time Constraints:

In order to be ready to report to the Legislature in mid-2013, Elections Ontario is aiming to complete its evaluation in 2012. As the timing of a by-election is impossible to predict, the overriding constraint is for Elections Ontario to be ready for a pilot as early as possible in 2012.

Process and Complexity Constraints:

In order to meet this schedule, and in order to integrate as well as possible with Elections Ontario strategy, the pilot must meet the following additional constraints:

- Keep integration with existing electoral systems and processes to a minimum, with special consideration for integration points around the voters list and results reporting;
- Impact on the organization, including potential changes to process, personnel, or system requirements, should be minimized;
- Offer network channels as a supplement to paper;
- Authenticate voters through a self-sufficient mechanism rather than integrating with and leveraging third-party authentication;
- Offer network voting during the advance period, but not on election day; and
- Provide accessible interfaces, with the objective of meeting the standard set by the recently implemented accessible ballot marking devices.

Principles:

Given the fact that network voting channels will be tested in a binding election, certain principles were chosen that led directly to elimination of certain options and the design of the recommended approach. A full description of each principle can be found in Section 3 of the Business Case. These key electoral principles are as follows:

1. Accessibility
2. One vote per voter
3. Voter authentication and authorization
4. Only count votes from valid voters
5. Individual verifiability
6. Voter privacy
7. Results validation
8. Service availability

Research Review

Scoring and Evaluation:

Based on a review of network voting in other jurisdictions, and the results of preliminary stakeholder consultation, the research identified seven basic network-voting mechanisms and six means of voter authentication. The intersection of these options produced ten feasible network voting scenarios, which have been assessed for their ability to support Elections Ontario's electoral principles, and for relative cost, complexity, and convenience factors.

Short List of Four Scenarios:

Of these ten scenarios, a short list of four scenarios qualified as suitable for a by-election pilot due to their ability to support Elections Ontario's principles:

1. Onsite computer voting with supervised authentication,
2. Onsite telephone voting with supervised authentication,
3. Remote computer voting based on password authentication, and
4. Remote telephone voting based on password authentication.

These four options were presented to the Elections Ontario senior leadership, who reviewed the short list and recommended further analysis to identify the most viable implementation options for the pilot.

Recommended Approach

Procure a Commercial Off The Shelf (COTS) Solution:

It is recommended that Elections Ontario procure, customize, and implement a Commercial-Off-The-Shelf (COTS) network voting system to be used in a by-election in 2012. To do this, a vendor must be selected by October 2011 and the solution must be ready for rollout in 2012.

Implement Remote Network Voting Channels Only:

The recommended model increases options and convenience to electors while supporting the need for security and integrity. The recommendation is to implement the following channels during the advance poll period as a supplement to the established paper ballot:

1. a remote internet voting channel based on a web interface that is compatible with assistive technology;
2. a remote telephone channel, as an option for electors without access to the internet and who find it difficult to attend a polling location in person.

Approach Overview:

The onsite channels short-listed by the research have been eliminated following detailed analysis. The onsite telephone channel presents several risks, introduces accessibility and privacy issues related to the administration of voter authentication. Onsite computer voting provides marginal accessibility and convenience benefits while increasing complexity for Elections Ontario significantly.

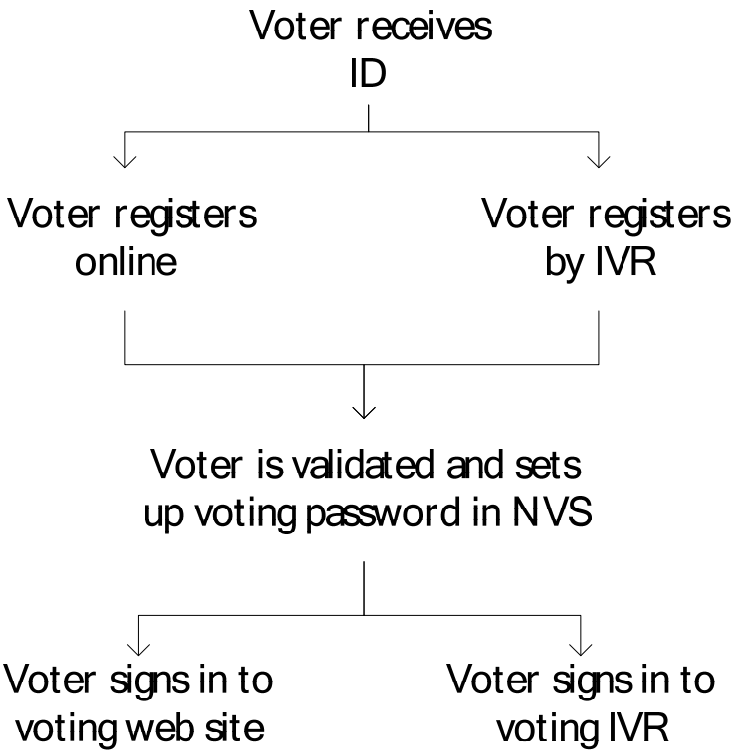
The recommended approach, therefore, is to pilot remote telephone and computer voting channels. All electors would receive an identification number in a secure letter and those who wish to use network voting channels would register in advance. Once registration is complete, electors will be able to vote online or by telephone during the advance polling period. The complete process would be as follows:

- While using government identification to support electors' identity claims is the most secure method, the fact that only Driver's Licence data is available to Elections Ontario will prevent electors who do not or cannot possess a licence to drive from registering via the standard process. Elections Ontario may, therefore, wish to allow these accessibility concerns to outweigh the need for security in this case.
- A registration process that uses a less secure form of identity support (address and date of birth) but introduces the incremental security benefit of a second letter will allow all Ontarians to access the same process. Elections Ontario must also accept that, while this alternative may be more accessible, it adds additional delays to the process that will make network voting more difficult and may reduce overall adoption, thereby reducing the sample size used to support the report to the Legislature in 2013.

Registration and Authentication:

1. Electors receive a network voting registration letter that includes a secure numeric Elector ID and instructions for accessing a remote network voting registration web site.
2. Electors who choose to register for remote network voting will visit the web site and enter their Elector ID and their date of birth to register. For added security, their driver's license number can be used to establish their identity. A second card could also be mailed at this stage to provide the voter a secure second PIN before proceeding to the next step.
3. Once authenticated, the system will validate their eligibility and allow them to set up a secure password to use for voting. Alternatively, electors who do not have easy access to the Internet can call a toll-free number to perform the same steps using an IVR interface that connects to the same backend system.
4. Once the advance poll period begins, voters who have registered for remote voting can log in to either the voting web site or the voting IVR system using their Elector ID and password.

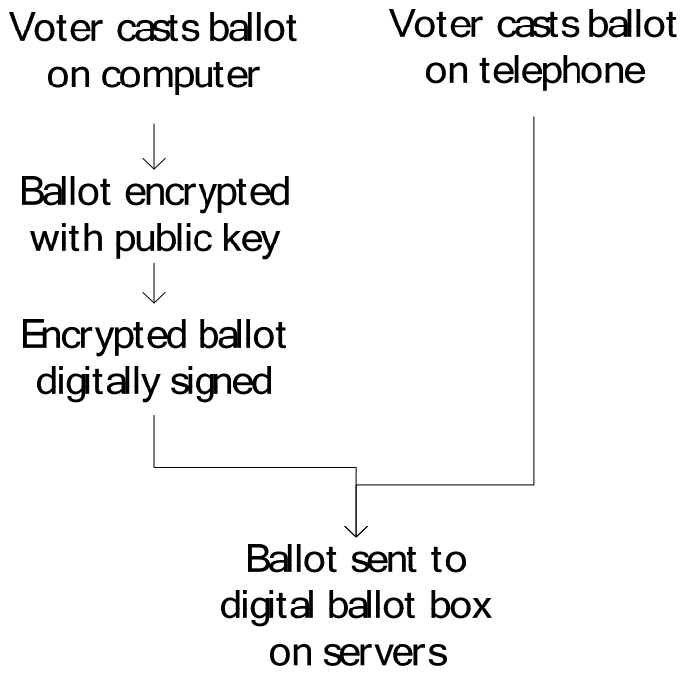
Registration and Authentication process



Online Voting Process:

5. Once a remote voter has been authenticated on the voting web site, he or she will cast a ballot by making a selection from an online screen. Voters who use the telephone will make their selections using an automated menu system. Both of these options must be optimized for usability and accessibility in order to provide the best user experience.
6. After voting on one of these channels, the voter will be struck from the voter's list and receive a receipt that will allow them to verify the inclusion of their ballot in the final election results.
7. The voters list could be managed through an online, real-time process to prevent the possibility of double-voting via multiple channels and to keep the network voting system up to date with revisions. Alternatively, voters could be locked in to the remote channels once they register in order to prevent them voting twice.

Online Voting Process



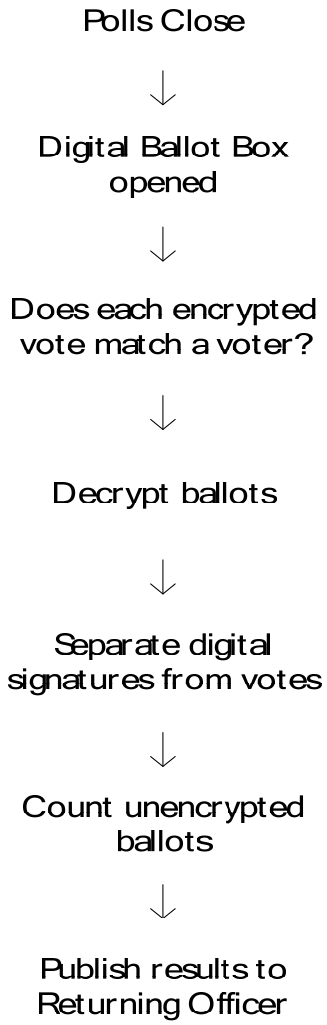
Vote Storage:

8. After a ballot has been cast on either the telephone or computer channels, it will be stored in a secure server environment that is subject to stringent physical and application security measures, as well as availability and performance requirements.
9. The ballot will be securely encrypted so that its contents cannot be read while stored in the ballot box.

Tabulation Process:

10. Once the voting period has closed, the electronic ballot boxes will be moved to an isolated and secure counting environment.
11. Before decryption, the system will check that all the votes contained in the ballot boxes are cast by eligible voters.
12. The ballots will be decrypted by authorized Elections Ontario officials who each possess a portion of the key required to decrypt the ballots.
13. Once decrypted, the ballots cannot be associated with a voter.
14. The system will count valid ballots and distribute combined network voting results to the Returning Officer, who will include them in the official count.

Tabulation Process



Audit:

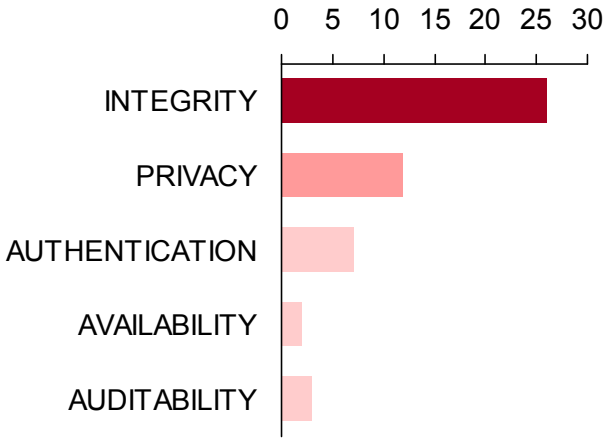
15. The system must allow the Network Voting Management Board to carry out new decryption and tabulation processes if required, under the supervision of independent auditors.
16. The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes. Auditors should be able to operate with the decrypted votes and obtain human-readable results that can be compared to the ones generated by the system.
17. The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes, including the authenticity of the software, the integrity of the system, the integrity and authenticity of the generated logs, etc.

Risk Assessment Summary

While this approach is being recommended for its ability to support accessibility, integrity and security, there are still risks. A network voting model based on a combination of computer and telephone voting is potentially vulnerable to several types of risk, with security being the most prominent.

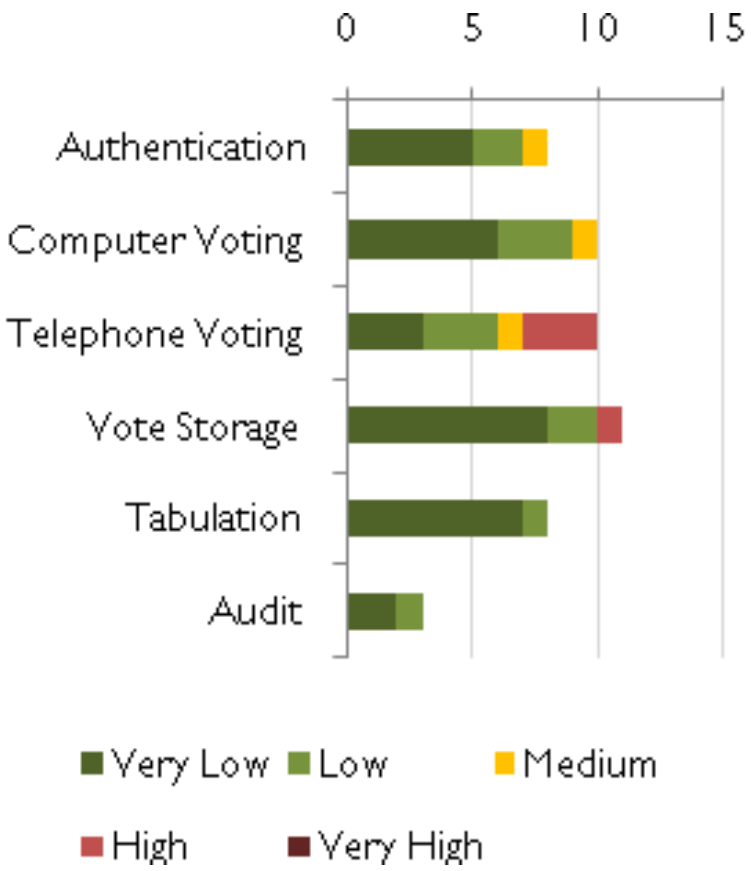
As seen in the graphic below labeled ‘Security Risk Categories’, the most prominent security risk category is made up of threats against the accuracy of the results, which have a direct bearing on the integrity of the election. These threats include the possibility that votes could be modified or deleted while they are being cast, once they are stored in the system, or as they are being counted.

Security Risk Categories



After integrity, there are a number of possible privacy threats that would result in the voter and their ballot choice being linked. Furthermore, if authentication protocols are not secure enough, voters could be impersonated or ineligible names could be added to the voters list. There are also potential denial-of-service threats that would compromise the availability of the system during voting, and a possibility that the data required for accurate election auditability could be compromised.

The following graphic labeled ‘Residual Risk Levels by Process Step’ presents a summary of the security risk assessment for the network voting system. It displays the number of potential threats for every step in the electoral process, with the voting step split into two rows – one for both voting methods. It displays the residual risk level that would be in place provided that the appropriate mitigation steps are taken.



Residual Risk Levels by Process Step

Data from graphic:

- Threats to the authentication stage of the voting process: 5 very low risk threats, 2 low, 1 medium, 8 total threats.
- Threats to computer voting: 6 very low risk threats, 3 low, 1 medium, 10 total threats.
- Threats to telephone voting: 3 very low risk threats, 3 low, 1 medium, 3 high, 10 total threats.
- Threats to vote storage: 8 very low risk threats, 2 low, 1 high, 11 total threats.
- Threats to the audit stage of the voting process: 2 very low risk threats, 1 low, 3 total threats.

For the most part, the threats can be mitigated to the point where they present only a low or very low risk. There are still some medium risks for areas such as telephone authentication and voter coercion.

The only step in the process that faces threats with a high residual risk is telephone voting, with three high-risk threats:

- an attacker could intercept the vote after it leaves the telephone but before it reaches the secure voting servers;
- an IVR system administrator could intercept the votes in transit, violating privacy and enable unauthorized publication; and
- an attacker who intercepts the votes could modify them.

While many of the technical risks of a network voting channel can be mitigated through the security technology selected, there remains a risk regarding public perception. While they may be a minority, there exist vocal opponents to network voting that contend that it is inherently less reliable, secure, or democratic than traditional means. While public perception has the potential to be a threat to a successful network voting implementation, it can be mitigated through a comprehensive communication strategy.

The strategy for addressing both the public concerns and the real risks regarding potential security, privacy, and integrity problems is the same: to specify and procure a system that provides the highest end-to-end security available and ensure that it is auditable. The privacy and integrity of the vote must be protected from the moment the voters cast the ballots until the vote is counted and this protection must be verifiable.

Success Criteria

1. The pilot must implement a system that preserves and records evidence of a continuous “Chain of Trust” that controls custody of the ballot data. The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes, including the authenticity of the software, the integrity of the system, the integrity and authenticity of the generated logs, etc.

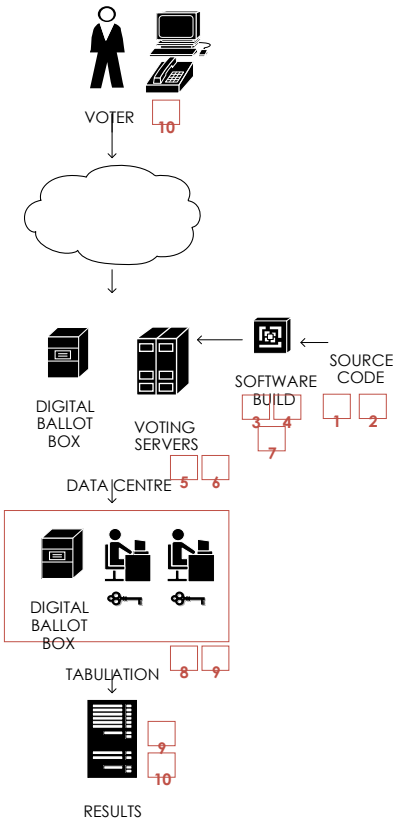
   The success and integrity of an election depends on eliminating the possibility that ballots have been tampered with. In a network voting system, tampering could occur through the installation of malicious code at some point in the ballot custody chain. To prove election integrity, Elections Ontario must be able to demonstrate that only authorized parties and software have come into contact with the digital ballot data.

If the implementation of the network voting system does not both support the Chain of Trust and provide auditable evidence, then the process is open to question. This Chain of Trust is a compilation of all the following measures:

1. Source code audit to verify that the code will do only what it is intended to do.
2. Digital signature of the audited source code to protect its authenticity and integrity.
3. Trusted build of the executable code in front of auditors (based on audited source code).
4. Signature of the executable code to protect its authenticity and integrity.
5. Deployment of the executable software in a clean system.
6. Logical sealing of the system to detect any later additions.
7. Logic and accuracy testing of the voting system to validate it works properly.
8. Continuous audit of the voting system during the election, through review and validation of logs and other data. The logs must be protected from external manipulations by using cryptographic measures.
9. Post-election audit that validates that the system behaved correctly by reviewing the logical seals and the protected logs.
10. Individual voter verification that proves their ballots were used in the final tally (by using special receipts).

A strong emphasis must be placed on audit. Independent auditors must be able to review the source code, verify the build and deployment, audit system logs during the election event, and finally to review both the counting process and the results.

Chain of Trust



2. An experienced project team must execute an effective implementation approach that focuses on the following:

- Procurement of secure, high-availability hosting;
- Procurement of a Custom off the Shelf (COTS) that provides strong end-to-end security, and a vendor experience in large scale binding elections;
- Thorough user and performance testing;
- Demonstrations and stakeholder review;
- Dedicated participation of subject matter experts from Elections Ontario to ensure customized solution is a tight fit; and
- Continued consultation with an emphasis on widening the scope of stakeholders consulted.

3. To evaluate success, and to provide a report on the suitability of network voting technologies for application in the province of Ontario, Elections Ontario will need to be able to evaluate the outcome of the pilot against a meaningful set of objectives derived from the key network voting principles. This business case provides ways that success or failure to uphold each principle could be assessed and measured.

   During the implementation of the project, specific measurement points and target values must be defined for each principle. Each principle can be measured by a number of means including post-event surveys, online experience surveys, audit results, and technical monitoring.

4. Equally important will be Elections Ontario's ability to communicate the security and integrity of the process through a detailed outreach campaign that demonstrates both that there are valid concerns and that they have been addressed.

Estimated Pilot Costs

Recommended Model - Two Remote Channels:

The estimated cost for a pilot of the two recommended channels is **$1,745,500.00**, of which approximately half is made up of the costs of the Custom Off the Shelf or COTS product. This figure is the total expenditure required to customize and test the COTS product, license 100,000 voters at $2.00 each, conduct voting, count the ballots, and audit the entire process.

However, the majority of these costs would not recur if a second by-election were to be held in the same year. The largest recurring item is the COTS cost, which is primarily composed of voter licensing and election support costs. The remaining recurring expenditure is the cost associated with the event implementation (approving and rolling out the system, support staff, and secure mailing). As a result, remote network voting in a second by-election with 100,000 electors would incur an additional total of approximately $649,500.00.

While it is difficult to project the costs accurately for a general election, it is worth noting that a key factor is likely to change: the per-user licensing fee charged by a COTS vendor will drop to as little as $0.25 per user. Due to this much lower per-voter license cost, the costs would be more evenly distributed among the COTS, Location Costs, and Implementation line items.

The costs reflected in this study are based on a review of industry pricing and may change substantially in the context of a competitive bid or a contract negotiation. The procurement process will identify actual cost.

The chart below breaks down the estimated cost of a pilot (remote only):

Pilot Costs

Costs for a pilot (remote only)	
Custom off the Shelf (COTS)	$837,000.00
Polling Location Costs	$0.00
Central Infrastructure	$162,000.00
Implementation Costs	$217,500.00
Project Resource Costs	$429,000.00
Other project costs	$100,000.00
TOTAL	**$1,745,500.00**

Key Recommendations

Remote Channels Only:

The objectives of the pilot can be achieved by implementing remote channels only. Given the complexity and cost of implementing onsite network channels, and the incremental benefits to accessibility of doing so, it would not be worth the investment for the pilot.

Authentication by Driver's License is Not Universally Accessible:

Voter authentication is one of eight key principles that must be supported during the pilot. However, the related process is the source of several key security risks, including the risk of voter impersonation. Part of the mitigation for these risks is the incorporation of personal voter data into the registration process in order to support the voter's identity claim. Currently, the most secure option is government identification in the form of Driver's Licence Number.

While verifying a user's identity using this form of identification is the best means currently available, it has a direct impact on voters who cannot obtain a driver's licence. While this compromise could be considered acceptable for the pilot, Elections Ontario would need to pursue a more universal form of identification or other personal data for future elections.

Pursue a More Universal Authentication Model:

Opportunities for a more universal authentication method exist and should be pursued. Elections Ontario should explore two directions simultaneously:

- obtaining a personal data element for verifying electors during registration that is more universal than a Driver's Licence Number; and
- integrating with and leveraging a third-party authentication mechanism, such as ServiceOntario.

For the purposes of the pilot, Elections Ontario may wish to consider a registration process that uses a weaker but more accessible process, such as the two-stage postal process described as an alternative in Section 6 of the Business Case.

An Electronic Poll Book is not a Dependency for Remote Voting Pilot:

If both remote and onsite network voting were implemented, the threats created by having multiple parallel voting mechanisms (paper, computer, and telephone) and differing types of authentication (physical and password), would put two key principles at risk: the ability to ensure that only one vote is counted for each voter and the need to only count votes cast by valid voters. The mitigation strategy would need to include an online, real-time poll book that manages network voting and paper channels simultaneously. Without an electronic poll book, voters could potentially vote twice: once online and once in person.

However, by removing the onsite network channels, the risk of multiple votes per voter is reduced and the cost and complexity of an electronic poll book is harder to justify. In this scenario, the risk can be controlled by restricting registered network voters to the remote channels. Their names would not appear on the paper poll books and they would be unable to vote by paper during the advance polling period.

Telephone Voting is a Risk Area but Increases Access to Voting:

The telephone voting channel presents inherent risks that are among the most difficult to manage or mitigate successfully. These risks stem from the fact that telephone voting uses an infrastructure that cannot be secured in the same way as computer voting can be. The public telephone lines are not secure, which opens up the possibility of privacy threats. Votes then pass unencrypted through the IVR environment, where they could be intercepted, deciphered, and even modified. However, the inclusion of telephone voting greatly increases the ease of access to network voting to segments of the population who have no access to or comfort with computers and the Internet. These risks can be mitigated to an extent, primarily by securing the IVR environment and implementing intrusion detection systems. Removing telephone voting would weaken support for principles, but also reduce risk, cost, and complexity.

Elections Ontario Must Control the Hosting Environment:

Elections Ontario's ability to control the network voting environment as much as possible will play a big part in establishing and maintaining the Chain of Trust. Elections Ontario should therefore procure the hosting environment (including web + IVR environments) under terms separate from the procurement of the COTS solution and the successful vendor will need to specify their detailed hardware and infrastructure requirements. Otherwise, the Request for Proposal (RFP) must specify that the hosting server is physically dedicated for the election project, in order to allow servers to be sealed in support of the chain of trust and support the audit process.

Emphasis on Audit:

The success and integrity of an election depends on eliminating the possibility that ballots have been tampered with. To prove election integrity, Elections Ontario must be able to demonstrate that only authorized parties and software have come into contact with the digital ballot data. A strong emphasis must be placed on audit. Independent auditors must be able to review the source code, verify the build and deployment, audit system logs during the election event, and finally to review both the counting process and the results.

Go/No Go Check-Point Reviews:

In planning for the Pilot, check-point reviews should be incorporated at the end of each Gate in the Network Voting project. A Go/No Go decision review to proceed to Pilot should be scheduled upon:

- Approval of the Business Case;
- Approval of the Project Charter;

- RFP response\vendor evaluation – based on cost;
- Completion of User Acceptance Testing (UAT), Systems Performance Testing, Threat Risk Assessment/Privacy Impact Assessment (TRA)/PIA), and
- Assessment of the by-election electoral district.

Conclusion

The recommended network voting approach, therefore, is to implement remote voting in the form of telephone and internet voting in an upcoming by-election. Doing so according to the general model described in Section 6 of the Business Case, but without implementation of onsite channels, will result in a pilot that is able to operate within Elections Ontario's business constraints, support core electoral principles, and achieve the strategic direction and objectives.

Conducting a pilot that is run during a by-election and consists of a mix of remote network voting channels that provides electors with a range of options, while still managing the overall cost and complexity of the implementation, will result in a solid and thorough basis for Elections Ontario's 2013 report to the Assembly. To do this, the pilot must be structured so that Elections Ontario is able to demonstrate whether key election principles can be well supported, whether risks can be managed, and whether the benefits outweigh the costs.

1. BACKGROUND

The current Election Act requires the Chief Electoral Officer to conduct a review of alternative voting technologies and submit a report on that review to the Speaker of the Assembly by June 30, 2013. Elections Ontario has determined that, if feasible, this review has the option of taking the form of a pilot of network voting technologies in a by-election held in 2012.

1.1 PURPOSE OF THIS DOCUMENT

RECOMMENDATIONS FOR IMPLEMENTATION

THIS BUSINESS CASE analyses network voting and recommends a combination of voting technologies and user authentication mechanisms that have been assessed for feasibility in the Ontario context. It uses Elections Ontario's unique drivers and constraints as a basis for analysis, incorporates the results of stakeholder consultation and a detailed industry scan, provides a specific approach to implementation, and includes a detailed risk analysis.

1.2 THE OPPORTUNITY

BENEFITS

Recent research indicates a large proportion of the population views online voting favourably and this is mirrored in the recent movement towards Internet voting at the municipal level. Coupled with Ontarians' high rate of access to the Internet, there exists an opportunity within Ontario to pilot network voting solution and position Elections Ontario as an innovator.

Network voting technology, in a general sense, can give an electoral authority numerous benefits and opportunities for better service:

- **Ease of Vote** Network voting provides an additional voting channel by letting voters cast their vote any time, any place, including electors residing or staying outside of Ontario;
- **Accessible Vote**: Network Voting widens access for voters with disabilities or those having other difficulties being physically present at a polling station and using the devices available there;

1.3 THE RISKS

SECURITY RISKS

While network voting has numerous benefits, it also presents risks that can, if unmanaged, compromise the integrity of an election. In recent years, ways of the mitigating the technical and security risks of a Network Voting channel have been developed by industry, but there remains the equally likely and relevant risk of public perception.

PUBLIC PERCEPTION RISKS

While they may be a minority, there exist vocal opponents to network voting that contend that it is inherently less reliable, secure, or democratic than traditional means. This perception has the potential to be a greater threat to a successful network voting implementation than the possible technical challenges.

1.4 PROJECT DRIVERS

REVIEW ALTERNATIVE VOTING TECHNOLOGY

In response to the passage of Bill231, which includes a provision requiring the CEO to conduct a review of alternative voting technologies and submit a report back by June 30, 2013, Elections Ontario initiated a project to research alternative methods of network voting. This project is being driven by the Chief Electoral Officer's commitment to modernize the electoral process in Ontario through both conventional and technological solutions.

OPPORTUNITY TO INNOVATE

Pilot in a By-election

Section 4.1 of the Election Act[1] gives Elections Ontario the opportunity to test and evaluate the Network Voting solutions in a binding election and demonstrate whether network voting will address the needs and challenges of the Ontario electorate. A pilot during a binding election should allow a range of network voting options to be measured against the voting principles that Elections Ontario must uphold. In order to make the most of the opportunity given by a by-election pilot, a range of network voting channels should be considered for testing and evaluation, in order to validate the technology and process options that could be feasible on the scale of a general election.

1.5 PILOT OBJECTIVES

The proposed pilot of network voting technology will allow EO to meet new legislative responsibilities. The pilot will review alternative voting technologies and submit a report on that review to the Speaker of the Assembly by June 30, 2013. The pilot should be an evaluation of network voting as an alternative voting channel and not of the specific solution or platform used to implement the Pilot. Objectives include:

- ***Assess*** network voting as an alternative channel that increases accessibility and convenience for all electors.
- Measure elector ***uptake and acceptance*** of alternative network voting channels and assess public attitude.
- Assess ***scalability*** of the alternative network voting channels to a General Election.
- Validate that Network Voting protects the ***security and integrity*** of the election standard equivalent (but not necessarily identical in each element).

1.6 RELATED DOCUMENTS

Elections Ontario, Network Voting Options Evaluation (version 2.0); 8 March 2011

1.7 DOCUMENT HISTORY

- Draft presented to the Chief Electoral Office and the senior leadership team on 29 April.
- Revised draft presented 31 May.

2. DECISION CONTEXT

The following section describes the factors that must be considered when evaluating and analyzing the application of network voting technology in Ontario and provides an overview of the strategic drivers and practical constraints that affect this initiative.

Inputs to Decision Making

WHILE THE RESEARCH described below in Sections 4 and 5 identify a number of potentially feasible network voting scenarios, there are time, cost, legal, and demographic factors that constrain how network voting approaches and technologies could be implemented in Ontario. Further, there are key stakeholder groups who have an interest in the outcome of Ontario's Network Voting solution. This section describes how the following factors contribute to the decision making context:

- Elections Ontario's strategic direction;
- project constraints;
- the target audience;
- stakeholder consultation outcomes; and
- a set of working assumptions that have guided the analysis of possible network voting methods.

2.1 STRATEGIC DIRECTION

The network voting approach recommended by this business case has been evaluated against its ability to support Elections Ontario's strategic direction, which is defined as a combination of the organization's Mission, Vision, and Values; specific project drivers; and Elections Ontario's Strategic Priorities.

Mission, Vision, & Values

Integrity & Accessibility

Elections Ontario's stated mission is to "protect the integrity and accessibility of the electoral process and to administer elections in a fair and impartial manner". These principles of integrity, accessibility, and fairness are supplemented values of key relevant values of responsiveness, innovation, and transparency. Finally, Elections Ontario has a vision to "set the standard for electoral process excellence" and to "innovate and lead in defining key benchmarks for electoral administration."[2]

Innovation

Project Drivers

The motivation for a potential Network Voting pilot is made up of the following three drivers:

Voter Choice

- Put voters' needs first by providing more choice.
- Make voting easy and accessible for all Ontarians.
- Set the standard for electoral process excellence by continuing to innovate and lead in the definition of key benchmarks for electoral administration.

Strategic Priorities

Any network voting method, or combination of methods, must support EO's strategic priorities for 2008-2011, which are as follows:

1. Maintaining the Permanent Register of Electors for Ontario and developing its products
2. Expanding EO's public education and outreach activities
3. Managing EO's business
4. Protecting the integrity of the electoral process

For the purposes of this Business Case, priorities 1 and 4 will be used to evaluate the recommended approach to network voting. This means the selected approach must be shown to support Elections Ontario's priorities of **developing** its range of products and protecting the **integrity** of the electoral process.

2.2 CONSTRAINTS

There are a set of practical constraints that limit the range of options possible for implementation. This section defines these constraints according to the following categories:

- Legislative constraints;
- Process constraints;
- Time constraints;
- Cost constraints; and
- Technical constraints.

Other factors, such as socio-demographic constraints, are dealt with in subsequent sections.

Legislative Constraints

REPORT ON ALTERNATIVE VOLTING BY JUNE 2013

The key legislative constraint is that the Chief Electoral Officer of Ontario is required to "conduct a review of alternative voting technologies, prepare a report of the review and, on or before June 30, 2013, submit the report to the Speaker of the Assembly". While this legislation provides Elections Ontario with the opportunity driving this business case, it also constrains Elections Ontario in terms of both the timeframe (see below) and format of the evaluation, as the review must be comprehensive and conclusive enough that it provides a means to report conclusively on the suitability of alternative voting technologies in general.

Process Constraints

REPORT BASED ON A PILOT DURING A BINDING ELECTION

In order to meet the challenges of the legislative opportunity, Elections Ontario has determined that, if possible, the evaluation of network voting can be done through a pilot during a binding election (likely a by-election) and not in a theoretical test setting; however, in order to mitigate foreseen risks, Elections Ontario has determined that there should be no network voting on Election Day.

NETWORK VOTING AS A SUPPLEMENT TO PAPER

Additionally, the Chief Electoral Officer is clear that network channels are to be implemented as a supplement to paper voting and that the current mechanism is to be available at all times during the event. Voters should be able to register for a network channel, but then decide to vote by paper and vice versa.

MINIMIZE ORGANIZATIONAL CHANGE

Elections Ontario has also determined that, as the pilot implementation may not necessarily lead to implementation of the same solution in a general election, there should be a minimum of change imposed on the organization. The approach considered for the pilot should therefore be designed to have as little impact as possible on existing Elections Ontario people, processes, and systems. The approach should keep integration with existing electoral systems and processes to a minimum, with special consideration for integration points around the voters' list and results reporting.

Time Constraints

System to be Piloted Should be Ready by the First Quarter of 2012

Should a pilot be considered as part of the assessment process, the network voting system must be ready for a by-election in 2012 in order to meet the June 30, 2013 reporting date.

Cost Constraints

Solution Should be Cost-Effective

Given that the actual costs of the network voting pilot will be determined largely by the costs associated with vendor products and services, there is no specific cost limit constraining the solutions recommended for the pilot.

However, there is a stated constraint that the implementation approach should be as cost-effective as possible. Earlier research scored each scenario based on a relative scale of cost-effectiveness.

Technical Constraints

Data will be Required to Support a Network Voting Implementation

In order to properly deliver any network voting solution, key information and data is required to support the voting and casting process. The information is contained in various forms within information systems found at EO or other provincial bodies and will need to be accessed as part of Network Voting solution.

Two key components would make critical contributions to a successful Network Voting implementation:

- a real time electoral list (Without a real-time list, each voting channel would have to be locked in and managed separately.); and
- a secure method for establishing voter identity.

The existing electronic electoral list (ELMS/EMS) must be kept up to date with changes to the electoral list at all times during an electoral event.

Voter authentication data is not currently held within EO would need to be obtained through other provincial bodies. The most likely candidate would be the One-key service[3] being launched by ServiceOntario, which is “designed to be a common access point for Ontario programs”; however, integration with this service will not be feasible in the time lines set out for the pilot. Therefore other means will need to be found in order to properly authenticate voters.

Constraints Summary

The following table provides the full list of constraints.

	CATEGORY	CONSTRAINT
1	Time	Elections Ontario must be ready for a pilot by January 2012.
2	Legal	The Act forbids network voting, but section 4.1 combined with 44.3 override that for by-elections. Section 44.2, which comes into effect in January 2012, overrides that for general elections under specific circumstances.[4]
4	Legal	Electoral data, including data captured and stored by a network voting system, must be stored for and decommissioned after a defined length of time (for both PIA gathered during registration and the election results).
5	Process	If possible, the evaluation of network voting should be done through a pilot during a binding election (likely a by-election) and not in a lab / test / POC setting.
6	Process	No network voting on election day.
7	Process	Paper ballots to be available at all times (do not remove any current mechanism - only add).
8	Process	The current electronic elector list (ELMS/EMS) is to be kept up to date at all times during an event.
9	Process	Minimize organizational change by defining an approach that has a minimal impact on Elections Ontario people, processes, and systems.
10	Technical	Given that access to broadband is not universal in Ontario, the solution should not rely on high-speed connectivity but should make a reasonable effort to support usable access through a dialup connection in terms of system transaction response times.
11	Technical	Plans to use Information Technology Services (ITS)for hosting the application could introduce significant additional constraints, depending on the length of the cycle required to obtain and finalize hosting arrangements.
12	Technical	Only the following data is stored for each elector: ED #, family name, given name, middle name, DOB, gender, civic address, mailing address.
13	Technical	Accessible interfaces used in pilot must meet the level of accessibility provided by EO's existing accessible ballot marking devices.
14	Technical	Keep integration with and changes to existing systems to a minimum for the pilot.

2.3 TARGET AUDIENCE

POST-ELECTION SURVEY, 2007

In a pilot situation, a network voting solution would be aimed at the entire electorate rather than singling out any specific group or demographic within the electorate. This would result in an average potential voter base of roughly 80,000 electors for a by-election in a single Electoral District, with larger Electoral Districts having as many as 130,000 electors.

The Ontario electorate is well positioned for the introduction of network voting. Polling research about recent elections indicates a large proportion of the population is favourable towards online voting[5] and Internet voting is becoming common at the municipal level. Coupled with the fact that Ontarians have a high rate of access to the Internet and telephone infrastructure, and a high rate of familiarity with the use of the, Ontario is well positioned for Network Voting.

Attitudes toward online voting

According to Election Canada's *Survey of Electors Following the 40th General Election*, 42% of respondents from the Ontario electorate would be "very likely" to vote online, which was the highest rate among Canadian provinces.

However, negative public and media perception of network voting still exists, as does the existence of groups opposed to the concept of network or electronic voting. While it is recognized that this may not be the dominant perception, the implementation should be mindful of the concerns and objections raised against network voting.

Experience with Municipal Network Voting

Several Ontario municipalities have used network voting technology in binding elections. The most recent examples include Markham, Peterborough, and Stratford, who used network voting in 2010 municipal elections and shared their experiences with Elections Ontario at a Municipal iVoting Learning Summit held in December of 2010.

To vote in Peterborough or Markham voters typically received a letter in the mail and then registered online to obtain final voting credentials, which were delivered by email in Peterborough and a second mailed letter in Markham. Stratford voters did not need to register in advance. Voters were able to cast ballots remotely in all three jurisdictions, with Stratford also providing voting locations. Network channels were offered as a supplement to paper ballots, except in Stratford where internet and telephone voting replaced the paper ballot.

Access to the Internet

In 2009, 80% of Canadians aged 16 and older, or 21.7 million people, used the Internet for personal reasons. The access rate is slightly higher in Ontario, at 81% of the population.[6] Of these Internet users, 75% use the Internet at least once a day[7] and 66.7% use it for banking or paying bills.[8]

Despite this high rate of access, however, there exist significant concerns regarding security and privacy. Of those who reported using the Internet for less than five years, 55% were very concerned about online credit card use and 50% about banking over the Internet. These proportions dropped to 42% and 37%, respectively, for those reporting five or more years of Internet use. [9]

Additionally, there appears to be an urban/rural divide with respect to Internet use. In 2005, only 58% of residents living in rural and small-town areas accessed the Internet, well below the national average. This gap between rural and urban areas may reflect the interaction of other socio-economic factors, or it may represent other effects, such as the availability of broadband. Broadband access, especially in rural areas, is still not universal. As a result, the selected solution should be designed to function well at slower (dialup) connection speeds.

Access to the Telephone

The 2006 Residential Telephone Service Survey indicated that 92.5% of Ontarians have a PSTN line in their homes. Among those households without a phone line (7.5% of Ontarians), 78.2% reported having cellular phone service and 31.7% reported using cable telephone or "VoIP" services.[10]. The survey also showed that1.2% of households did not have any telephone service at all. This rate was unchanged from the previous year.

Use of Assistive Web Technology

Users with visual impairment may rely on screen readers to access web pages. These assistive tools interpret the page's HTML code and reproduce it as speech. While conformance to web accessibility standards and practises is critical, any network voting solution must also be designed specifically with screen reader compatibility in mind. Refer to Appendix C for a discussion of screen readers within the context of general web accessibility.

A 2011 survey conducted by WebAIM (a partnership of the Center for Persons with Disabilities and Utah State University), has found that 59% of respondents use JAWS as their primary screen reader, followed by Windows-Eyes, Apple's VoiceOver, and NVDA all at around 10%.[11]

While JAWS and Windows-Eyes still dominate the market, comparing results from previous WebAIM surveys shows that these established products are losing popularity. As shown in the Figure 5, JAWS and Windows-Eyes have fallen from being used by 97% of users in 2009 to 70% in 2011. This loss of share is the result of the growing popularity of newer low-cost or free products such as NVDA and Apple's VoiceOver.

As the conclusions of the survey note, there is "no typical screen reader user". The network voting system should be designed for compatibility with not just the leading products, but for a reasonable range of products that include free and low-cost alternatives. Compatibility with low-cost software will also contribute to lowering barriers to users who do not ordinarily use assistive web technologies but may be encouraged to do so in order to use internet voting.

Figure 4: 2011 Market Share

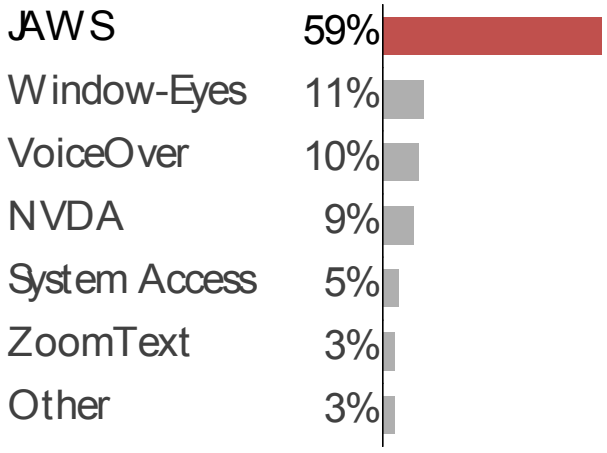
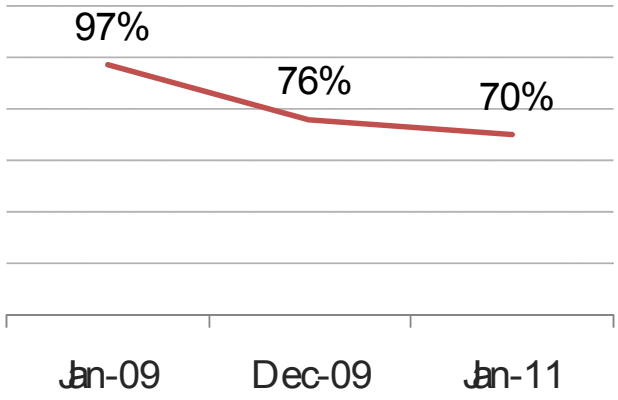


Figure 5: JAWS & Windows-Eyes are losing popularity



2.4 STAKEHOLDER CONSULTATION

ACCESSIBILITY ADVISORY COMMITTEE

Consultation for this phase of the initiative has been limited to consultation with the Chief Electoral Officer's Accessibility Advisory Committee This section provides an overview of the methodology for consulting with members of the Accessibility Advisory Committee (AAC). The consultation took the form of a series of questions designed to gather information on:

- Voting patterns and preferences; and
- Technology engagement.

Process & Outcomes

QUESTIONS & FEEDBACK

Following a project briefing at the meeting of the AAC held in Toronto on January 26, a number of questions were presented to the members of the committee who answered them in a round-table fashion. Follow up questions were also distributed via email and responses were gathered and analyzed. This section summarizes the results of the feedback received. For a detailed list of the questions, please refer to Appendix B.

In terms of the advantages and disadvantages of Internet voting, the members of the AAC noted the advantages to accessibility and the potential to support dignity, independence and equal access for all voters. They also noted that there was a potential barrier for electors without access to (or the means to access) a computer or high-speed internet. Another concern was the lack of the social nature of voting and the possibility of public mistrust.

Pros & Cons

The AAC members noted that telephone voting had the advantage of being more widely available but the disadvantage of posing distinct accessibility and usability problems. They also observed that, while they increased convenience for some voters, smart phones are not universally available.

Confidence & Security

In terms of the relative importance of Network Voting attributes, Members of the AAC were nearly unanimous in their ranking of *Confidence in the System* and *Security* as one of the top-two attributes for Network Voting. There was also great emphasis placed on both Privacy, and Convenience and Ease of Use.

There was a near-unanimous emphasis on the AAC's potential to participate in User Acceptance Testing (UAT) for Network Voting. Whether as participants in the testing itself, or by helping to oversee the selection of individuals to participate in the testing, this emerged as a strong theme throughout the responses. They felt that their breadth of expertise positions members of the ACC well to assist with Elections Ontario's UAT process.

Universal Design

Many of the comments made in the committee meeting and in a follow-up session with Elections Ontario's accessibility advisor strongly support the conclusion that both the technology and process must be easy to use and as universally accessible as possible for all electors - with an emphasis on reasonable accommodation and avoiding any type of differential treatment.

2.5 WORKING ASSUMPTIONS

In order to construct as accurate and complete a recommendation list, there are certain conditions that must be evaluated, which either cannot be known in advance or cannot be described adequately by principles or constraints. These assumptions include characteristics of a possible by-election; and general operational assumptions.

By-Election Characteristics

Based on an analysis of Ontario by-elections held in the past five years, several characteristics emerge as having implications for the planning and sizing of a networking voting pilot.

Figure 6: Selected By-Election Statistics

		Registered and Revisions	Voter Turnout	Number of Advance Polls	Total Votes Cast	Votes Cast in Advance Polls	Votes Cast in Advance Polls	Registered Voters who used Advance Polls
2010	Ottawa West-Nepean	86,809	33%	4	28,595	2,267	8%	3%
	Leeds-Grenville	76,053	37%	10	27,846	3,709	13%	5%
	Toronto Centre	96,846	33%	4	26,177	2,033	8%	2%
2009	St. Paul's	83,183	33%	5	27,830	3,353	12%	4%
	Haliburton-Kawartha	90,351	39%	10	35,541	6,370	18%	7%
	Burlington	77,749	29%	11	22,834	2,733	12%	4%
2007	York South-Weston	66,308	29%	6	18,977	1,328	7%	2%
	Markham	110,902	17%	14	18,522	1,901	10%	2%
	Toronto-Danforth	68,782	40%	5	27,437	3,129	11%	5%
2006	Nepean-Carleton	105,802	29%	8	30,170	3,251	11%	3%
	Parkdale-High Park	73,317	39%	14	28,646	2,226	8%	3%
	Whitby-Ajax	106,028	32%	5	34,376	4,623	13%	4%

SELECTED BY-ELECTION STATISTICS 2006-2010

Maximum values for key indicators shown in red.

As shown in the preceding chart, eight to thirteen per cent of by-election votes can be cast in the six-day advance poll (For by-elections, advance polls are for six days during the seven-day period that ends on the sixth day before polling day. See section 44(3) of the Election Act.), with the number of polls ranging from five to fourteen locations. If Markham, with upwards of 110,000 electors (currently confirmed at 133,000) experienced a voter turnout closer to the average by-election turnout of thirty-two per cent and the average advance poll rate of eleven per cent, it would result in almost 5000 votes being cast across fourteen locations.

If network voting attracts the same interest that it did in recent municipal elections, closer to 10,000 votes could be cast using network channels. In fact, ninety per cent of Markham voters polled in a 2010 survey that they would vote online provincially or federally if it were available.[12]

It can be reasonably expected that the publicity surrounding the introduction of network voting in a provincial by-election would have two relevant effects: that voting patterns may shift toward use of advance polling; and that this shift would in turn drive adoption of network channels at a similar rate to that observed in recent municipal elections (10-20% of votes cast[13]). For practical purposes, the recommended solution should therefore be able to function concurrently in fourteen advance poll locations and service the needs of, at a minimum, ten thousand voters accessing the system over six ten-hour days.

System should support 10,000 Votes over a six-day Advance Poll period

3. PRINCIPLES: EVALUATING NETWORK VOTING

For any initiative of this importance, a set of well-defined metrics must be used to evaluate success. This section provides an overview of the methodology used to create a list of core principles that are being used to evaluate network voting scenarios for this business case and that will ultimately be used to assess the success of the network voting solution and possibly a pilot should it be considered.

Choosing the Core Principles

IN ORDER TO CREATE a valid business case for network voting, there must be a direct link between the criteria used to evaluate the network voting options, the business case for the preferred options, and the success of the eventual Network Voting solution and/or pilot. The foundation for these criteria must be traceable to a core set of voting principles.

3.1 ELECTION PRINCIPLES

Any election must be universal, equal, free, and secret; and any Network Voting system must meet the basic requirement of supporting these fundamental principles. Before defining the subset of core principles that will guide the analysis, recommendation, and implementation of a Network Voting, a full list of principles must be defined. For the purposes of this analysis, these principles are divided into two groups*:

- **Universal principles**, which are derived from the four fundamental principles of universality, equality, freedom, and secrecy; and
- **Procedural principles**, which are derived from three fundamental procedural processes that are necessary to support the universal principles: Transparency, Verifiability & Accountability, and Reliability & Security.

*The principles used for this analysis were based on those recommended by the Council of Europe.

Universal principles

The following table illustrates the detailed principles that were derived from the four basic universal principles[14]:

1. Universality
    1.1. Usability
    1.2. Accessibility
    1.3. Reachability (location)
2. Equality
    2.1. One vote per voter
    2.2. No privileged voters
    2.3. No privileged actors
    2.4. Voter authentication and authorization
    2.5. Right to be on the Voters List
    2.6. Only count votes from valid voters
    2.7. Fair ballot layout
    2.8. No cost for voters
    2.9. Fair Voters List generation
3. Freedom
    3.1. No coercion or vote selling
    3.2. Individual verifiability
    3.3. Integrity
4. Secrecy
    4.1. Personal data privacy
    4.2. Ballot secrecy
    4.3. Voter privacy
    4.4. No intermediate results
    4.5. Secure data decommissioning

Procedural principles

The following table illustrates the detailed procedural rules or guidelines that were derived from the three basic procedural principles:

1. Transparency
    1.1. Voter training
    1.2. Information/diffusion
    1.3. Easy to explain to voters
2. Verifiability and accountability
    2.1. Source code auditability
    2.2. Process auditability
    2.3. Certification
    2.4. Results validation
    2.5. Election Monitor
    2.6. Review logs/forensics
    2.7. Potential partial reruns
3. Reliability and security
    3.1. Service availability
    3.2. No single point of trust
    3.3. Platform integrity
    3.4. Access control
    3.5. Ballot box integrity
    3.6. Logs integrity
    3.7. Voters List integrity
    3.8. Election configuration integrity
    3.9. Ballot Integrity

3.2 ASSESSING PRIORITY

To define the core set of Network Voting principles, each item on the full list of Universal and Procedural principles (see above) was assigned one of three priority levels (high, medium, and low). The principles given the highest priority rating are those by which the success of the pilot will be measured.

PRIORITY RANKING

High – these principles will be used to measure the success of the pilot in a by-election and to evaluate whether to proceed with Network Voting in a provincial election. This information will be used as criteria in the Network Voting Options and the Business Case documents.

Medium – these principles will form the mandatory system and procedural requirements for the business case (and piloted system). They will be defined as requirements in the Network Voting Options and the Business Case documents; and in the RFP that will be tendered for a Network Solution.

Low – these principles will be used as the nice-to-have system and procedural requirements of the business case (and piloted system). They will be used as criteria in the Network Voting Options and in the RFP that will be tendered for a Network Solution.

METHODOLOGY

The methodology that was applied to determine categorization considered the answers to the following questions with respect to a by-election pilot:

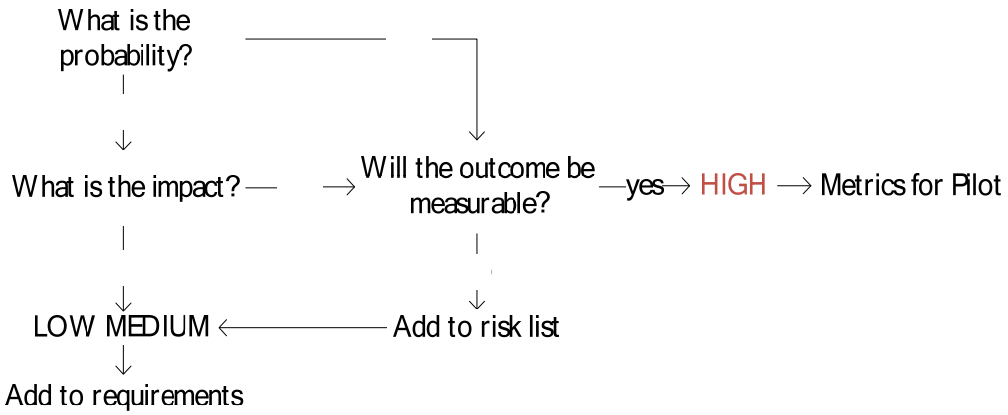
Will the outcome be difficult to measure or verify?

What is the probability that the ability to fulfill the principle will be challenged in a network voting context?

What would the impact be of a potential failure to fulfill the principle? I.e. would failure impact the perception of Network voting both provincially and federally?

Principles were ranked as 'high' priority if they had *either* a) a high probability of being challenged *or* b) a high impact of failure *and* c) the outcome can be measured in a quantifiable way. The following diagram illustrates the logic used to identify High priority principles.

SELECTION LOGIC



3.3 SHORT LIST OF PRINCIPLES

The following short list of principles was developed using the methodology outlined above. The numbers next to the name of each principle refer to the numbering used in the complete list of principles given in the following section. These principles will be used to measure the success of the pilot in a by-election and to evaluate whether to proceed with Network Voting in a provincial election. This information will be used as criteria in the Network Voting Options and the Business Case documents.

In some cases, the principles meet all three criteria of being (1) measurable, (2) having a high probability of being challenged by electors, and (3) would have a high impact on the perception of network voting if compromised. Others met criteria 1 and 3: measurability and high impact.

	PRINCIPLE	CRITERIA	RATIONALE
1	Accessibility[1.2]	**Checked** Measurable **Checked** High Probability **Checked** High Impact	Providing integrated and equal voting opportunities to all Ontarians that respect the independence and privacy of each elector is one of the key drivers for the Network Voting initiative and has a high public visibility.
2	One vote per voter[2.1]	**Checked** Measurable High Probability **Checked** High Impact	An electronic voting solution introduces perceived security vulnerabilities that do not exist in a paper ballot. If the vote count is compromised, the public perception of Elections Ontario would be damaged and the integrity of the election results would be affected.
3	Voter authentication and authorization[2.4]	**Checked** Measurable **Checked** High Probability **Checked** High Impact	A network voting channel must provide a feasible way to authenticate voter's identity remotely. This poses challenges, as no existing provincial infrastructure exists to authenticate voters digitally. While ServiceOntario would be the logical candidate, effort and time will be required to implement a handshaking protocol with EO's list of electors and ServiceOntario's existing service suite.

	PRINCIPLE	CRITERIA	RATIONALE
4	Only count votes from valid voters[2.6]	**Checked** Measurable High Probability **Checked** High Impact	If votes were counted other than those cast by valid and eligible voters, the integrity of the election would be severely affected. A network voting system may be vulnerable to malicious interference or ballot stuffing in a way that a paper system is not. Online voting could invite hackers and the impact would compromise the results of the election.
5	Individual verifiability[3.2]	**Checked** Measurable **Checked** High Probability **Checked** High Impact	It may be challenging to provide voters the same feeling of verification as a paper ballot / box system gives. Failure to provide the voter with feedback to verify that his or her vote has been recorded may call into question results, EO and damage the perception of network voting.
6	Voter privacy[4.3]	**Checked** Measurable High Probability **Checked** High Impact	While the likelihood of a network voting system compromising voter data and results is low, the impact should it occur, would compromise public trust in EO.
7	Results validation[6.4]	**Checked** Measurable High Probability **Checked** High Impact	Results validation is a basic tenet of elections and the ability to support a recount or audit, is critical. Failure to do so would call into question the election results and would impact future Network Voting solutions.
8	Service availability[7.1]	**Checked** Measurable High Probability **Checked** High Impact	Although public perception of system downtime can be mitigated, the electorate may not be as forgiving with a provincial interruption. System outages will be reported in the media and would impact the public perception of Network Voting solutions.

4. WHAT IS NETWORK VOTING?

The following section provides a basic introduction to some of the key concepts in Network Voting, including the main components and actors involved, as well as the methods for casting ballots and establishing and verifying voter identity.

NETWORK VOTING IS A MEANS of both casting and counting votes electronically. It involves the transmission of ballots and votes via telephones, private computer networks, or the Internet. Network voting technology can provide Ontario voters with options beyond conventional paper ballots by allowing them to cast votes using means that include the Internet, dedicated voting kiosks, or telephone.

This section provides a look at the basic elements of a generic network voting implementation:

- The components of a basic network voting system;
- The methods that can be used to cast a ballot; and
- The mechanisms that can be used to establish a voter's identity when voting.

4.1 A BASIC NETWORK VOTING SYSTEM

As shown in the diagram below, a network voting system consists of technology components, such as a network and a data centre, and actors, such as voters and elections staff, who interact with these components.

Voter: A voter is an elector who accesses the voting platform in order to cast a vote. To do that, a voter uses a voting device, either from a polling place or remotely.

Poll worker: If on-site voting is implemented, the Election Authority must have trained staff to assist and supervise the on-site electronic voting process.

Call centre: Any network voting scenario will require a call centre to support voters and poll workers.

Network: The network is the channel or channels used by the different actors to communicate with each other. It can be the Internet, the cellular network, the landline telephone network, or others.

Data Center: This facility hosts the voting platform and stores the electronic ballots until the polls close and they can be processed by the Electoral Authorities. A backup data centre can be set up to take over if the main data centre fails**.**

System Administrator: The person(s) that operate and maintain the data center facilities, including the servers and the digital ballot box.

Voting Servers: The technical infrastructure required to host and protect the electronic voting system.

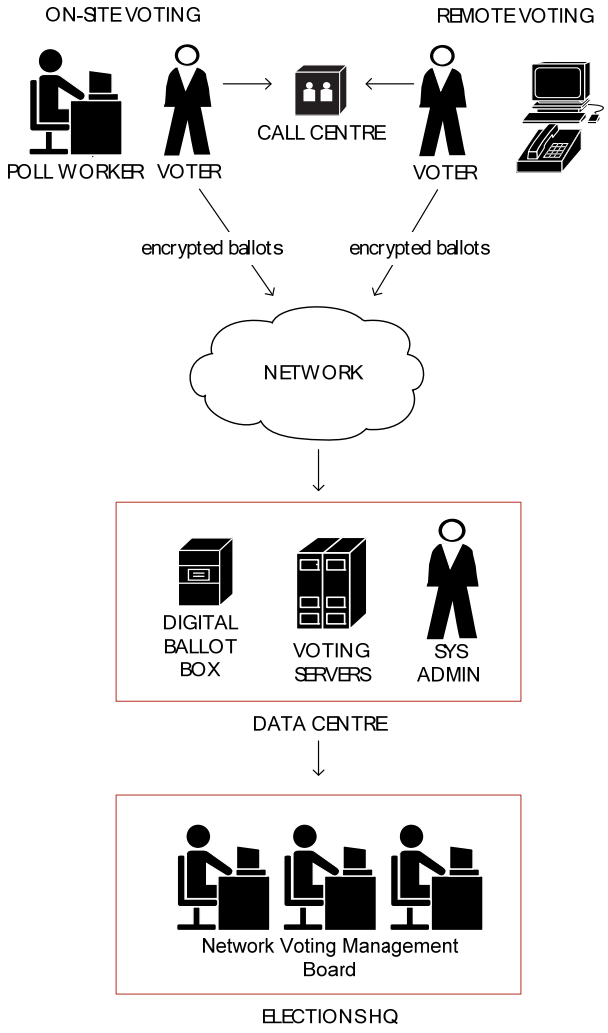
Digital Ballot Box: The place (usually a database) where cast ballots are stored pending final processing.

Elections HQ: The location where the election definition takes place. When polls close, electronic ballots are processed here (and merged with the results from other voting channels) by the Network Voting Management Board.

Network Voting Management Board: The group of persons responsible for supervising the processing of the electronic ballots.

Optional elements (not shown): Depending on the voting mechanism, there are some elements that may be present in the scenario, such as an IVR system or an SMS Gateway.

Figure 7 - Key components and actors



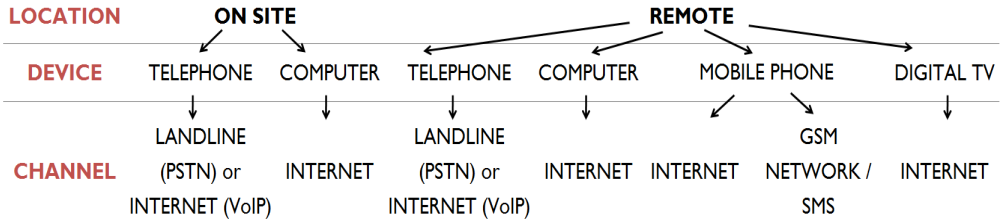
To support a system like this, certain elements must be in place:

- The data center (where voting servers are located and ballots are processed) must be reliable and secure.
- Electoral authorities must prepare all data required to configure the voting system.
- New procedures must be created to address new activities that network voting adds to the paper-based voting process.
- Some form of audit process to validate the voting system.
- A communications and public outreach campaign to introduce the new voting mechanisms to the population.

4.2 VOTING METHODS

As shown in the following diagram, voting methods can be classified based on the location from where votes are cast, the device used to vote, and the channel used to transmit votes to the servers.

Figure 8: Voting methods



Possible Combinations

By combining the locations, devices, and channels in this diagram, seven basic methods can be created:

1. On-site telephone-based voting through a landline (PSTN) or the Internet (VoIP)
2. On-site computer-based voting through the Internet
3. Remote telephone-based voting through a landline or the Internet
4. Remote computer-based voting through the Internet
5. Remote mobile phone-based voting through the Internet
6. Remote mobile phone-based voting through SMS
7. Remote digital TV-based voting through the Internet

Even after a brief analysis, it becomes obvious that not all of these combinations are appropriate for use in Ontario given current conditions. The infrastructures used by Digital TV and SMS are inherently less secure because third parties (cable companies, the cell phone provider) become trusted parts of the voting chain. Digital television, while very common, is not adopted widely enough in Ontario to currently be worth using as the basis for a voting channel. This leaves variations of both internet voting (from a computer or mobile device) and telephone voting (from a fixed line or a mobile phone) as the methods that are broadly feasible in Ontario.

4.3 AUTHENTICATION MECHANISM

The method or channel for transmitting the vote (internet, telephone, etc.) is only part of the picture. A far greater challenge is creating a system that is able to establish the voter's identity with confidence. In technical terms, the process of requiring a system user to prove his or her identity is referred to as *authentication*. Authentication goes hand in hand with another process – *authorization* – which, once identity has been verified, determines the actions the user is permitted to carry out.

In network voting systems, voter authentication techniques can be divided into three main categories, depending on which of the following is used as the basis of the authentication security.

1. **Information** – the system asks for something that is only known to the voter and to the authentication, such as a SIN or Health Card Number. The voter has to keep this information secret from third parties.
2. **Credentials** – the voter has a credential that can only be possessed by him or her, without requiring the voter to send this credential to the authenticator (the voting system). For electronic authentication, this authentication method is often based on the use of PIN-protected 'smart' ID cards. Alternately, this could take the form of a physical ID card.
3. **Physical Characteristics** – The authenticator captures biometric data from the voter (such as a fingerprint) and verifies that they correspond with those stored in a database (e.g., Electoral Roll).

As with the previous overview of voting methods, it is clear that some of these authentication options are not currently viable for use in Ontario. There is no government ID that currently supports a digital certificate that could be used by a network voting system.[15] Additionally, the Ontario and Canadian governments do not store biometric data that could be used for voter authentication. This leaves a few viable options; the first three based on information in the form of passwords or personal information, the last based on credentials:

Use of a password. Each user is provided with a user ID or login and an associated password. The login is a claim of the user's identity, and the password is the evidence supporting the claim. The password is typically a string of characters (letters or numbers) that is used both to prove the voter's identity and to grant access to the system. This password serves as a shared secret between the user and the system, which then checks the voter's eligibility to access the ballot.

Use of secret personal data. The Electoral Authority must have access to personal data for each voter, which the voter enters in order to get access to the system. The data itself can include, if applicable, the name of the voter, their address, their date of birth, their ID number, mobile phone number, email address, etc. Security increases as the data used for authentication becomes more secret. Due to the limited range of personal data that Elections Ontario stores or has access to for each Elector, this kind of authentication *alone* would not offer the level of security required for network voting in Ontario. Use of personal data can, however, be used in combination with password authentication to help strengthen the overall confidence level.

Third-party authentication systems. Authentication is delegated to a third-party system such as a government web site or an online banking site. The voter signs on to the third party site, which then shares enough identity information with the voting system to confirm voter eligibility and grant access the electronic ballot. Unfortunately, there is no system that is currently integrated with Elections Ontario systems and the complexities of such an integration would be too great to implement for a pilot.[16]

Use of physical ID (drivers licence, passport) to prove identity. This can only be done in person at a polling station. Since this only proves the voter's identity to a human being and not to the system itself, it also requires a further mechanism for authorizing the voter's use of the system to cast a ballot.

5. RESEARCH FINDINGS

The previous section gave an overview of the basic components and flow of a network voting system. It described the methods that can be used to cast a ballot and the mechanisms that can be used to establish voter identity. It also gave an overview of the voting methods and authentication mechanisms that are not currently feasible in Ontario. The following section presents the findings of detailed research into the ten remaining feasible methods and mechanisms.

A MATRIX RELATIONSHIP

THE VOTING METHODS and authentication mechanisms described in the previous sections can combine to create a matrix of potential network voting *scenarios*. The diagram below illustrates the full range of possible combinations and identifies the ten scenarios that were the subject of research:

Combinations that are not possible in a real environment are marked **N/A.**

Combinations that are not feasible for implementation in Ontario are marked **OOS** (out of scope).

The remaining feasible scenarios are numbered **1** through **10**.

	Physical ID	**Digital certificates**	**Passwords**	**Personal data**	**Third –party systems**	**Biometrics**
On-site computer voting	**1**	OOS	**3**	OOS	**8**	OOS
On-site telephone voting	**2**	N/A	**4**	OOS	N/A	OOS
Remote telephone voting	N/A	N/A	**5**	OOS	N/A	OOS
Remote computer voting through the Internet	N/A	OOS	**6**	OOS	**9**	OOS
Remote mobile phone voting through the Internet	N/A	OOS	**7**	OOS	**10**	OOS
Remote mobile phone voting through SMS	N/A	N/A	OOS	OOS	OOS	N/A
Remote Digital TV voting through the Internet	N/A	N/A	OOS	OOS	OOS	N/A

Voting methods based on SMS or Digital TV, and authentication options based on Digital Certificates, or use of Personal Data and Biometrics were eliminated from detailed research due to their lack of applicability in Ontario. These technologies and approaches were deemed either too risky or simply infeasible.

Each of the ten scenarios was researched in detail, with emphasis on their individual advantages, disadvantages, and risks. Each scenario was then scored against the principles and constraints that are discussed in Sections 2 and 3, above:

1. On-site, computer-based voting with authentication based on physical identification
2. On-site telephone-based voting with authentication based on physical identification
3. On-site computer-based voting through the internet with password-based authentication
4. On-site telephone voting with password-based authentication
5. Remote telephone voting with password based authentication
6. Remote computer voting through the internet with password-based authentication
7. Remote mobile phone voting through the internet with password-based authentication
8. On-site computer-based voting with authentication based on existing third-party systems
9. Remote computer-based voting through the internet with third party authentication
10. Remote mobile phone-based voting through the internet with third party authentication

RESEARCH METHOD

The research conducted a detailed review of Network Voting literature and research into recent implementation of Network Voting in Europe, the United Kingdom, Australia, and the United States. Based on this research, the advantages, disadvantages, and risks particular to each of the ten scenarios were documented and each scenario was evaluated against the eight measurable principles defined above in Section 3. The results were documented in the form of relative scoring.

5.1 SCENARIO 1: ON-SITE/ COMPUTER/ INTERNET/ PHYSICAL

On-Site, Computer-Based Voting With Authentication Based on Physical Identification

In this scenario, ballots are cast on-site using a variation on a desktop computer. Voters attend the polling place and show proof of identification to a poll worker. This identification can be any document accepted by the electoral authority; usually a government issued photo ID, such as a passport or driver's licence. The poll worker then validates the eligibility of the voter by checking their identity against a poll book. If the voter is eligible, the poll worker will grant the voter access to the voting device, using an approved authorization method, such as a programmable Smart Card. This scenario also allows voters to print a secure ballot receipt once their vote has been cast electronically to serves as a physical 'proof' for the voter.

If this scenario is to be combined with a remote voting channel (such as those described in Scenarios 5, 6, and 7), the polling place will require access to a real-time centralized electoral list so that voters can be prevented from casting multiple votes.

Pros

- On-site voting with physical identification provides the most secure mechanism for identifying and authorizing voters.
- Provides the highest level of security attainable: voting electoral authorities control the computers, and networking can be private.
- Allows Elections Ontario to control the physical and computing environments in order to provide high levels of usability and accessibility.

Cons

- Introduces complexity for Elections Ontario people, processes, and systems.
- Requires a significant logistics effort to prepare, deploy and decommission the network voting equipment.
- Requires specialized training for poll workers, support staff, technical teams, et cetera.
- Voters are still required to visit a polling location to cast a ballot.

Risks

- Dependent on the power and networking infrastructure/coverage that exists in each polling place.
- Dependent on a central electronic voter list to ensure one vote per voter. There are alternatives to a central list, but they limit the convenience of this scenario if combined with remote voting.

5.2 SCENARIO 2: ON SITE/ TELEPHONE/ PSTN/ PHYSICAL

On-Site Telephone-Based Voting With Authentication Based on Physical Identification

As in Scenario 1, voters attend a polling place and show proof of identification to a poll worker. The poll worker will then validate the eligibility of the voter by checking their identity against a poll book. If the voter is eligible, the poll worker will grant the voter access to the voting device, which, in this case, is a telephone.

Telephones used for casting votes can have multiple physical formats (depending on which technologies are available), and multiple models can be combined in a single polling place. The four basic telephone systems supported in this scenario are: Standard PSTN, Standard Cellular, SIP, and VOIP.

As telephones can only accept numeric input, authorization is limited to the use of a Voter Identification Number (VIN) that will activate the audio ballot. This unique identifier may be pre-printed and presented to the voter in a sealed envelope, or the poll worker may select and assign the voter a VIN from a pre-printed list of available numbers.

Telephone voting cannot provide a receipt of the ballot cast and, as a result, cannot provide the same level of individual verifiability that a computer can offer (through use of a printer).

If this scenario is to be combined with a remote voting channel (such as those described in Scenarios 5, 6, and 7), the polling place will require access to a real-time centralized electoral list so that voters can be prevented from casting multiple votes.

Pros

- On-site physical ID provides the best mechanism for identifying and authorizing voters.
- Security can be controlled well, with the exception of full end-to-end protection (see cons).
- Usability and accessibility can be very good for voters with visual disabilities.
- Telephone voting is the least expensive way (in terms of logistics and costs) to provide network voting at polling places; however, on the server side, its scalability is far lower than with on-line voting (i.e. the same server can support more on-line voters than telephone voters).

Cons

- On-site telephone voting requires a significant logistics effort to prepare, deploy, and decommission the network voting equipment, check telephone lines, cellular coverage, and networks (especially if using VOIP).
- Requires specialized training for poll workers, support staff, and technical teams with spare units, et cetera.
- Voters are still required to visit a polling place to cast a ballot.

- End-to-end security cannot be achieved without a big toll on usability: although the voting terminals are controlled by the electoral authorities, data leaving the telephone is not protected from external attacks that may happen in the network (PSTN, cellular, etc.) or internal attacks inside the IVR system.
- Not accessible for voters with auditory or severe motor disabilities.
- The process of casting a ballot takes much more time when compared to a computer-based system.

Risks

- Dependent on the telephone infrastructure/coverage that exists in each polling place, and on power and networking infrastructures if using VoIP.
- Possibility of man-in-the-middle attacks or voting session spoofing while data is on the PSTN.
- Dependent on a central electronic voter list to ensure one vote per voter. There are alternatives to a central list, but they limit the convenience of this scenario if combined with remote voting.

5.3 SCENARIO 3: ON SITE/ COMPUTER/ INTERNET/ PASSWORD

On-Site Computer-Based Voting Through the Internet with Password-Based Authentication

As in Scenarios 1 and 2, voters attend a polling place to cast their ballot on-site; however, in this scenario, voters will use *password authentication* in place of physical ID. This password based authentication process allows voters to go directly to the voting terminal without showing proof of ID to a poll worker. Instead, the voter enters credentials themselves at the voting system by inputting a unique password distributed through the electoral authority's chosen delivery channel. This scenario allows for the use of any type of password system (login and password / VIN; traditional / one-time use), which is entered using either a peripheral or on-screen keyboard. The system itself then authenticates the voter and determines their eligibility to cast a ballot. This process ensures that each voter votes only once.

When using password based authentication, the chosen delivery channel for passwords must strike a balance between convenience and security, and specific controls must be provided to ensure that each voter obtains only one password. Delivery channels may include on-site pickup, physical mail, electronic distribution, one-time link, or through confirmation of personal data via call centre or online.

Once a password is received, the use of a keyboard as an input device in this scenario can cause accessibility challenges for some users; however, these can typically be overcome either through use of assistive input devices, or by enlisting the assistance of poll workers to input the password on behalf of the voter. In this way, poll workers are

required only to supervise the voting process and provide assistance to voters when requested.

As in Scenario 1, this scenario also allows voters to print a secure ballot receipt once their vote has been cast electronically to serves as a physical 'proof' for the voter.

Pros

- Computer voting enables a high level of security, as end-to-end protection can be ensured. Voting terminals are controlled and a private network can be used.
- Allows Elections Ontario to control the physical and computing environments in order to provide high levels of usability and accessibility.
- Accessibility issues regarding password input can be addressed with assistance from a poll worker.
- Password-based authentication does not require a centralized electoral list system to avoid duplicate voting (unless this scenario is combined with other channels).

Cons

- Requires a significant logistics effort to prepare, deploy, and decommission the network voting equipment.
- Requires specialized training for poll workers, support staff, and technical teams with spare units, et cetera.
- Requires a mechanism or procedure for delivering passwords to voters.
- The identification of voters relies on the security of the password delivery process, which is not as secure as a mechanism based on physical identification.
- Voters are still required to visit a polling place to cast a ballot, unless this option is combined with a remote voting scenario.

Risks

- Dependent on the power and networking infrastructures available in each polling place.
- Relies on the password delivery system to ensure voter identity and eligibility.

5.4 SCENARIO 4: ON SITE/ TELEPHONE/ PSTN/ PASSWORD

On-Site Telephone Voting with Password-Based Authentication

As in Scenario, 2, voters attend a polling location and cast their ballot on-site using a telephone system; however, like Scenario 3, password authentication allows them to go directly to the voting terminal without showing proof of ID to a poll worker. Voters enter their unique password (with assistance from a poll worker when required) and are authenticated by the system, which determines their eligibility to cast a ballot.

As described in Scenario 2, a telephone system will require a numeric password in the form of a voter identification number (VIN) that is used to authenticate the user and activate the audio ballot. This VIN must be distributed through a delivery channel that strikes a balance between convenience and security, and provided specific controls to ensure that each voter obtains only one VIN.

Telephone systems cannot provide a hard copy of the ballot cast.

Pros

- Provides medium to high level of security, but is unable to offer either a) full end-to-end protection or b) the security of physical ID (see cons).
- Usability and accessibility can be very good for voters with visual disabilities, if the poll workers can be used to assist these individuals with entering the password.
- Telephone voting is the least expensive way (in terms of logistics and costs) to provide network voting at polling places; however, on the server side its scalability is far lower than with on-line voting (i.e. the same server can support more on-line voters than telephone voters).
- Does not require a centralized electoral list system at the polling station to avoid duplicate voting, if used on its own or in combination with an integrated network voting channel.

Cons

- On-site telephone voting requires a significant logistics effort to prepare, deploy, and decommission the network voting equipment, check telephone lines, cellular coverage, networks (especially if using VOIP).
- It also requires specialized training for poll workers, support staff, and technical teams with spare units, et cetera.
- Requires a mechanism or procedure for delivering passwords/VINs to voters.
- Voter authentication relies on the integrity of the VIN delivery process, which is not as secure as a mechanism based on physical IDs.
- Voters are still required to visit a polling place to cast a ballot (unless this scenario is combined with a remote voting scenario).

- End-to-end security cannot be achieved without a large toll on usability: although the voting terminals are controlled by the electoral authorities, data leaving the telephone is not protected from external attacks that may happen in the network (PSTN, cellular, etc.) or internal attacks inside the IVR system.
- Not accessible for voters with severe auditory and/or motor disabilities.
- The process of casting a ballot takes much more time when compared to a computer-based system.

Risks

- Dependent on the telephone infrastructure/coverage that exists in each polling place, and on the power and networking infrastructures if using VOIP.
- Possibility of man-in-the-middle attacks or voting session spoofing while data is on the PSTN.
- Relies on the password delivery system to ensure voter's identity and authenticity.

5.5 SCENARIO 5: REMOTE/ TELEPHONE/ PSTN/ PASSWORD

Remote Telephone Voting with Password Based Authentication

In this scenario, electors can vote from any location, provided that they have access to a telephone, which can be a conventional phone, a mobile phone, or voice over IP (VOIP) from a computer or a telephone. Voters dial a toll free number, select their preferred language, and then type a predetermined password using the keypad. The system itself authenticates the voter and determines eligibility to cast a ballot. If the authentication is approved, the voter will gain access to an audio ballot.

As described in Scenarios 2 and 4, a telephone system will require a numeric password in the form of a voter identification number (VIN). This VIN must be distributed through a delivery channel that strikes a balance between convenience and security, and provided specific controls to ensure that each voter obtains only one VIN.

Telephone systems cannot provide a hard copy of the ballot cast.

Pros

- Provides a medium to high level of Security, but is unable to offer either a) full end-to-end protection, nor b) the security of physical ID (see cons).
- Usability and accessibility can be very good for voters with visual disabilities, provided that the VIN is of sufficient legibility for persons with disabilities, or that someone can read the VIN for them and/or type it on the telephone keypad (if needed).
- Voters can participate from any telephone, which are available in almost 100% of Ontario and can be used by voters of any level of technical knowledge.
- If a toll-free number is offered, then voters will not have to pay for the call.

- Denial-of-Service attacks are less effective in this scenario than for Scenarios 2 or 4, as there are many vulnerable segments (the links between each voter and the data centre) and each one transmits a small proportion of the total votes.
- If the link between a polling place and the data centre goes down, many votes are affected; whereas, if the line from a voter's home is affected, the impact is much less.

Cons

- Requires a mechanism/procedure to deliver VINs to voters.
- Voter authentication relies on the integrity of the VIN delivery process, which is not as secure as a mechanism based on physical ID.
- End-to-end security cannot be achieved without a large impact on usability: the voting terminals are not controlled by the electoral authorities, and data leaving the telephone is not protected from external attacks that may happen in the network (PSTN, cellular) or internal attacks inside the IVR system.
- Not accessible to voters with severe auditory and/or motor disabilities.
- Not as user-friendly as a computer based interface.
- The voting process takes more time when compared to a computer voting interface.
- Central infrastructure (the IVR system) does not scale up as well as a web infrastructure.
- Toll-free numbers are an added operational cost

Risks

- Phone lines needed for voting can be easily saturated if not sized accordingly.
- Possibility of man-in-the-middle attacks or voting session spoofing while data is on the PSTN.
- Relies on the password delivery system to ensure the voter's identity and authenticity.

5.6 SCENARIO 6: REMOTE/ COMPUTER/ INTERNET/ PASSWORD

Remote Computer Voting Through the Internet with Password-Based Authentication

In this scenario, electors can cast votes from any location, provided that they have a computer (with the appropriate software) and access to the Internet. Voters will usually access a voting website using a web browser and type a password that authenticates them to the voting system. The system will verify their identity and their eligibility to vote, and then display an online ballot. The authorization to access the voting system allows any kind of password-based system, not just numerical ones.

As with any remote voting system that relies on passwords for authentication, the delivery of the passwords must strike a balance between convenience and security. Specific controls must be used to ensure that each voter obtains only one password.

This scenario also allows voters to print a secure ballot receipt once their vote has been cast electronically to serves as a physical 'proof' for the voter. This scenario could be combined with an on-site voting channel if required. If remote computer voting is done in parallel with on-site computer voting, a centralized electoral list that can be accessed and updated from the polling station will be required to avoid duplicate voting.

Pros

- Remote computer voting allows a very high level of security, with the exception of the voter identification process (see cons).
- End-to-end security can be achieved through encryption, enabling protective measures against external and internal attacks.
- Usability and accessibility can be very high for voters with any type of disability, provided they are familiar with computers and have the required accessibility interfaces.
- Voters can participate from any available computer with Internet access, which means nearly 100% of Ontarians will have access. Voting could take place not just from home, but also from locations such as places of work, libraries, or internet cafés (which creates risks as well as opportunities).
- Only the central infrastructure is required; with no requirements for other components at the server or polling location level. This infrastructure can be made to scale up very efficiently when compared to other voting channels, especially telephone voting.
- Both online registration and the voting process can be very convenient and quick (often less than 5 minutes).

Cons

- Remote, password-authenticated voting requires a mechanism for delivery of passwords to voters.
- Voter authentication relies on the integrity of the password/VIN delivery process, which is not as secure as a mechanism based on physical identification documents.
- Voters may need to cover the costs related to internet access.
- Only voters who have access to and are familiar with computers can use this voting channel easily. The same applies to voters with disabilities: only those familiar with browsing the Internet will be easily able to vote.
- There is no control over the security or stability of the computers used by voters to cast their ballots (viruses, malware, etc.).

Risks

- Possibility of Denial of Service attacks, as voting servers are accessible via the internet.
- Lack of control over the specifications of voter's computers.
- Some segments of the population may not be enthusiastic to use this mechanism due to the digital divide:
    - Voters not used to computers.
    - Voters with disabilities who have not used to computers and/or who have no accessibility interfaces.
- Relies on the password delivery system to ensure voter identity and authenticity.

5.7 SCENARIO 7: REMOTE/ MOBILE PHONE/ INTERNET/ PASSWORD

Remote Mobile Phone Voting Through the Internet with Password-Based Authentication

In this scenario, voters can vote from anywhere, provided that they have a suitable (see below) mobile phone (which may require specific software) and access to the Internet. Once the appropriate application or website is accessed using the phone, voters will key in a password to authenticate. If the voter is eligible, the system will automatically display the voting options. Authorisation to access the voting system may be achieved using any kind of password-based system; however, numerical passwords are preferred, as not all mobile phones include a full keyboard.

As with previous password-based scenarios, passwords must be distributed through a delivery channel that strikes a balance between convenience and security, and provides specific controls to ensure that each voter obtains only one password.

The device used for casting votes can be almost any mobile phone, provided it can run either a custom-built application or an appropriate web browser. Given the limitations on screen size, CPU power, OS features and keyboard of many standard mobile phones, the devices most suited for this purpose are smart phones; however, the penetration rate of these devices is low when compared to the whole cellular market (usually <30%), and not all users are familiar with advances features, such as applications.

Whether voting is done using a web browser or custom application, voters need to cover the costs associated with an Internet connection. Also, accessibility mainly depends on the built-in capabilities provided by the device itself, which are very limited when compared to the options available for computers.

This scenario can be combined with an on-site voting channel if required. Depending on the on-site voting requirements, a centralized electoral list that can be accessed and updated from the polling station will likely be required to avoid duplicate voting.

In order to support individual verifiability, the system can be designed to provide a soft copy "receipt" that helps voters verify that their ballots were counted by the electoral authorities.

Pros

- Remote mobile Internet voting can off a very high level of security, with the possible exception of voter identification (see cons).
- End-to-end security can be achieved, enabling protective measures against external and internal attacks.
- Voters can vote anywhere a 2G or higher cellular network is available (>95% of the province).
- Mobile phones are less prone to malware or viruses than computers.
- Only the mandatory central infrastructure is required; no extra components are needed at the server or polling place level. This infrastructure can be made to scale up very efficiently (when compared to other voting channels).

Cons

- Usability and accessibility are marginal and depend totally on the features of the cellular phone. Only newer smart phones offer truly acceptable levels of interface usability.
- Requires a mechanism/procedure to deliver passwords to voters.
- The identity of voters is based on the delivery process of passwords, which is not as secure as the mechanism based on physical ID.
- Voters will need to cover the costs related to Internet access.
- Only for voters who are used to browsing the Internet and/or employing applications from mobile phones.
- There is the possibility of Denial of Service attacks, as voting servers are accessible via the internet.
- Requires extra effort to develop for multiple device platforms (including corresponding impact on testing and support).

Risks

- Possibility of Denial of Service attacks.
- Some portions of the population would less willing to use this mechanism:
- Voters using standard mobile phones.
- Voters not familiar with smart phone functionality.
- Voters with disabilities.
- Having multiple applications for various phones/browsers increases support demands and related costs.
- Relies on the password delivery system to ensure voter identity and authenticity.

5.8 SCENARIO 8: ON SITE/ COMPUTER/ INTERNET/ THIRD PARTY

On-Site Computer-Based Voting with Authentication Based on Existing Third-Party Systems

In this scenario, voters attend a polling place and go directly to the voting terminal, where they will authenticate themselves to the voting system through a third-party website (such as ServiceOntario). After voters have been identified, they will be redirected back to the voting portal where they will be authorised to vote.

Poll workers do not have to perform any action in this scenario except to supervise the voting process and assist voters when requested.

Because authentication involves interaction with a third party site, both security and accessibility become dependent upon the standards set for that site. It is, therefore, of critical importance that these be trusted, highly secure third party sites that provide necessary accessibility options.

This scenario can be combined with a remote voting channel without the need for a centralized electoral list in the polling stations, as the control on voters to avoid duplicate voting is done by the voting system itself.

As in other computer based scenarios, this scenario also allows voters to print a secure ballot receipt once their vote has been cast electronically to serves as a physical ‘proof’ for the voter.

Pros

- Security is high, as end-to-end protection can be ensured, voting terminals are controlled, and a private network can be used.
- Usability and accessibility can be very high depending on the configuration of the voting kiosks and standards of the third party authenticator (this excludes password entry, which may require assistance from a poll worker).
- Does not require a centralized elector’s list to avoid duplicate voting. The voting system itself manages this.

Cons

- Requires a significant logistics effort to prepare, deploy and decommission the network voting equipment.
- Requires specialized training for poll workers, call centre support, and technical teams with spare units, et cetera.
- Requires integration with third party sites. The integration would require detailed assessments of third party security levels and procedures.
- The identification of voters is based on third party systems, which must be trusted and are not as secure as a mechanism based on physical IDs.

- Only voters with access to these third party systems could vote using the networked system.
- Voters are still required to visit a polling place to cast a ballot, unless this option is combined with a remote voting scenario.

Risks

- Dependency on polling places' power and networking infrastructures.
- Relies on third party systems to ensure voter's identity and authenticity.
- Participation limited to voters that can access the third party systems.

5.9 SCENARIO 9: REMOTE/ COMPUTER/ INTERNET/ THIRD PARTY

Remote Computer-Based Voting Through the Internet with Third Party Authentication

In this scenario, voters can vote from anywhere provided that they have a computer (with the appropriate software) and access to the Internet. They will authenticate themselves to the voting system through a trusted third party website. After voters have been identified, they will be redirected back to the voting portal where they will be authorised to vote.

As stated in Scenario 8, this authentication mechanism implicitly implies that the electoral authorities trust the mechanisms used by the participating third parties for authenticating their users. Therefore, some type of assessment and/or audit should be considered to validate that the process used to identify users is sufficiently secure.

Pros

- Security can be very high, although the system is trusting third party authentication mechanisms and the computers from voters (see cons).
- There is no need to set up complex processes for delivering voting credentials (e.g. passwords) to voters, as third parties take care of this.
- End-to-end security can be achieved, enabling protection measures in front of external and internal attacks.
- Usability and accessibility can be very high for voters with any type of disability, provided they are used to computers and have the required accessibility components; however, third parties must also provide accessible sites.
- Voters can participate from any available computer with Internet access, which means close to 100% of the region. This includes places of work, libraries, Internet cafés, et cetera.
- Only the mandatory central infrastructure is required; no extra components needed at server or polling place level. This infrastructure can be made to scale up very efficiently (when compared to other voting channels).
- The voting process can be very convenient and fast (less than 5 minutes).

- Does not require a centralized elector's list system to avoid duplicate voting. The voting system itself manages this.

Cons

- Requires different integrations with third party sites. The integration would require detailed assessments on security levels and procedures followed by the third party.
- The identification of voters is based on third party systems, which must be trusted and are not as secure as a mechanism based on physical IDs.
- Only voters with access to these third party systems could vote using the networked system.
- Voters may need to cover the costs related to Internet access.
- Only voters accustomed to using computers, including those with disabilities, can use this voting channel.
- Denial of Service attacks are easier in this scenario.
- There is no control over the computers used by voters to cast their ballots.

Risks

- Denial of Service attacks and the lack of control over voters' computers.
- Some portions of the population would less willing to use this mechanism:
- voters who are not comfortable using computers.
- voters with disabilities not used to computers and/or with no accessibility components.
- voters with no relationship to any of the third parties used for authentication.
- Relies on third party systems to ensure voter's identity and authenticity.

5.10 SCENARIO 10: REMOTE/ MOBILE PHONE/ INTERNET/ THIRD PARTY

Remote Mobile Phone-Based Voting Through the Internet with Third Party Authentication

In this scenario, voters can vote from any location provided that they have a mobile device with a web browser and access to the Internet. They will authenticate themselves to the voting system by selecting a third party website, which will request them to identify themselves. After voters have been identified, they will be redirected back to the voting portal where they will be authorised to vote.

As stated in Scenarios 8 and 9, this authentication mechanism implicitly implies that the electoral authorities trust the mechanisms used by the participating third parties for authenticating their users, and that such third party site is compatible with the accepted mobile devices.

Determination of voter eligibility is done at the voting system (i.e. the third party only takes care of identifying the user). This approach avoids having to share the electoral roll with the third parties.

This scenario presents some usability issues because it is rather complicated to navigate through different websites with a mobile phone, especially when one takes account that some third party sites may not be adapted to mobile devices.

Pros

- Voters can participate using certain mobile devices, and they can be located anywhere a 2G or newer cellular network is available.
- Security can be very high, although the system is trusting third party authentication mechanisms and the mobile terminals from the voters (see cons).
- Mobile phones are less prone to malware.
- Only the mandatory central infrastructure is required; there are no extra requirements for other components at the server or polling location level. This infrastructure can be made to scale up very efficiently when compared to other voting channels.
- There is no need to set up complex processes for delivering voting credentials (e.g. passwords) to voters, as third parties take care of the delivery.
- Does not require a centralized electoral list system to avoid duplicate voting. The voting system itself manages this.

Cons

- End-to-end security cannot be achieved due to limitations of the network and use of third parties, opening the door to internal attacks.
- Usability and accessibility depend totally on the features of the cellular phone. Only the newer smart phones offer acceptable interfaces in terms of usability, but accessibility is very limited.
- Voters will need to cover the costs related to Internet access.
- Only voters who own these types of devices can use this voting channel.
- Denial of Service attacks are easier in this scenario as the access to the voting servers is based on standard internet portals.
- Requires extra effort to develop for multiple device platforms (including corresponding impact on testing and support).
- Requires integration with third party sites. The integration would require detailed assessments on security levels and procedures followed by such third parties.
- The identification of voters is based on third party systems, which must be trusted and are not as secure as the mechanism based on physical IDs.
- Only voters with access to these third party systems could vote using the networked system.

Risks

- Possibility of Denial-of-Service attacks.
- Some portions of the population would less willing to use this mechanism:

- citizens who do not own smart phones.
- voters with disabilities.
- voters with no relationship with any of the third parties used for authentication.
- Many options increase the difficulty and cost of supporting them.
- Relies on third party systems to ensure voter's identity and authenticity.

5.11 RESEARCH RESULTS: SHORT LIST OF SCENARIOS

As an outcome of the network voting research, Scenarios 7, 8, 9, and 10 were eliminated from consideration, for the following reasons:

Scenario 7, which is based on a mobile Internet / smart phone platform, scores poorly against accessibility criteria.

Scenarios 8 and 9, which score comparably to other computer voting scenarios, must be eliminated because a third-party authentication system or service is not available in Ontario at present. This option should be explored in the future, however, as conditions change.

Scenario 10, which is also based on a mobile Internet platform, has a poor accessibility score.

Six of Ten Scenarios Eliminated

Scenarios 3 and 4, which scored well in the evaluation, were eliminated through consultation, as requiring electors to pre-register and bring a password to a polling station created an unnecessary barrier without delivering a substantial benefit to voters.

Four Scenarios (1, 2, 5, and 6) are therefore still potential candidates for a pilot and form a Short List of scenarios that are further evaluated in this Business Case document:

Short List of Four Channels

SCENARIO	LOCATION	PLATFORM	AUTHENTICATION
1	On-site	Computer	Physical ID
2	On-site	Telephone	Physical ID
5	Remote	Telephone	Password
6	Remote	Computer	Password

Since each of these scenarios delivers a unique set of advantages, this Business Case evaluates how these four channels can be combined into a single model that:

- includes on-site and remote telephone voting;
- includes on-site and remote computer voting;
- uses physical ID to authenticate on-site voters;
- uses a combination of pre-registration and a password authentication for remote voting; and
- offers a paper ballot in parallel using the current method of authenticating voters.

Advantages of On-Site Network Voting

By providing on-site network voting options, this model is able to authenticate voters using a method that is not only the most secure, but also one that voters are familiar with. A voter would not need to pre-register for network voting before voting on-site by computer or telephone; they simply need to present their identification before a poll worker gives them access to the voting device. While this is simplest for the voter, it is also relatively complex for Elections Ontario in terms of poll worker training, rollout of infrastructure, and system development.

Advantages of Remote Network Voting

By providing remote voting options, which can only be authenticated using a password-based process, this model is able to deliver the unique benefits of remote voting. Voters can vote in their homes or workplaces and they can use either the telephone or the internet, depending on which channel is more convenient or accessible to them, and they can do so very quickly.

The next section describes the details of how these four channels can be implemented in an Elections Ontario pilot.

6. WALKTHROUGH OF THE SHORT-LISTED SCENARIOS

This section gives a process-based review of how the four short-listed channels could be implemented in an Elections Ontario pilot. The details of how these four channels could be implemented are based on an evaluation of the current Elections Ontario business. The processes described here are designed to support the core election principles selected to guide this initiative and to operate within the needs and constraints specific to the current Ontario context.

THE RESEARCH FINDINGS identified a short list of four network voting channels: on-site telephone voting, on-site computer voting, remote telephone voting, and remote computer voting. To provide a clear picture of how these four channels could be implemented in an Elections Ontario pilot, this section describes their implementation in terms of the five steps in the voting process:

1. **Registration & Authentication**

   The features and processes required to set up the list of electors, register them for network voting, prove their identity, and validate their eligibility for voting.

2. **Voting**

   The features and processes required to allow voters to cast ballots using network voting channels.

   There are three key subjects: onsite voting; remote voting; and the electronic poll book.

3. **Vote storage**

   The processes required to securely and accurately manage the storage and management of ballots in the network voting system after they have been cast.

4. **Tabulation**

   The features and processes required to tabulate and report results in the Network Voting environment and merge them with results from the conventional stream after the voting period has closed.

5. **Audit**

   The features and processes that must exist to support external audit.

   The ability to audit and review the network voting system is critical to establishing the transparency recommended by this business case.

As it could be possible to introduce all four channels in a pilot context, the following section provides a view of how they could be implemented in an integrated model. The feasibility of each individual channel will be assessed in subsequent sections.

Overview

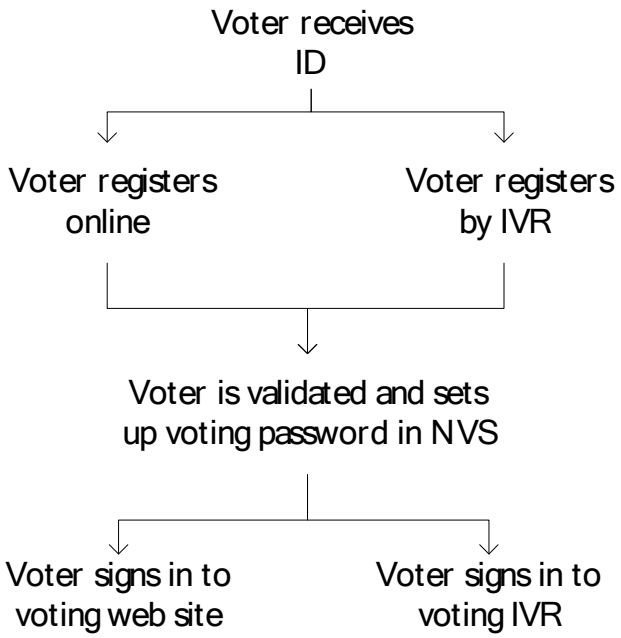
New Processes & Technologies

Provided below is an overview of this integrated model, organized according to the five above steps. For each step, the overview describes, at a high-level, how the various stakeholders (voters, poll workers, Elections Ontario head office staff, etc.) will interact with the new processes and technologies required to support network voting. Further discussion on each step of the voting process is then provided in the proceeding sub-sections.

While references may be made to specific key requirements, risks, or risk mitigation strategies, these subjects are dealt with in greater detail in subsequent sections of this document.

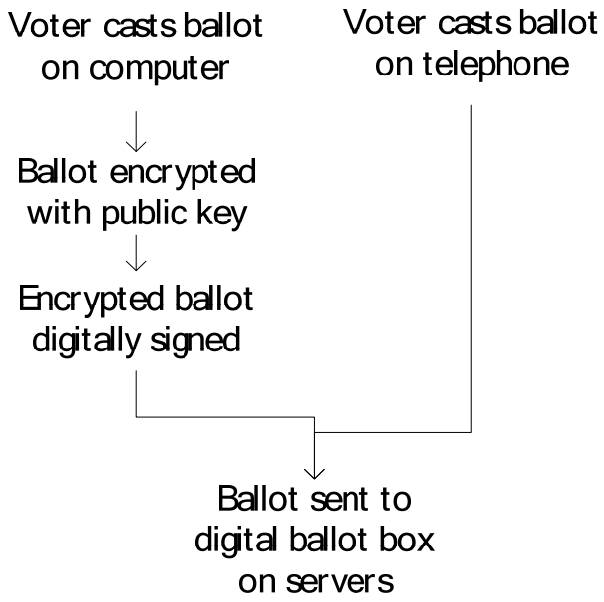
Registration & Authentication

1. All Electors on the preliminary list of electors receive a network voting registration letter that includes a secure numeric Elector ID and instructions for accessing a remote network voting registration web site.
2. Electors who choose to register for remote network voting will visit the web site and enter their Elector ID and their date of birth to register. For added security, their driver's license number can be used to establish their identity. A second card could also be mailed at this stage to provide the voter a secure second PIN before proceeding to the next step.
3. Once authenticated, the system will validate their eligibility and allow them to set up a secure password to use for voting. Alternatively, electors who do not have easy access to the Internet can call a toll-free number to perform the same steps using an IVR interface that connects to the same backend system.
4. Once the advance poll period begins, voters who have registered for remote voting can log in to either the voting web site or the voting IVR system using their Elector ID and password.



Voting

5. Once a remote voter has been authenticated on the voting web site, he or she will cast a ballot by making a selection from an online screen. Voters who use the telephone will make their selections using an automated menu system. Both of these options must be optimized for usability and accessibility in order to provide the best user experience.
6. After voting on one of these channels, the voter will be struck from the voter's list and receive a receipt that will allow them to verify the inclusion of their ballot in the final election results.
7. The voters list could be managed through an online, real-time process to prevent the possibility of double-voting via multiple channels and to keep the Network Voting system up to date with revisions. Alternatively, voters could be locked in to the remote channels once they register in order to prevent them voting twice.

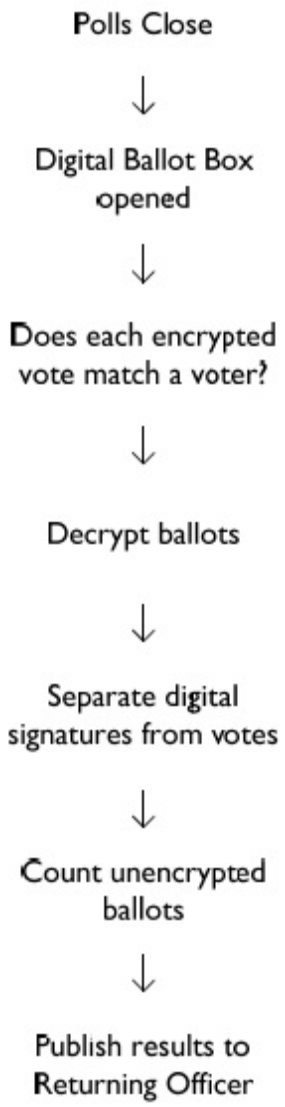


Vote Storage

8. After a ballot has been cast on either the telephone or computer channels, it will be stored in a secure server environment that is subject to stringent physical and application security measures, as well as availability and performance requirements.
9. The ballot will be securely encrypted so that its contents cannot be read while stored in the ballot box.

Tabulation

10. Once the voting period has closed, the electronic ballot boxes will be moved to an isolated and secure counting environment.
11. Before decryption, the system will check that all the votes contained in the ballot boxes are cast by eligible voters.
12. The ballots will be decrypted by authorized Elections Ontario officials who each possess a portion of the key required to decrypt the ballots
13. Once decrypted, the ballots cannot be associated with a voter.
14. The system will count valid ballots and distribute combined Network Voting results to the Returning Officer, who will include them in the official count.



Audit

15. The system must allow the Network Voting Management Board to carry out new decryption and tabulation processes if required, under the supervision of independent auditors.
16. The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes. Auditors should be able to operate with the decrypted votes and obtain human-readable results that can be compared to the ones generated by the system.
17. The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes, including the authenticity of the software, the integrity of the system, the integrity and authenticity of the generated logs, etc.

6.1 VOTER AUTHENTICATION

The ability to securely and definitively establish an elector's identity is one of the core principles driving this initiative. It is a fundamental democratic requirement, and would therefore be a critical technical and procedural component of a network voting pilot. For voting in person at a polling location, the means of authentication would be the current one: presentation of approved physical identification to a poll worker; however, remote voting presents a more complex challenge.

As Elections Ontario is currently unable to leverage any established form of electronic authentication*, it must (at least for the pilot) implement its own, self-reliant means of authenticating voters.

This section provides the process flows and exceptions for three voter authentication processes:

- **Standard remote authentication**, in which electors register in advance for remote network voting channels using proof of identification;
- **Alternative remote authentication,** in which electors register in advance using a postal-based process with two separate mailings; and
- **Supervised authentication**, in which an Elections Ontario poll worker verifies a voter's identity and authorizes the voter to use a voting device.

* One of the easiest ways for Elections Ontario to authenticate a remote voter's identity would be to challenge them to provide information that is only known to the voter and to Elections Ontario.

However, Elections Ontario only has access to a limited range of personal data for voters; most of which is not secret and, therefore, not secure.

Alternatively, Elections Ontario could leverage a secure means of remote authentication provided by a third-party government agency. However, such a mechanism is not currently mature enough or adopted widely enough to be suitable for integration with a Network Voting system.

Standard Remote Authentication

To cast a ballot using remote network voting channels (telephone and computer), voters would authenticate themselves through a combination of unique ID and password. To do this, they must first register for the channel.

While balancing the electorate's need for a simple process, the strongest means available to Elections Ontario would be to confirm the elector's identity *during* the registration process so that, when the time comes to log in and vote, the credentials are as secure as possible.

Each step of the process must, therefore, strike a balance between presenting as few barriers to the voter as is reasonable, and establishing voter identity through as secure a means as is possible, given the external constraints.

The process flow would be as follows:

1. Elections Ontario generates the list of electors and this list is imported into the network voting system and made available to electronic poll book (ePB) devices and software.
2. The system generates a unique identifier for each voter on the list.
3. Elections Ontario generates a letter that contains the unique identifier and distributes it by post to each elector. This letter should be as secure as possible.**

   ** Due to timeline constraints, it will likely not be possible to leverage the existing Notice of Registration Cards.

4. The elector registers online by visiting a secure web site provided in the letter or card (the registration site). The elector signs in with the unique ID provided on the card and authenticates (establishes their identity) by entering information that is typically known only to the elector and the Government, such as:
   - Date of Birth (DOB); in combination with
   - a Government-issued ID number, such as Driver's Licence (DLN) number or the last four digits of the Health Care Number (HCN).†

   †DLN may be sufficient for the pilot; however, a more universal ID source should be used in future.

5. If the authentication is successful, the system allows the voter to create **voting credentials**, which consist of the same unique identifier plus a secure password. The password, which is set up and delivered to the voter in real time at time of registration could consist of either:
   - a password selected by the elector (which must meet complexity/strength requirements); or
   - a random password generated by the system.
6. Once the voting period is open, the voter votes using their preferred network voting channel and authenticates using the credentials set up in the previous steps (Elector ID and personal password).
7. If the voter chooses to vote by computer, he or she signs in to the secure voting web site (the voting site) with their unique voter ID and the secure password created in step 5.
   i. The voter casts a ballot using the online interface.
   ii. The system strikes the voter from the voter's list automatically.

8. If the voter chooses to vote by telephone, he or she calls the toll-free voting number and authenticates by entering their unique voter ID and the secure password created in step 5.
    i. The voter casts a ballot using the IVR interface.
    ii. The system strikes the voter from the voter's list automatically.

The following nine cases are exceptions that could occur during the standard flow described above and would therefore require special handling:

1. A voter forgets his or her password.
2. A voter forgets/misplaces his or her unique identifier.
3. A voter claims his or her credentials have been used by another person (impersonation).
4. A voter wishes to vote using a different channel.
5. New voters are added to the list of electors after the original credentials are sent (if allowed).
6. Voters are removed from the list of electors after credentials are sent.
7. Package not received.
8. Package cannot be read.
9. Voter does not have required government ID, or authentication using government ID fails.

The following table provides an overview of how exceptions to the remote authentication and registration process can be handled at three different points in the process:

- Before voting starts;
- While voting is open but before the credential has been used; and
- After the credentials have been used to vote.

The exception handling proposed in this section assumes that a real-time electronic poll book is in place with some degree of integration between Elections Ontario systems and the network voting system.

	Before voting starts	Voting open but before the credential is used	The credentials have been used to vote	
1	Voter accesses the registration site again with the original data and resets the password.	Voter accesses the registration site again with the original data and resets the password.	No impact.	Forgot password
2	The voter contacts the help desk and authenticates (using DOB, DLN, etc.) The voter attends the Returning Office OR The voter is sent a second package	The voter contacts the help desk and authenticates (using DOB, DLN, etc.) The voter attends the Returning Office OR The voter is sent a second package	Treat as an impersonation (see below).	Forgot identifier
3	The voter contacts the Returning Office.	The voter contacts the Returning Office.	The voter contacts the Returning Office.	Impersonation claim.
4	No impact. The voter can vote using any channel and is crossed off the electronic list after having done so.	No impact. The voter can vote using any channel and is crossed off the electronic list after having done so.	If used, the electronic Poll book could have an interface option to cancel the original vote. This assumes that the identity is linked to the ballot (which requires that the ballot is encrypted).	Voter wishes to vote using a different channel.
5	New letters are printed and sent automatically. OR New voters need to apply personally as if they had lost their unique ID.	New letters are printed and sent automatically. OR New voters need to apply personally as if they had lost their unique ID.	N/A	New voters are added to the list of electors after original credentials are sent.
6	Help desk cancels voter credentials so they cannot vote.	Help desk cancels voter credentials, so they cannot vote.	Ballots related to these voters are cancelled (without affecting their privacy).	Voters are removed from the list of electors after credentials are sent.

	Before voting starts	Voting open but before the credential is used	The credentials have been used to vote	
7	The voter calls the help desk, who will either • send new card; or • instruct the voter to attend a returning office if they have changed address	The voter calls the help desk, who will either • send new card; or • instruct the voter to attend a returning office if they have changed address	N/A	Registration package not received.
8	Voter registers physically at a Returning Office.	Voter registers physically at a Returning Office.	N/A	Registration package cannot be read.
9	Voter registers physically at a Returning Office.	Voter registers physically at a Returning Office.	N/A	Voter does not have required government ID.

Alternative Remote Authentication

Instead of using government ID to confirm the voter's identity during the registration, a second package containing a second PIN could be used to help assure that the person registering is in fact the elector. As a result, there is some additional deterrent to impersonation risk (as it is more difficult to intercept two pieces of mail than one). Without using a strong shared secret, voters prove their identity using only the fact that they reside at their mailing address. The overall security is reduced, but the process is made accessible to all electors.

The process would function as follows:

1. Elections Ontario generates the list of electors and this list is imported into the network voting system and made available to electronic poll book (ePB) devices and software.
2. The system generates a unique identifier for each voter on the list.
3. Elections Ontario generates a letter that contains the unique identifier and distributes it by post to each elector. This letter should be as secure as possible.**
4. The elector registers online by visiting a secure web site provided in the letter (the registration site). The elector signs in with the unique ID provided on the card and supports their identity claim by entering their date of birth.

5. The elector creates a secret password to during voting.
6. The system generates a second number (a VIN) and a second letter is printed and mailed.
7. Once the elector receives the second letter, they are ready to vote online (or by telephone).

** Due to increased timeline pressure, it will likely not be possible to leverage the existing Notice of Registration Cards.

While checking identity using the same method twice adds very little additional security, it can add the *perception* of greater security and therefore contribute to the mitigation of impersonation risk.

ADVANTAGES

However, the chief advantage of using a second mailing to provide the elector with a second unique identifier is that it would allow Elections Ontario to implement a process that is more universally accessible and does not require electors to possess a drivers licence, as current constraints on available shared secrets would dictate. A process that effectively repeats the initial mailing with a follow up package is also less technically complex than integrating authentication based on any third-party system or data element.

DISADVANTAGES

The chief disadvantage of using a second mailing is that it greatly increases the time that must elapse between registering online and setting up credentials. In the standard remote process described in the previous sub-section, it is instantaneous. In this alternative process, the wait time between registering online and receiving the final voting credential in the mail could be up to one week. This reduces the potential voting time by up to a week, and forces a shorter window for voter registration, as an early cut-off must be imposed to allow time for second letter to arrive. Delay will likely reduce adoption, especially for electors living in areas without home delivery. In fact, it is possible that the card arrives so late that voters will have very little or no time left to vote.

Supervised Authentication

Voters who visit a polling station to vote using a Network Voting channel would be authenticated by Elections Ontario staff. A poll worker would check the voters physical ID, verify their eligibility, and authorize them to use the voting device. Use of physical ID is the strongest means of authentication available; however, it would require poll staff to facilitate a second manual step: authorizing the voter to use the voting device.

The process flow would be as follows:

1. Elections Ontario generates the list of electors and this list is imported into the network voting system and made available to the electronic poll book (ePB).

2. The system generates a unique identifier for each voter on the list.
3. The voter arrives at polling station with physical ID.
4. The poll clerk verifies the voter's identity manually and checks eligibility in a centralized electoral list using the ePB.
5. If the voter prefers to vote using the paper ballot, the poll clerk strikes the voter from the list using the ePB software.
6. If the voter prefers to vote by computer, the poll clerk codes a smartcard using the ePB, and handles it to the voter. The smart card now contains the voter's unique identifier.*
    i. The voter inserts the smart card into the voting computer, which authenticates the voter using the unique ID stored temporarily on the card.
    ii. The voter makes selections using the on-screen ballot
    iii. To decline/intentionally spoil the ballot, the voter uses the computer interface to over or under vote.
    iv. The voter casts the ballot using the online interface
    v. The voter is automatically struck from the voter list as soon as the ballot is submitted.

* Only the voting computer can read the contents of the card.

i. If the voter prefers to vote by telephone, the poll clerk uses the ePB software to generate a unique voter identification number (VIN) that will be used to authenticate the voter through the IVR system.** Note that there is a single system for remote an on-site voting, and the identifiers must be the same for all the channels.

ii. The poll clerk prints the VIN and hands the printout to the voter.

* *The VIN includes: the voter's unique ID plus a random pass code. This is typically up to 16 digits in length.

i. The voter enters the VIN using the telephone's keypad. Assistance could be provided for voters with disabilities, through an assistive device or poll worker assistance.

ii. The voter makes selections using the IVR menu.

iii. To decline/intentionally spoil the ballot; the voter uses the IVR to over or under vote.

iv. The voter casts the ballot using the IVR.

v. The voter is automatically struck from the voter list (as soon as the ballot is submitted).

The following four cases are exceptions that could occur during the standard flow described above and would therefore require special handling:

	Exception	Handling
1	The ePB shows that the voter has already voted.	The Returning Officer will decide if the previous ballot is to be cancelled using the ePB and the voter is allowed to vote again.
2	The smart card assigned to the voter does not work.	The ePB allows a new one to be generated. There is no impact.
3	A voter not in the electoral roll wants to be added and vote using the network system. (permissible)	• The voter is added to the voter list using the ePB (by a revisions officer), but can only vote using paper. (preferred) • If no paper ballots: there are options for adding voters and issuing new credentials in real time.
4	There is no Internet connection. The ePB cannot be used, smart cards cannot be created, computer votes cannot be cast, and voters cannot be struck from the list. **Note** that the risk of this happening can be mitigated through the use of redundant internet connections.	Voters will not be able to use the network voting system If there is paper ballot, voters should either: 1. not be allowed to vote 2. cast provisional paper ballots which must be validated later 3. cast standard ballots, which creates a risk of multiple ballots In cases 2 and 3, the poll clerk will have to track updates to the poll book manually and synchronize them later.

Key Recommendations

- For Standard Remote Authentication, a two-stage registration process with a single mailing and use of a shared secret in the form of government ID is the most secure. This process would consist of using the system-generated unique ID in conjunction with DOB and DLN, resulting in online delivery of the final voting password. Using a second mailing would provide no added security.
- An elector's date of birth, which can be known to many individuals, is not secure enough to authenticate an elector during the registration process.

  - Government ID is therefore a much stronger means of verifying identity.
  - While the Driver's Licence is not an ideal mechanism, due to the factor that many electors do not or cannot obtain a licence to drive, it is likely that it is the only form of ID that Elections Ontario will be able to use for authentication in the pilot.
  - In the event that an elector is unable to authenticate using the driver's licence, they can register by attending a Returning Office.
- Elector must always be able to attend a Returning Office to register in person in the event that online registration does not work (for example, if they do not have the required proof of identification).
- To enable both remote computer and remote telephone voting, both the User ID and password must consist of strong numeric strings.
- Cancellations and issuance of new credentials should require voters to physically attend an EO office.
- New credentials can be sent by SMS/email from the voting platform to prevent help desk staff from having access to them. This will require voters to provide SMS or email contact information when making a claim.
- One mailed package is sufficient for the Standard Remote Authentication process, as it strikes an acceptable balance between security and ease-of-use for the electorate.

6.2 VOTING

The following section provides a view of how all four of the short-listed voting channels could be implemented in an integrated model. The feasibility of each individual channel will be assessed in subsequent sections.

On-site Voting

After identifying the voter using legally accepted identification, the poll worker would validate the voter's eligibility using an online poll book (i.e., check that the voter is on the electoral list and has not yet cast a vote). The poll worker will then give the voter a token (e.g., a smartcard, or a VIN on a piece of paper) that will allow the voter to use one of the supplied voting devices (computers or telephones).

If using a computer, the voter will authenticate by inserting the token into the voting computer. The ballot will be designed to appear as clear and readable as possible. The ease of the voter's interaction with the system will be enhanced as much as possible through the provision of assistive technology such as a touch-screen display, screen readers, headphones, and other assistive devices. Voters will be able to clearly distinguish the candidates' names in an online ballot that conforms as closely as possible to the requirements set out in the Election Act; however, it is recommended that the ballot layout support a random display order of candidate names in order to prevent any possible loss of secrecy due to fingerprints left on touch screens.

While the system will include features (confirmation dialogues, etc.) to help ensure that voters do not under or over vote in error, it will also allow voters to intentionally cast spoiled or invalid ballots if they choose to.

If voting by telephone, the voter will authenticate by typing the VIN provided by the poll worker the ballot using the telephone's twelve-digit keypad. The ballot will take the form of clear and easy to understand audio instructions. The voter will be able to control the playback speed and volume of the instructions and voting menu options and receive clear confirmations of selections.

Remote Voting

Voting remotely will use the same computer and telephone interfaces as used on site, with the exception that voters must authenticate by typing their Elector ID and the numeric password obtained during the registration process. The telephone menu system and online ballot interface will otherwise be the same.

Receipts

The system must provide voters with a voting receipt once they have cast their ballot. This receipt, will allow them to verify that their vote was present during the decryption and counting process. In order to avoid enabling coercion or bribery, the receipt will not contain readable evidence of the voter's actual selection. The receipt must also not allow anyone with access to the system to link voters with their cast ballots.

The Electronic Poll Book (ePB)

If remote network voting runs in parallel with on-site network voting, an electronic poll book will be required to manage the list of electors and prevent multiple votes from the same voter. In this scenario, Elections Ontario staff could use the existing Electoral Management System (EMS) to manage the list of electors in real time throughout the event, including striking voters, adding and deleting electors, updating records, and recording tokens to access the voting terminals.

Polling places would need computers to access the electronic poll book and support both network voting and paper voting onsite. This would require a set of interactions between EMS and the Network Voting System (NVS) supplied by a vendor.

The following process outlines the interfaces that would be required to exist between EMS and the NVS during the three principal phases of the event (before, during, and after voting). Data transferred between EMS and the NVS should ideally be done using web services.

BEFORE VOTING STARTS

1. EMS provides the voting system with an initial list of voters (e.g. 100,000 names)
2. The NVS pre-generates 120,000 voter credentials (VINs/passwords). The extra 20,000 are kept in reserve to handle new additions, cancellations, resets, etc.
3. To manage the login sent to the voters by post:
    i. EMS identifies electors who will receive a network voting Registration package with an NV ID and sends this data to the NVS through an interface.
    ii. EMS manages the process of sending the cards
4. The NVS sends data to EMS to identify which electors set up a password on-line using the NVS web interface.

DURING THE VOTING PERIOD

5. As changes to the voters list are managed through EMS, changes that affect network voting must be kept synchronized with the NVS*:
    i. Electors who are removed from the system (if the voter has already cast an electronic vote, then the encrypted ballot could be identified and marked as invalid).
    ii. Electors who move from one ED to another and therefore vote on a different ballot. (The encrypted ballot could be identified and marked as invalid.)
    iii. New voters added: a spare credential is assigned to this new voter.
6. The list of electors in EMS is kept up to date using data from the NVS that indicates whether an e-voter has cast a ballot. *
7. EMS must also be able to request the NVS to cancel an electronically cast ballot (linked to a voter). *
8. The poll worker uses EMS to code a token that authorizes the voter to use the voting computer, then its interface must support this action, and another communication must be established with the NVS, which is the one providing the data to be included in the token for voter authentication.

AFTER THE VOTING PERIOD

9. The NVS sends the final list of e-voters to EMS.
10. This could be done using a file transfer instead of a web service.

* Changes are required to EMS to allow the poll workers to execute these actions.

Operating without an Electronic Poll Book

In the event that only remote voting is implemented in parallel with conventional voting, and on-site network channels are not used, an electronic poll book is not strictly necessary. The main function of the electronic poll book is to control the number of votes cast by a given individual user across multiple channels while at the same time allowing the voters list to be dynamic by allowing additions and deletions during the voting process. If network voting is conducted only by remote channels, and the voters list is kept static during the voting period, an electronic poll book will not be necessary.

In a scenario that uses only remote network voting combined with paper ballots, an online poll book is not strictly required, provided that another means can be implemented to prevent voters from voting online and then voting on paper, or vice versa. Each channel (network and paper) will effectively manage its own list in parallel and any need to synchronize will be handled manually as exceptions and will not be in real time.

- ELMS or EMS will provide the back end voters list 'of record' and will generate the paper lists used at the polling locations.
- ELMS or EMS will also provide the network voting system with the preliminary list of electors (PREO). The network voting system will then assign a unique identifier to each elector (the Elector ID).
- Electors who wish to vote remotely will register online or by phone and associate additional credentials with their Elector ID.
- Voter registration must end in advance of the advance poll date so that printed lists can be generated and distributed.
- Electors who register for the remote network voting channels will then be 'locked in' to network voting and would be unable to vote by paper. (*exceptions are possible for electors to request that their NV credentials be cancelled so that they can vote by paper).
- The voters list at polling locations will not be automatically synchronized with the online network voting list.

The network voting system's electronic electoral roll contains the real-time list of voters who are permitted to vote using the network channels. It functions independently of EO's voters list and is designed to provide a) real-time strike off of network voters; and b) linking of voters to encrypted ballots. It is not optional, and will be included as part of the network voting product.

If locking voters into the network voting channel constrains elector choice to an unacceptable degree, the ELMS/EMS list could be synchronized regularly (daily) with the online system by reviewing the list of paper strike-offs and striking them electronically from the network voting list. Doing this, however, would put the principle of 'one vote per voter' directly at risk.

Alternatively, network votes cast by voters who also voted in person using a paper ballot could be removed on a daily basis, or after the election; however, this will leave the impression that multiple voting is somehow possible, and give the appearance that the 'one vote per voter' principle is not being supported.

Onsite voting, which would be conducted only using the traditional paper ballot method, would operate as follows:

1. Printed list is distributed to polling locations, indicating voters that have registered to vote remotely.
2. Voter presents ID at polling location and poll worker checks eligibility on printed list.
3. The poll worker will give a ballot only to voters who are not registered to vote online.
4. The poll worker strikes the voter from the paper list.

Network voting, which would be available only through remote channels, would operate as follows:

1. Voter registers to vote remotely (using telephone or computer) before the advance polling period begins.
2. Voter authenticates online using Elector ID and password.
3. Network voting system processes the vote and strikes the voter.
4. Voter is not able to vote a second time using either remote channel.

In the absence of a live link between the list of electors stored and managed by the network voting system and the Elections Ontario voter list, revisions would be handled as follows:

1. EO staff correct and update the voters list using the current back end systems and processes.
2. The updates are synchronized as needed with the network voting system using manual processes.
3. A final sync is run between the network voting system and ELMS/EMS after the event.

Voters could register for network voting and then either decide not to or be prevented from doing so. If they remain 'locked in', they could be unable to vote at all. Electors who registered for network voting but had not done so by the close of the network voting period could have their credentials cancelled so that they can still vote by paper on Election Day.

Additions to the list would require more complexity and elapsed time:

- Adding a name would require the mailing of Elector ID cards, synchronization with the network voting system, and the addition of processes to track extra cards.
- Voters who must be deleted from the list once it is in the online system can be removed manually through an administrative interface.

Key Recommendations

- If on-site network voting is provided, electronic poll book functionality must be implemented – including a real-time interface for poll staff.
- If only remote network voting is provided, and the electronic poll book is eliminated, then the list of network voters should be kept static during the voting window – that is, network voters will be 'locked in' as a rule.
- Use two separate authorization systems for onsite voting; one for computer voting based on a smart card and another for telephone voting based on a printed VIN. The principle behind this recommendation is to use the more usable system (smart card) wherever possible and limit the use of VINs, which have usability and accessibility challenges.
- If a voter attends on site and is marked as having voted already, then the Returning Officer will rule on the matter of voter impersonation.
- The system should allow voters to decline ballots by providing a 'decline ballot' or 'none of the above' option, in addition to allowing under votes and over votes.
- Touch screen displays, which are recommended due to usability and accessibility reasons, may show fingerprints and therefore popular voting selections if the candidate order is static as per regulation (subsection 34(2) of the Election Act). To mitigate this potential privacy risk, Elections Ontario should seek an exception to section 34(2) and implement a random candidate name order for the online ballot.

6.3 VOTE STORAGE

The encryption takes place either in the voter's computer or in the voting servers when cast through a telephone.

After the voter has submitted his or her ballot using either the computer or the telephone, it is stored in the network voting system's 'digital ballot box', where it remains encrypted for absolute secrecy. The system will now be responsible for maintaining the security and integrity of the vote data it stores until it is time to start the decrypting and tallying process.

While the election is under way, the network voting's security measures (intrusion detection systems, activity logs, etc.) will detect any attempt by external or internal users to delete votes from the ballot box or to add counterfeit votes. The system will implement security measures to prevent compromises of voter privacy, unauthorized publication of intermediate results, ballot stuffing, or vote modification and deletion.

6.4 TABULATION

The voting system will ‘close’ automatically at the time specified by Elections Ontario: voters will be unable to log in to system but voters who are in the process of casting their vote will be allowed to finish within a defined period of time.

Only the members of the Network Voting Management Board can initiate the decryption process. A pre-defined majority of Network Voting Management Board members will assemble to construct the election decryption key, which is not available during the voting process.

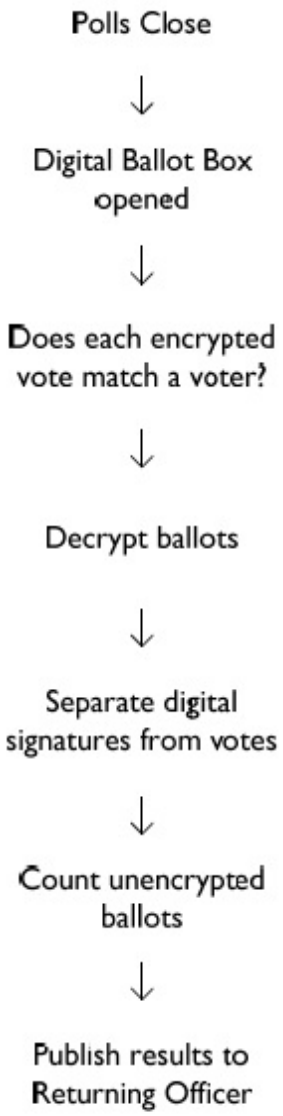
Ideally, the ‘ballot box’ is moved to a secure and isolated environment on Elections Ontario’s premises that is not connected to the Internet or any other communication network.

The system will verify that all the votes contained in the ballot boxes are cast by eligible voters. It will also prevent multiple votes by the same voter from being decrypted, including the prevention of counting votes tagged as invalid by an authorized user (as in cases of an impersonation claim).

It will be impossible to correlate the order of the decrypted votes with the order they were cast and, therefore, prevent any link between the decrypted votes and the voters by using a Mixing process.

Once complete, the Network Voting Management Board will certify the list of decrypted votes and prepare the output reporting, including all valid and invalid ballots for each candidate by Electoral District.

The results will be reported to the Returning Officer of each Electoral District, and added into the results consolidation system managed by Elections Ontario.



6.5 AUDIT

The system will allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes, including the authenticity of the software, the integrity of the system, the integrity and authenticity of the generated logs, etc. At any time during the election auditors will be able to verify that the votes in the ballot box belong to eligible voters.

This will allow independent auditors or the Network Voting Management Board to carry out parallel recounts from the certified list of decrypted votes or even new decryption and tabulation processes if required. Auditors should be able to operate with the decrypted votes and obtain human-readable results that can be compared to the ones generated by the system.

7. ANALYSIS OF THE SHORT-LISTED SCENARIOS

Detailed research into network voting options eliminated six of ten options, leaving four options for further study. The previous section provided a walkthrough of how each of these scenarios would fit into the voting process. This section provides an analysis of how well the remaining four scenarios fit the current context documented in Section 4, analyses the support for network voting principles short list documented in Section 5, and provides a detailed analysis of risk and security considerations.

Evaluate Suitability for Pilot

THE NETWORK VOTING RESEARCH process resulted in a short list of four Network Voting scenarios that required further analysis. It is the finding of this Business Case that combining these four scenarios into a single model could support the selected principles and is broadly capable of operating within the constraints and meeting the objectives of the pilot. These four channels consist of:

1. Onsite computer voting with supervised authentication;
2. Onsite telephone voting with supervised authentication;
3. Remote computer voting based on password authentication; and
4. Remote telephone voting based on password authentication.

Organization of this Section

In the following sections this integrated model is evaluated according to:

- a contextual analysis based on the constraints defined in Section 2;
- an analysis based on the core network voting principles defined in Section 3; and
- an overview of the security, operational, and voter risks that each scenario would face.

7.1 CONTEXTUAL ANALYSIS

The four short-listed scenarios described fit with the contextual factors defined in Section 2 to varying degrees. The following section provides an analysis of how well each scenario fits with Election Ontario's Strategic Direction, works within the known constraints, meets the needs of the target audience, and supports the defined voting principles.

Analysis based on Strategic Direction

INCREASE THE RANGE OF VOTING OPTIONS

Conducting a pilot of telephone and computer voting, which are the foremost channels for casting electronic ballots, is aligned with Elections Ontario's strategy of innovating and setting new benchmarks. Furthermore, providing new network voting channels fits well with Elections Ontario's strategic intent to provide the electorate with more choice, increase opportunities to vote, and to support the overall accessibility of the process.

The analysis, however, does not support the conclusion that providing on-site channels will add significantly to the range of choices. While electors who have difficulty attending a location will welcome the option to vote from home or work, on-site voting would only provide an additional option to voters who wish to cast a ballot electronically but do not have easy access to the internet or telephone. Providing accessible network voting locations would add another choice, but the benefit would be marginal – especially in the context of a pilot.

Analysis based on Constraints

SUPPORT UNIVERSAL ACCESS

Although the timing will be tight, it is feasible to procure, customize, and implement a Commerical-Off-The-Shelf (COTS) network voting system that can be used during a by-election by the first quarter of 2012. A system that combines computer and telephone channels, as recommended by this document, will be able to provide a convenient process and interface to a wide range of voters.

The remote channels can include a very accessible web interface that is both usable and compatible with assistive technology, provided that the correct standards are enforced and that the user experience is both well designed and well tested.

While the reach of the Internet is wide in both geographic and demographic terms, the addition of a telephone channel ensures that remote voting is as accessible as possible. Electors without access to the Internet will still have the option to vote using the telephone. While providing on-site options would increase the options available and help ensure that an accessible and supported experience is available, implementing such a channel is not necessary in order to deliver a significant accessibility benefit to voters.

RESPOND TO PUBLIC CONCERNS THROUGH SECURITY & TRANSPARENCY

Public and media concerns regarding potential security, privacy, and integrity problems associated with electronic voting can be met by specifying and procuring a system that provides the best security solutions available. Independent and published audit and verification results will be critical to meeting and overcoming these valid concerns.

In addition to meeting the concerns through a technical means, the perception itself can be managed through a detailed and effective public communications campaign that acknowledges the concerns as valid and demonstrates how these concerns are being addressed.

OPERATE WITHIN PROCESS CONSTRAINTS

Remote telephone and computer voting provide a good fit with the process and operational constraints identified by Elections Ontario. These channels can be adapted easily for use during advance polling, and not on Election Day itself. In fact, eliminating electronic voting on Election Day has the benefit of reducing the risk of collisions between online and paper voters and eliminates the risk that an elector is turned away from voting due to not having registered in advance.

CHALLENGES EXISTING PERSONNEL & SYSTEM CONSTRAINTS

The on-site channels, however, provide a more challenging operational fit, as they would increase complexity for Elections Ontario and would require organizational change. Specifically, having remote voting run in parallel with on-site voting would require the implementation of a real-time electronic voters list (poll book) in order to control the number of ballots that a voter could cast in a single day.

ON-SITE CHANNELS WILL STRAIN CHANGE CAPACITY

Implementing a electronic poll book system would require changes to Elections Ontario's existing back-end voters list systems and would require additional training and logistics at the polling station level – notably the need to distribute and support poll book hardware and software. With only remote channels in play, the need for the real-time poll book is reduced.

Similarly, implementing on-site voting will result in a greater expenditure, as both voting and poll book hardware will need to be procured, distributed, supported, and managed. Implementing remote channels only will eliminate this expenditure and improve cost scalability.

Implementing remote channels only would provide the best fit with Elections Ontario's current capacity for change, while simultaneously achieving strategic goals and pilot objectives. Given the risks associated with a very tight timeline (a implementation project window of approximately six month), the acquisition of a Commercial-Off-The-Shelf (COTS) system from a proven vendor is recommended.

Analysis based on Target Audience & Stakeholder Considerations

The stakeholders consulted echoed Elections Ontario's stated strategy by emphasizing the need for options and increasing elector convenience. Their concerns reveal a need for the solution to emphasize security, privacy, and independence.

REACH AS MANY ELECTORS AS POSSIBLE

While Ontarians' access to the Internet is very broad (80% use it daily) and the telephone is near universal (99%), it is important that the solution be widely accessible. By offering network channels in addition to the current paper ballot, an integrated four-channel model would reach as many Ontarians as possible through a range of voting options. Onsite computer voting would provide an accessible option for those who have challenges with paper voting, but have no Internet service at home. Telephone voting would provide an option to those who find it difficult to attend in person but have no Internet access.

7.2 ANALYSIS BASED ON PRINCIPLES

The four scenarios must also be evaluated for their support for the eight key principles that Elections Ontario is using to guide the Network Voting project.

	PRINCIPLE	ANALYSIS
1	Accessibility	All four channels are accessible to varying degrees. While telephone voting poses usability and accessibility challenges to some users, it is also the most universally available technology. The accessibility challenges of telephone voting, particularly with regard to the difficulty of on-site authorization for visually impaired voters, would be overcome by making an accessible computer channel available in parallel. **Accessible Technology** The accessibility of the computer channel can be greatly enhanced by implementing an assistive technology strategy. For example, by making the web interface compatible not only with WCAG specifications but also with screen reader technology will deliver a practical benefit to voters who use this type of technology. Furthermore, by focusing on emerging screen reader solutions, which tend to be very low cost or free, the strategy can reduce both rollout costs and reduce barriers for new adopters. **Registration Process** The greatest accessibility challenge that the short-listed scenarios face is related to the registration process. In order to confirm the elector's identity during registration for network channels, a piece of government ID will be required. However, Elections Ontario has access only to Drivers Licence numbers. This type of identification is not universal, especially among electors with certain disabilities.

	PRINCIPLE	ANALYSIS
		The model recommends that electors who are unable to supply a Drivers Licence number during registration must attend a Returning Office to register. This has the effect of creating an accessibility barrier for Electors without a driver's licence, many of whom may have disabilities that already make travel difficult. Rather than proceed with an authentication method that discourages electors without drivers licenses from participating, Elections Ontario may prefer to pursue an approach that is less secure but meets the needs of the broader electorate. Use of a registration process based on two sequential mailings, while not technically as secure (if the first mailing can be intercepted, then the second could as well), has proven successful in municipal elections including Markham 2010. The target end state for authentication is ability to integrate with third-party authentication providers such as ServiceOntario (see Scenario 9 for benefits of this approach). **Other authentication challenges: onsite voting** Printing a VIN, which is the best feasible option for authorizing voters to use the onsite telephone scenario presents a number of inconveniences, including an accessibility compromise. Voters whose vision is impaired and would require assistance in reading the printed VIN. This also presents a voter privacy challenge (see below). The authentication option for onsite computer voting, however, does not reduce accessibility to anywhere near the same degree.
2	One vote per voter	If both onsite and remote channels were implemented, a central electronic electoral list integrated in real time with the voting system would be necessary in order to ensure that only one vote is counted per voter. Additionally, the VIN delivery process must be designed and tested to ensure that only one VIN is delivered to each voter. If only remote channels were implemented, the voters list could be managed without an electronic poll book. As the online network voting system will not be synchronized with the backend voters list (ELMS/EMS), voters list maintenance would need to be carried out in other ways: • freezing the online list based on the preliminary voters list (PREO). This is a reasonable measure to take for a pilot, as

	PRINCIPLE	ANALYSIS
		the volume of edits is likely low (<5% of total names); or • updating the online list manually as revision occur (e.g. by using an NVS back office interface or by uploading data files). In the absence of an electronic poll book there would be a high risk that voters could vote twice (once remotely, once on site) if voters were not locked in to their selected channel. Although this risk exists now with paper advance polls, the risk would have a much higher public profile with network voting and should be managed more aggressively.
3	Voter authentication and authorization	The password authentication mechanism used for remote computer and telephone voting can be a very secure way of establishing voter identity. To support this, the Elector ID delivery process and registration mechanism should be reliable and secure; and strict pass code length and complexity requirements can be enforced. Additionally, the identification data required to support an elector's identity claim during registration must be as secure and strong as possible. Personal information that can easily be discovered (date of birth, address, telephone number etc.), is not secure enough, as it would make impersonation too easy. A malicious actor who intercepted an elector's NRC and had access to this type of information could register as the voter and subsequently steal their vote. Government-issued ID (SIN, Health Card Number) is more suitable and has the benefit of being universally held among the electorate. As Elections Ontario will not have access to this data for the pilot, Drivers Licence Numbers (which EO can obtain) are an acceptable short-term solution. The chief drawback is the impact on Electors who do not or cannot hold a Drivers Licence (see Accessibility, above). It is the combination of these types of data that reduces the probability of citizen impersonation. By using physical ID for authentication wherever possible (on site) The four-channel model includes use of the best identification and authorization mechanism possible for network voting. It is difficult to predict what percentage of network votes will be cast remotely versus on site, but the pilot will give Elections Ontario the opportunity to evaluate both. Once voter identity has been established, an electronic poll book will be an extremely reliable means of verifying the elector's eligibility, as it will allow both poll workers and the network voting

	PRINCIPLE	ANALYSIS
		system to assess eligibility in real time.
4	Only count votes from valid voters	To ensure votes cannot be introduced by anyone other than valid voters, the servers and the voter list must be securely protected.
5	Individual verifiability	Both the online and telephone (IVR) interface can be designed to give voters a usable means to confirm their selections before casting the ballot. For the computer-based channels, a printable receipt could be generated in order to provide the voter with maximum verifiability.
6	Voter privacy	The end-to-end encryption that is part of the recommended approach will ensure voter privacy when using computers. For telephone voting, specific procedures and measures need to be in place.* *Telephone voting presents specific privacy risks that must be mitigated. For onsite channels, the physical placement and design of the voting kiosks is essential to guarantee that voters are able to cast ballots privately and independently. Printing a VIN, which is the best feasible option for authorizing voters to use the onsite telephone option presents a number of inconveniences, including an accessibility compromise. Voters whose vision is impaired and would require assistance in reading the printed VIN, which will violate their privacy and affect their ability to cast a vote independently. The authentication option for onsite computer voting, however, does not reduce a voter's privacy.
7	Results validation	Results validation will rely on the effectiveness of the end-to-end security measures and on robust system logging and auditing specified in the requirements.
8	Service availability	While there could be a relatively high impact in terms of number of votes affected if there is an outage at a polling station, the risk and impact go down dramatically for the remote channels. The best protection against services outages involves the kind of robust hardware and hosting infrastructure recommended in this Business Case: • a reliable and secure data centre; • reliable and redundant internet connectivity at polling

PRINCIPLE	ANALYSIS
	locations; and • a responsive hardware support and replacement process.

7.3 RISKS

Although this analysis suggests that while these four scenarios, can offer good fit with Ontario's needs, they still pose a set of risks, which are grouped into the following categories:

- Security risks;
- Operational risks; and
- Voter risks.

These risks are described briefly below and assessed in detail in Section 9, Risk Assessment.

Security Risks

The security risks that must be managed and mitigated can be divided into four categories, which also map directly to the principles list:

- Voter privacy and confidentiality;
- Vote integrity and accuracy of results;
- Election system availability; and
- Auditability.

Operational Risks

There are a series of operational risks related to the short-listed scenarios, which can be organized by the following four areas of operation:

- Polling Places
- The data centre
- Elections Ontario's Head Office
- The Help Desk supporting the Network Voting initiative

Voter Risks

There are two categories of risks related to voters: the results of their interaction with the Network Voting system at different stages; and their perceptions of the system and of network voting in general.

7.4 SECURITY OBJECTIVES

In order to be able to mitigate risk effectively, it is important to establish the security objectives that should be taken into consideration when implementing a Network Voting platform. The security objectives that should be emphasized for the pilot are as follows:

1. **Voter authenticity**: security objectives associated with the authentication of eligible voters.
2. **Voter secrecy**: objectives that will ensure voter privacy.
3. **System access control**: objectives associated with the identification and authentication methods implemented in the voting platform.
4. **Election integrity**: objectives that guarantee the consistency and accuracy of the cast ballots.
5. **Service availability**: requirements related to the availability of the election system and its information during the electoral process.
6. **Service protection**: objectives associated with the protection of the election system.
7. **Open auditing and accounting**: objectives that will ensure the accurate auditability of the election system and the traceability of the electoral process, and other requirements associated with the openness of the software.

7.4.1 Voter authenticity

1. The network voting platform shall ensure the identification of voters in a unique way (voters shall be unmistakably distinguished).
2. A voter shall be able to vote only in the Electoral District in which he or she is registered.
3. The network voting platform shall be configurable to require authentication one time per contest or one time per vote.
4. The network voting platform shall be able to authenticate voters by the approved authentication methods.
5. The voter credentials shall be created, distributed, and protected, in a way to ensure they are secret.
6. The voter credentials shall be strong enough to ensure they are not possible to obtain or guess (through a brute force attack or public information).

7.4.2 Vote secrecy

1. The network voting platform shall ensure that votes cast by voters are secret.
2. It shall be impossible to reconstruct a link between the voter and the vote content. It is applicable not only when the vote is cast and stored, but also when the votes are being counted.
3. When confirming to the voter that the vote has been properly processed and stored in the ballot box, the content of the ballot shall not be revealed in clear text.
4. The network voting platform shall provide for secure storage and encryption of the votes.
5. The traces and logs of the auditing features shall not reveal any information regarding the voter, the vote contents, and shall not be able to use these logs to link the voter with his vote.
6. The network voting platform shall ensure the secrecy of the votes at all stages of the election, even with the election is finished.
7. The network voting platform shall protect the privacy of voters. Any voters' personal information (e.g. contained in the electoral roll) shall be properly protected.
8. Temporal or residual information managed by the voting applications (e.g. cookies or temporal records) shall be destroyed after the vote casting, removing any possible trace containing the voter information or vote selections.
9. The security mechanisms used to protect the secrecy and anonymity of votes (passwords or cryptographic keys among others) shall be used and managed in a secure way, to ensure they cannot be used to compromise the secrecy of the vote.

7.4.3 System access control

1. Access to the network voting components shall be restricted and recorded.
2. The network voting platform shall restrict access to its functionalities and published services, according to the user identity and granted role, to those functionalities explicitly assigned to him.
3. The network voting platform shall request user authentication before any action can be carried out.
4. The user credentials shall be secret. The user accounts shall be based on the principle of least privilege.

5. The network voting platform shall protect authentication data so that unauthorized entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data.
6. The authentication process and procedures shall provide segregation of duties capabilities.
7. Anyone accessing to the voting platform (electoral officers, election administrators, operators or auditors) shall use strong authentication mechanisms, i.e. two factor authentication mechanisms.

7.4.4 Election integrity

1. Only one valid vote shall be counted per voter per contest.
2. The network voting platform shall prevent to insert a vote directly in the ballot box.
3. The network voting platform shall prevent to delete or modify a vote in the ballot box.
4. The solution for voting in a remote environment shall issue a message to inform the voter whether the vote has been successfully cast - properly recorded in the ballot box – or not.
5. The network voting platform shall ensure the integrity of the ballot box in all circumstances.
6. The network voting platform shall ensure the integrity of the votes stored in the ballot box in all circumstances.
7. The network voting platform shall prevent to alter, delete or add a counterfeit vote during transfer in the network.
8. The integrity of any configuration data communicated to the network voting platform shall be protected. The authentication of data-origin shall be ensured; it includes information like the electoral roll, the list of candidates, or any other election configuration information.
9. The network voting platform shall provide a message confirmation to the voter indicating that the vote was recorded as intended. This confirmation shall be protected against manipulation.
10. The network voting platform shall ensure that the voter’s choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.
11. It should be impossible to obtain intermediate results; it shall be impossible to know the number of votes cast for any candidate until the end of the polling phase.

12. The integrity of data communicated between software modules shall be maintained.
13. The integrity of data communicated from the pre-voting stage (e.g. voters' registers and lists of candidates) shall be maintained.
14. It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.
15. It shall be ensured that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system.

7.4.5 Service availability

1. The network voting platform shall implement mechanisms (such as redundancy) to protect the availability of the services during all the election process. It shall be resistant to system failures, breakdowns, and denial of service attacks among others.
2. In case of a system restart, the system shall be quickly restored to the last consistent status of the platform.
3. The network voting platform shall perform regular checks to ensure that the components are operating as expected.
4. The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained.

7.4.6 Service protection

1. A risk assessment of the e-voting platform shall exist, keeping a continuously updated threat model enumerating the identified threats, vulnerabilities and corresponding mitigations, and systematically using this throughout the system development lifecycle to mitigate identified vulnerabilities.
2. When cryptographic techniques are used, private or secret cryptographic keys shall be strongly protected.
3. All the modules from the network voting platform shall be properly protected against hacking, malicious software of any kind, and any other attacks.
4. The network voting platform shall maintain reliable synchronized time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observation data, as well as for maintaining the time limits for registration, nomination, voting, or counting.

7.4.7 Open auditing & accounting

1. The network voting platform shall provide the voter with 'end-to-end' proof that the vote has been received, recorded and counted as the voter intended (without violating the privacy requirement).
2. The network voting platform shall generate reliable traces or logs with enough detail level so that election can be audited and verified. The authenticity, availability, integrity, and timely of the audit data shall be ensured.
3. End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities and providing verification facilities.
4. The fact that a vote has been cast within the prescribed time limits shall be ascertainable.
5. The audit system shall be open and comprehensive, and actively report on potential issues and threats.
6. All modules of the network voting platform shall be verifiable.
7. The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.
8. The audit system shall provide the ability to cross-check and verify the correct operation of the election system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all valid votes have been counted.
9. Before any election takes place, the network voting platform shall enable to the electoral officials, observers, or auditors, to verify that the election system is genuine and operates correctly. It shall be possible to ascertain that only approved and audited software is being executed.
10. The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.

8. RISK ASSESSMENT METHODOLOGY

The Network Voting model presented by this business case has been selected based on a detailed study of the available technologies and of Elections Ontario's specific needs, goals, and constraints. Nevertheless, Network Voting presents a unique set of risks that must be assessed and managed.

To assess the risk level presented by the Network Voting model recommended by this Business Case, a number of potential threats were identified. For each threat, the following factors were then assessed:

Complexity: a rating of the technical skills needed to carry out the attack. Generally speaking, the more complex the attack, the less likely such an attack will be.

Impact: a rating of the effect of the attack if it were to happen.

Risk: the risk level that would remain once appropriate countermeasures were implemented.

8.1 COMPLEXITY / PROBABILITY

In cases where a malicious actor could carry out a technical attack, the likelihood that the resulting security threat will occur relates directly to the complexity of the potential attack and the skill or access levels required. For these types of threats, the complexity of the potential attack is rated from one to five. For other types of threat, where there would not be an actor responsible for a technical attack, a probability assessment is used to supplement the analysis. The values used to rate these factors are shown in the following table:

COMPLEXITY / PROBABILITY	
1- Very Complex / Very Low	Very Complex: Requires a very high technical skill level combined with a very large effort. Very unlikely.
2- Complex / Low	Complex / Requires a very high technical skill level or a very large effort. Unlikely.
3 – Standard / Medium	Standard / Requires a high technical skill level or a significant effort. It is difficult to predict whether it will happen or not.
4 – Easy / High	Easy: / Requires only a basic technical skill level with a minimum of effort. Likely to happen, a common occurrence.

COMPLEXITY / PROBABILITY	
5 - Very Easy / Very High	Very Easy: Any user is capable of performing the attack. Very Likely to happen, a very common occurrence.

8.2 IMPACT

For each threat, the potential impact is also rated. The values used to rate impact factors are shown in the following table:

IMPACT	
1 - Very low	Very low impact: information is not disclosed or modified. Public perception of the NVS can be negatively affected, but there is no actual impact on the election.
2 - Low	Low impact: non-critical information is disclosed. Individual polling places or individual voters can be affected.
3 - Average	Average Impact: the contents of some random votes could be disclosed, or the Network Voting System is temporarily unavailable. An entire voting channel could be affected (i.e. some polling places (or all of them)). A large group of voters can be affected.
4 - High	High Impact: Individual ballots can be modified, the contents of specific votes can be disclosed, or the Network Voting System is unavailable at critical times. The whole election can be affected (all voting channels). All the voters can be affected, causing minor difficulties or unavailability for a short period of time (short delay on election start time for instance).
5 - Very high	Very High Impact: Election results are seriously compromised, ballot box privacy is broken, or voting system is permanently unavailable. The whole election can be affected (all voting channels). All the voters can be affected, causing major difficulties or unavailability for a long period of time (inability to start the election).

8.3 RESIDUAL RISK LEVEL

After considering the complexity or probability of a potential threat and combining this factor with the likely impact of the threat, an inherent risk exists. There are four accepted techniques for managing risk:

Avoidance: eliminate the risk by avoid the activity that produces the risk.

Reduction: optimize implementation approaches in order to mitigate the risk and reduce the probability, the impact, or both.

Sharing: transfer the risk to other parties through outsourcing, partnerships, etc.

Retention: accept the risk and then plan and budget for dealing with the consequences.

Due to the criticality of the voting system, the best approach in this case is to reduce each risk by implementing mitigating countermeasures. For each threat, therefore, a mitigation section describes controls or countermeasure that can effectively reduce the risk level.[17]

Since effective countermeasures or mitigation strategies exist for most threats; this assessment rates the ***residual risk*** level that remains once countermeasures appropriate to the potential attack or threat have been implemented.

The possible risk values are shown in the following table:

RISK	
1 - Very low	Very low residual risk level, considered an acceptable risk for any existing risk level tolerance.
2 – Low	Low residual risk level.
3 – Medium	Medium residual risk level, considered as moderate.
4 – High	High residual risk level, as either the likelihood or the impact is high and there are no effective countermeasures to reduce it.
5 - Very high	Very high residual risk level, as both the likelihood and impact are very high and there are no effective countermeasures to reduce it. Election results could be compromised or the system could be unavailable permanently.

9. RISK ASSESSMENT

This section provides the results of a detailed assessment of the risks that pertain to the four short-listed Network Voting scenarios. For details on the methodology used to assess risk, please refer to the previous section.

Types of Risk

THIS SECTION is organized into three major subsections, each dealing with a specific type of risk:

Security Risk Assessment, which analyzes the mainly technical risks that could affect the security of the network voting process and platform.

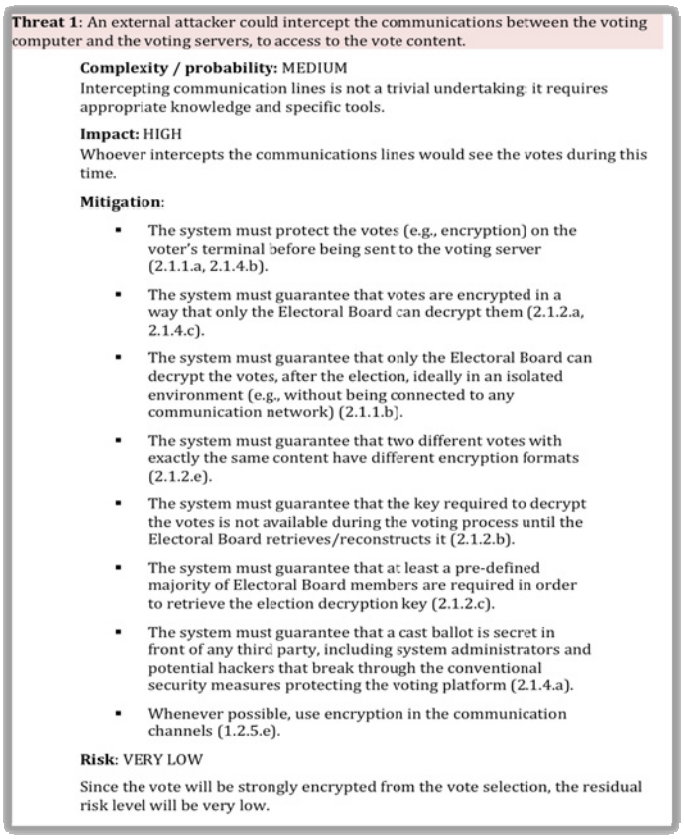
Operational Risk Assessment, which analyzes the mainly procedural risks that may occur at different levels of business operations.

Voter Risk Assessment, which analyzes the risks that are unique to the way individuals could interact with the system and related processes.

Each subsection contains a number of threats, which represent potential vulnerabilities that need to be understood and managed. Analysis of each threat includes a definition of the Complexity of the attack or the Probability of the threat occurring; an assessment of the impact level created if the threat were not managed; detailed steps for mitigating the threat; and a residual risk level assesses the risk level that remains after mitigating steps have been taken.

The following figure provides a look at a typical threat analysis:

Threat Description, Complexity & Impact, Ways to Manage the Risk Residual Risk.



Threat 1: An external attacker could intercept the communications between the voting computer and the voting servers, to access to the vote content.

Complexity / probability: MEDIUM
Intercepting communication lines is not a trivial undertaking: it requires appropriate knowledge and specific tools.

Impact: HIGH
Whoever intercepts the communications lines would see the votes during this time.

Mitigation:

- The system must protect the votes (e.g., encryption) on the voter's terminal before being sent to the voting server (2.1.1.a, 2.1.4.b).
- The system must guarantee that votes are encrypted in a way that only the Electoral Board can decrypt them (2.1.2.a, 2.1.4.c).
- The system must guarantee that only the Electoral Board can decrypt the votes, after the election, ideally in an isolated environment (e.g., without being connected to any communication network) (2.1.1.b).
- The system must guarantee that two different votes with exactly the same content have different encryption formats (2.1.2.e).
- The system must guarantee that the key required to decrypt the votes is not available during the voting process until the Electoral Board retrieves/reconstructs it (2.1.2.b).
- The system must guarantee that at least a pre-defined majority of Electoral Board members are required in order to retrieve the election decryption key (2.1.2.c).
- The system must guarantee that a cast ballot is secret in front of any third party, including system administrators and potential hackers that break through the conventional security measures protecting the voting platform (2.1.4.a).
- Whenever possible, use encryption in the communication channels (1.2.5.e).

Risk: VERY LOW

Since the vote will be strongly encrypted from the vote selection, the residual risk level will be very low.

9.1 SECURITY RISK ASSESSMENT

Organization of this section

This section is organized according to the five basic process steps. Each subsection discusses the potential threats associated with each step of the process, and provides a risk analysis and mitigation strategies for each threat.

1. **Registration & Authentication**

   This section contains risks related to the authentication procedure (based both on physical ID or password authentication), and the countermeasures necessary to mitigate them to an acceptable level.

2. **Voting**

   This section includes the risks and controls that apply to the period of time when voters are casting ballots

In this case, there are two sections:

- one for the computer environment; and
- one for the telephone environment

3. **Vote storage & ballot box management**

   This section includes the risks and counter-measures associated with securing the digital ballot box from the time voting begins until the ballot box is opened to perform the Tabulation process

4. **Tabulation**

   The Tabulation section incorporates all the risks and controls related to the revision of the votes and the counting process.

5. **Election auditing**

   The last section includes the risks and controls associated with the ability to review the electoral system, and its openness and transparency properties

Risk categories

A network voting approach that includes computer and telephone voting is potentially vulnerable to several types of security risk. As seen in the chart at right and demonstrated in the following section, the most prominent risk group is made up of threats against the accuracy of the results, which would have a direct bearing on the integrity of the election. These threats include the possibility that votes could be modified or deleted while they are being cast, once they are stored in the system, or when they are being counted.

Next, there are a number of possible privacy threats that would result in the voter and their ballot choice being linked. Furthermore, if authentication protocols are not secure enough, voters could be impersonated or ineligible names could be added to the voters list. There are also potential denial-of-service threats that would compromise the availability of the system during voting, and a possibility that the data required for accurate election auditability could be compromised.

Figure 9: Risk Categories

Summary of Results

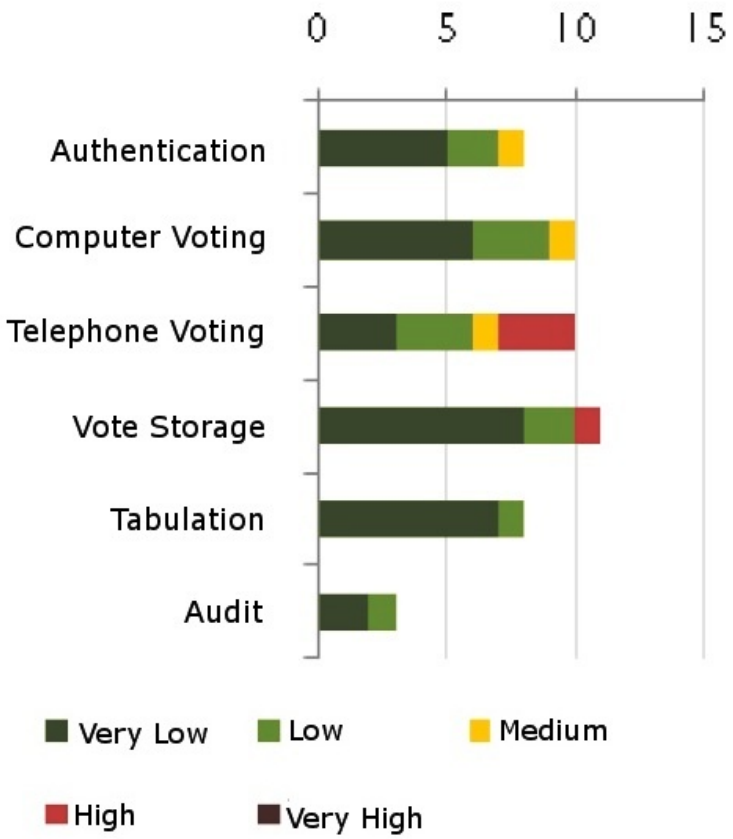
The chart at right presents a summary of the security risk assessment of the four network voting scenarios. It displays the number of potential threats for every step in the electoral process, with the voting step being split into two rows – one for each voting method. The chart also displays the residual risk level that would be in place, given that provided that the appropriate mitigation steps are taken.

For the most part, the threats can be mitigated to the point where they present only a low or very low risk. There are still some medium risks for areas such as telephone authentication and voter coercion,

The only step in the process that faces threats with a high residual risk is Telephone Voting, with three high-risk threats:

- an attacker could intercept the vote after it leaves the telephone but before it reaches the secure voting servers;
- an IVR system administrator could intercept the votes in transit, violating privacy and enable unauthorized publication ; and
- an attacker who intercepts the votes could modify them.

Figure 10: Residual Risk Levels by Process Step



Results by Scenario

Additionally, as the four short-listed scenarios analysed for this business case have different risk ratings, the following graphic presents the risk assessment for each analyzed scenario.

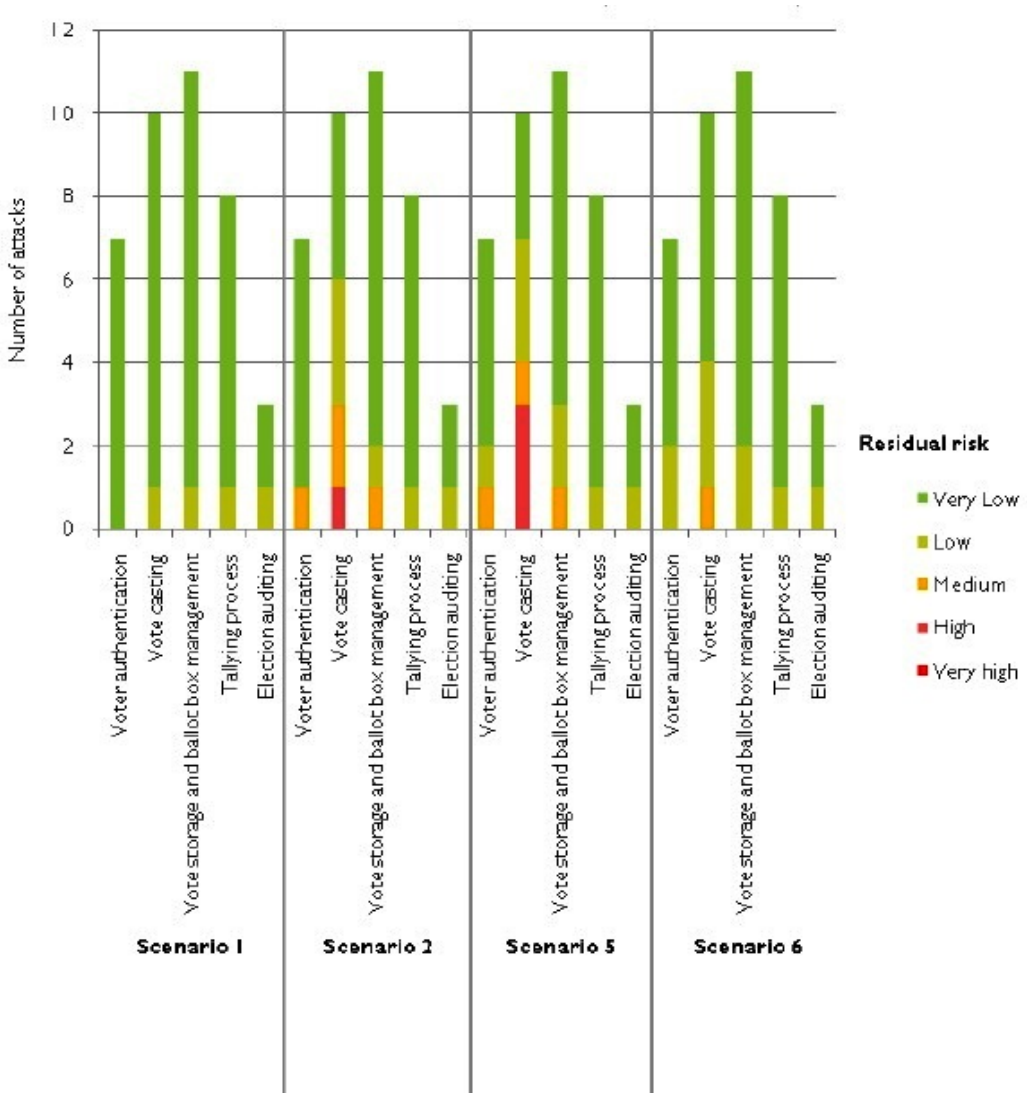
Scenario 1: On-site computer-based voting with authentication based on physical identification.

Scenario 2: On-site telephone-based voting with authentication based on physical identification.

Scenario 5: Remote telephone voting with password based authentication.

Scenario 6: Remote computer voting with password based authentication.

Figure 11: Security Risk Assessment by scenario



9.1.1 VOTER AUTHENTICATION RISKS

Voter authentication threats are largely driven by risks created by insufficient system security:

- people other than eligible voters can enter the system and vote, by circumventing or defeating a weak login process.
- voter credentials could be intercepted and a valid voter could be impersonated.
- rules about which Electoral District the voter is eligible to vote in are not well enforced.
- unauthorized names are added to the electoral list.

9.1.1.1 VOTER IMPERSONATION (VOTER AUTHENTICITY)

A voter or an attacker could try to cast a vote on behalf of another person, or on behalf of multiple people.

Threat 1: An attacker could steal all the voter credentials from the voting servers, and enter valid votes on behalf of authorized voters.

Complexity: HIGH

The ability to access the voting servers and steal voting credentials will require advanced technical skills.

Impact: VERY HIGH

Non-authorized votes could be processed on a massive scale, and the election results could be seriously compromised.

Mitigation:

- Voter credentials shall be combined with personal data to grant access to the voting system for casting a ballot (1.2.2.b).
- The system must use unique digital certificates for authenticating voters (2.1.9.g).
- The service provider is responsible for deploying the required software on top of the operating system (including application servers, databases, etc.), as well as of the operating system configuration and hardening (2.3.6.d).

Risk: VERY LOW

Since the credentials in the voting servers, which store the credentials, will be encrypted and strongly protected, the residual risk level will be very low.

Threat 2: An attacker could try to obtain valid voter credentials (by guessing them, or through brute force attacks or by intercepting a telephone call) and cast a valid vote on behalf of authorized voters.

Complexity: EASY

Once the credentials are securely generated and stored in the voting system, attacks could be made that attempt simulate a voter using the external interfaces (e.g. guessing a credential or brute force attack) **or** by intercepting weak communications inside (e.g. the IVR segment). Basic technical skills would be required to conduct a brute force attack. An IVR administrator could have access to the information by monitoring the call when voting over a telephone.

Impact: HIGH

Non-authorized votes could be processed as valid, affecting the election results.

Mitigation:

- Voter credentials shall be combined with personal data to grant access to the voting system for casting a ballot (1.2.2.b).
- The system must use unique digital certificates for authenticating voters (2.1.9.g).
- Appropriate procedures are in place to guarantee that IVR technical operators have no access to the system during the voting process unless something critical happens (e.g. a system reboot is necessary).
- Appropriate measures are in place to avoid external attacks and network sniffing.

Note that an attacker that could intercept a telephone vote could also intercept the voter credentials of the voters using the telephone, and impersonate them. However, this would be detected by the voter as he or she would later be unable to vote (unless multiple votes per voter are allowed).

Risk: LOW for computer-based voting; MEDIUM for telephone voting.

If sufficient controls are in place, the residual risk level will be low for computer-based voting, but MEDIUM for telephone voting.

Threat 3: An attacker could steal a voter's credentials and cast a valid vote on behalf of the authorized voter

Complexity: COMPLEX

If credentials are not generated and stored in the voting system securely, they could be vulnerable to attacks from malicious insiders or external attackers that get obtain access into the servers.

A major effort would be required to steal a voter's credentials from the voting system, even for system administrators, if they are individually protected.

Impact: HIGH

Non-authorized votes could be processed as valid, affecting the election results.

Mitigation:

- The system must be able to export data to supply the existing Notice of Registration Card (NRC) process with sufficient data to populate and distribute Elector IDs via mail (1.1.2.c).
- Voter credentials shall be combined with personal data to grant access to the voting system for casting a ballot (1.2.2.b).
- The system must use unique digital certificates for authenticating voters (2.1.9.g).
- Voter credentials must be protected if/when stored in the voting system.

Risk: LOW

Since the voter will be strongly authenticated, the impersonation risk will be low, considering that voter credentials are well protected.

9.1.1.2 UNAUTHORIZED VOTERS CASTING VOTES (VOTER AUTHENTICITY)

Non-eligible voters could cast a vote for a specific contest.

Threat 1: A person not on the official voters list could be able to cast a vote.

Complexity: EASY

If the system is not sufficiently secure, a person who is not on the voters list could be able to cast a vote.

Impact: HIGH

Non-authorized votes could be processed, affecting the election results.

Mitigation:

- The system must require voters to use specific credentials to access the voting system (1.2.2.a).
- The system must guarantee that only eligible voters can log into the voting platform (2.1.9.a).
- Before accepting a cast vote, the system must verify the identity of the voter who casts the vote (2.1.9.b).
- The system must allow verifying, at any time during the election, that the votes within the ballot box belong to eligible voters (2.1.9.d).
- The system must prevent the addition of counterfeit ballots in the ballot box from both external users and system administrators (2.1.9.f).
- The system must use unique digital certificates for authenticating voters (2.1.9.g).

- The system must use unique voter digital certificates for digitally signing the votes cast (2.1.9.h). Note that for telephone voting, the signature is done in the servers rather than in the voter's computer as when voting over the Internet

  Risk: VERY LOW

  Since there will be effective countermeasures to validate the eligibility of the voters, the residual risk level will be very low.

Threat 2: A voter could be able to cast a vote in an Electoral District that he or she is not registered in.

Complexity: EASY

Any person could try to cast a vote, even for a race outside of the Electoral District he or she is registered for.

Impact: HIGH

Non-authorized votes could be processed, affecting the election results.

Mitigation:

- The system must require voters to use specific credentials to access the voting system (1.2.2.a).
- The system must guarantee that only eligible voters can log into the voting platform (2.1.9.a).
- Before accepting a cast vote, the system must verify the identity of the voter who casts the vote (2.1.9.b).
- The system must allow verifying, at any time during the election, that the votes within the ballot box belong to eligible voters (2.1.9.d).
- The system must prevent the addition of counterfeit ballots in the ballot box from both external users and system administrators (2.1.9.f).
- The system must use unique digital certificates for authenticating voters (2.1.9.g).
- The system must use unique voter digital certificates for digitally signing the votes cast (2.1.9.h).

  Risk: VERY LOW

  Since there will be effective countermeasures to check the eligibility of the voter in each contest, the residual risk level will be very low.

Threat 3: An attacker could try to modify the list of voters managed by the voting application, to be included as an eligible voter.

Complexity: MEDIUM

The voting system needs to manage its own list of electors, which will be imported from Elections Ontario's systems. It would require considerable technical skills for an attacker to modify the electoral roll.

Impact: VERY HIGH

Non-authorized votes could be processed, affecting the election results.

Mitigation:

- The system must check that the election information is certified by the Network Voting Management Board before starting the voting and counting processes (1.1.4.a).
- Any independent auditor must be able to certify the integrity and authenticity of the system components installed in the voting platform (1.1.4.e).
- The service provider will be responsible for deploying the required software on top of the operating system (including application servers, databases, etc.), as well as of the operating system configuration and hardening (2.3.6.d).

Risk: VERY LOW

Since all the components of the voting system - like the electoral roll - will be protected and digitally signed, the residual risk level will be very low.

Threat 4: An attacker – as a non-eligible voter – could try to cast a vote by circumventing the authentication process.

Complexity / Probability: MEDIUM

It would be complicated to circumvent the authentication process.

Impact: HIGH

Non-authorized votes could be processed as valid, affecting to the election results.

Mitigation:

- The system must require voters to use specific credentials to access the voting system (1.2.2.a).
- The system must guarantee that only eligible voters can log into the voting platform (2.1.9.a).
- Before accepting a cast vote, the system must verify the identity of the voter who casts the vote (2.1.9.b).
- The system must allow verifying, at any time during the election, that the votes within the ballot box belong to eligible voters (2.1.9.d).

- The system must prevent the addition of counterfeit ballots in the ballot box from both external users and system administrators (2.1.9.f).
- The system must use unique digital certificates for authenticating voters (2.1.9.g).
- The system must use unique voter digital certificates for digitally signing the votes cast (2.1.9.h).

  Risk: VERY LOW

  Since there will be controls in place to strong authenticate users, the residual risk level will be very low.

9.1.2 VOTING BY COMPUTER

Casting votes using a computer, either on-site or remotely, creates several categories of risk:

- voter privacy could be compromised.
- voter coercion or vote buying could be enabled.
- votes could be modified after they are cast.
- votes could be deleted after they are cast.
- the voter could feel uncertain that their vote has been cast.

9.1.2.1 VOTER PRIVACY COMPROMISE (VOTER PRIVACY &CONFIDENTIALITY)

An attacker could violate voter privacy, linking the voter with her ballot selection through the following means:

- intercepting communications between the voting computer and the servers;
- accessing the network voting infrastructure directly from the inside; and/or
- installation of malicious software on voting computers.

Threat 1: An external attacker could intercept the communications between the voting computer and the voting servers, to access to the vote content.

Complexity / Probability: MEDIUM

Intercepting communication lines is not a trivial undertaking: it requires appropriate knowledge and specific tools.

Impact: HIGH

Whoever intercepts the communications lines would see the votes during this time.

Mitigation:

- The system must encrypt the votes on the voter's terminal before being sent to the voting server (2.1.19.b).
- The system must guarantee that votes are encrypted in a way that only the Network Voting Management Board can decrypt them (2.1.18.a).
- The system must guarantee that only the Network Voting Management Board can decrypt the votes, after the election, ideally in an isolated environment (e.g., without being connected to any communication network) (1.3.2.a, 2.1.19a).
- The system must guarantee that two different votes with exactly the same content have different encryption formats (2.1.18.e).
- The system must guarantee that the key required to decrypt the votes is not available during the voting process until the Network Voting Management Board retrieves/reconstructs it (2.1.18.b).
- The system must guarantee that at least a pre-defined majority of Network Voting Management Board members are required in order to retrieve the election decryption key (2.1.18.c).
- The system must guarantee that a cast ballot is secret in front of any third party, including system administrators and potential hackers that break through the conventional security measures protecting the voting platform (2.1.18.a).
- Whenever possible, use encryption in the communication channels (1.2.5.e).

Risk: VERY LOW

Since the vote will be strongly encrypted from the vote selection, the residual risk level will be very low.

Threat 2: A system administrator of any intermediate infrastructure component (e.g. voting servers) would have access to the votes with the voting options selected by the voters.

Complexity: EASY

It would be easy for a system administrator of an intermediate server to access the data in transit.

Impact: HIGH

Whoever has access to the intermediate infrastructure components would see the votes during this time.

Mitigation:

- The system must protect the votes (e.g., encryption) on the voter's terminal before being sent to the voting server (2.1.19.b).
- The system must guarantee that only the Network Voting Management Board can decrypt the votes, after the election, ideally in an isolated environment (e.g., without being connected to any communication network) (2.1.19.a).

- The system must guarantee that votes are encrypted in a way that only the Network Voting Management Board can decrypt them (2.1.18.a).
- The system must guarantee that the key required to decrypt the votes is not available during the voting process until the Network Voting Management Board retrieves/reconstructs it (2.1.18.b).
- The system must guarantee that at least a pre-defined majority of Network Voting Management Board members are required in order to retrieve the election decryption key (2.1.18.c).
- The system must guarantee that two different votes with exactly the same content have different encryption formats (2.1.18.e).

Risk: VERY LOW

Since the vote will be encrypted from the vote selection until the decryption process, the residual risk level will be very low.

Threat 3: Malicious software running on computers used to access the network voting system could try to access the voting options selected by a voter.

Complexity: COMPLEX

Advanced technical skills would be necessary to install malicious software on voters' computers specifically designed to identify the voting options. This attack is even less feasible in voting terminals at the polling places.

Impact: AVERAGE

Whoever compromises the computer could see the cast votes through this terminal.

Mitigation:

- *On-site computer voting:* The service provider must describe its needs in terms of hardware, accessibility peripherals, COTS software, networking and security appliances in order to ensure the required availability and performance. Provide estimates for back up elements (2.3.3.b).
- *On-site computer voting:* The service provider is responsible of deploying the required software on top of the operating system, as well as of the operating system configuration and hardening, and the accessibility peripherals configuration. (2.3.3.d).
- *Remote computer voting:* The risk assessment performed has made the assumptions that personal computers will be free of malicious software and they will have proper anti-spyware/anti-virus/anti-malware tools installed.

Risk: LOW

Although the voting terminals were properly hardened against malware, there would be some risk that malware could be undetected by the security tools (e.g. antivirus).

9.1.2.2 VOTER COERCION AND VOTE BUYING (VOTE INTEGRITY & RESULTS ACCURACY)

An individual or organization could force or bribe a voter to vote for a specific candidate through the following means:

- Voting is supervised by the coercer; and
- The voter is able, and can therefore be compelled, to show proof of his or her ballot selection.

Threat 1: The voter could be casting a vote under the surveillance of a vote buyer or coercer.

Complexity: LOW

Buying someone's vote or coercing him or her to cast a vote with a specific intention is possible but it is not common in well-established democracies.

Impact: HIGH

- Someone who is able to bribe or coerce a voter could alter the accuracy of the results.

Mitigation:

- The system must generate voting receipts that do not allow voters to prove who they had voted for to a third party (2.1.13.a).
- The system must prevent anybody, even privileged managers or auditors, to correlate votes with voters (2.1.13.b).

Risk: MEDIUM

It is possible to buy a vote or coerce a voter when voting remotely with no poll worker supervision. This is common to any remote or unsupervised voting system (such as postal ballot).

However, network voting systems allow implementation of specific measures to mitigate this risk: to allow voters to vote several times, and to only count the last vote cast.

Threat 2: A voter is able to demonstrate her voting options to a vote buyer / coercer.

Complexity / Probability: LOW

Bribing or coercing a voter to cast a vote with a specific intention is possible but it is not common in well-established democracies.

Impact: HIGH

Whoever buy votes or coerces could alter the accuracy of the results.

Mitigation:

- The system must generate voting receipts that do not allow voters to prove who they had voted for to a third party (2.1.13.a).
- The voting receipt must preserve the vote's secrecy (i.e., the selected voting options should never be able to be deduced) (2.1.14.b).
- The system must prevent anybody, even privileged managers or auditors, to correlate votes with voters (2.1.14.b).

Risk: VERY LOW

Since the voting receipt does not contain information regarding the selected voting options, the voter would not be able to demonstrate his or her ballot selection.

9.1.2.3 VOTE MODIFICATION (VOTE INTEGRITY & RESULTS ACCURACY)

The vote contents could be modified to change the election results through the following means:

- Installation of malicious software on voting computers; and
- Interception of the traffic between the voting computer and the voting server.

Threat 1: Malicious software running on the computers used to access the network voting system could modify the voting option selected by the voter.

Complexity / Probability: COMPLEX

High technical skills and deep knowledge of the network voting system would be necessary to install malicious software on voter computers that is specifically designed to modify ballot selections.

Impact: HIGH

Individual ballots could be modified.

Mitigation:

- *On-site computer voting:* The service provider must describe its needs in terms of hardware, accessibility peripherals, COTS software, networking and security appliances in order to ensure the required availability and performance. Provide estimates for back up elements (2.3.3.b).
- *On-site computer voting:* The service provider is responsible of deploying the required software on top of the operating system, as well as of the operating system configuration and hardening, and the accessibility peripherals configuration. (2.3.3.d).
- *Remote computer voting:* The risk assessment performed has made the assumptions that personal computers will be free of malicious software and they will have proper anti-spyware/anti-virus/anti-malware tools installed.

Risk: LOW

Although the voting terminals can be properly hardened against malware, there would be some risk that a program could be undetected by the security tools. However, the skills and effort required limit the attack feasibility.

Threat 2: An external attacker could intercept the communications between the voting computer and the voting server, and modify the voting option selected by the voter.

Complexity / Probability: MEDIUM

Intercepting communication lines is not a trivial undertaking: it requires appropriate knowledge and specific tools.

Impact: HIGH

Individual ballots could be modified.

Mitigation:

- The system must preserve during the whole electoral process the integrity of each individual cast vote (2.1.15.a).
- Vote integrity should be protected by means of strong cryptography, such as digital signatures (2.1.15.e).
- For computer voting, the system must protect the privacy and integrity of the cast vote, along with the voter's identity by cryptographic means, so that that the vote cannot be tampered with during its transportation or storage (1.2.5.b).
- For computer voting, the system must allow voters to protect their votes on their voting computer before casting it, instead of only protecting the votes when received in the voting servers (1.2.5.c).
- The cast votes must be protected against both external and internal attacks (e.g. system administrators) by employing appropriate cryptographic measures that can be demonstrated in front of a security expert or auditor (1.2.5.d).

Risk: VERY LOW

Since the vote will be digitally signed from the selection of the candidates, the residual risk level will be very low.

9.1.2.4 VOTE DELETION (VOTE INTEGRITY & RESULTS ACCURACY)

An attacker could try to delete valid votes by intercepting the ballot and preventing it from reaching the voting servers.

Threat 1: An external attacker could intercept the vote after it leaves the voting computer and prevent it from reaching the voting server successfully, while still making the voter believe the ballot has been successfully cast.

Complexity / Probability: MEDIUM

Intercepting communication lines is not a trivial undertaking: it requires appropriate knowledge and specific tools.

Impact: HIGH

Individual ballots could be deleted.

Mitigation:

- The system must provide voters with a voting receipt once they have cast their vote. This receipt, will allow them to verify that their vote was present during the decryption and counting process (1.2.6.a).
- The system must allow voters to verify if his/her vote was present during the decryption and Tabulation process, by means of a voting receipt (2.1.14.a).
- The communications channel must be protected by means of encryption (1.2.5.e).

Risk: VERY LOW

Since the vote will be confirmed through a verifiable voting receipt, the residual risk of deleting a vote in transit will be very low.

9.1.2.5 VOTER UNCERTAINTY ON THE CAST BALLOT (VOTE INTEGRITY & RESULTS ACCURACY)

If a voter does not have a way to verify the correct reception and count of his or her vote, the voter could develop uncertainty about the voting process.

Threat 1: The voter could feel doubtful that his or her vote has been stored in the ballot box.

Probability: HIGH

It is quite possible that a voter is uncertain that his or her electronic vote was correctly stored in the ballot box.

Impact: HIGH

The election may lose credibility.

Mitigation:

- The online ballot screen or IVR menu must be usable enough that voters can clearly distinguish their selections and be warned from making inadvertent selections or other errors (1.2.4.g, 1.2.4.h, 2.1.2.e).
- The system must provide voters with a voting receipt once they have cast their vote. This receipt, will allow them to verify that their vote was present during the decryption and counting process (1.2.6.a).

- The system must allow voters to verify if his/her vote was present during the decryption and Tabulation process, by means of a voting receipt (2.1.14.a).
- The verification process must allow the detection of manipulated or counterfeit receipts to prevent fraudulent claims by voters (2.1.14.c).

Risk: VERY LOW

Since the voter will have a voting receipt and will have the possibility of checking that his/her ballot was used in the tally, the residual risk level will be very low.

Threat 2: The voter could feel that his or her vote has not been cast properly.

Probability: HIGH

It is quite possible that many voters feel that their vote has not been cast properly.

Impact: HIGH

The elections may not have enough credibility in front of the citizens and other stakeholders.

Mitigation:

- The online ballot screen or IVR menu must be usable enough that voters can clearly distinguish their selections and be warned from making inadvertent selections or other errors. (1.2.4.g, 1.2.4.h, 2.1.2.e).
- The system must provide voters with a voting receipt once they have cast their vote. This receipt, will allow them to verify that their vote was present during the decryption and counting process (1.2.6.a).
- The system must allow voters to verify if his/her vote was present during the decryption and Tabulation process, by means of a voting receipt (2.1.14.a).
- The verification process must allow the detection of manipulated or counterfeit receipts to prevent fraudulent claims by voters (2.1.14.c).

Risk: LOW

Since the voter will have a voting receipt and will have the possibility of checking that his/her ballot was used in the count, the residual risk level will be low.

9.1.3 VOTING BY TELEPHONE

Voting by telephone involves the same categories of risk as computer voting, but the specific threats and mitigation factors are different:

- voter privacy could be compromised
- voter coercion or vote buying could be enabled
- votes could be modified after they are cast
- votes could be deleted after they are cast
- the voter could feel uncertain that their vote has been cast.

9.1.3.1 VOTER PRIVACY COMPROMISE (VOTER PRIVACY & CONFIDENTIALITY)

An attacker could violate voter privacy, linking the voter with her ballot selection through the following means:

- intercepting communications between the voting telephone and the servers;
- accessing the IVR or network voting infrastructure directly from the inside; and
- installation of malicious software on telephones used for voting.

Threat 1: An external attacker could intercept the communications between the telephone and the IVR, or between the IVR and the secure voting servers.

Complexity / Probability: MEDIUM

Intercepting telephone communication lines is not a trivial undertaking: it requires appropriate knowledge, specific tools and specific access point to monitor the telephone network. However, the communications between the IVR and the secure voting servers are a bit easier to intercept.

Impact: HIGH

Someone who did manage to intercept the communication lines would be able to see the votes cast during this time.

Mitigation:

- Whenever possible, use encryption in the communication channels (1.2.5.e).

Risk: HIGH

As the phone communication channels does not permit encryption, a telephone vote is not encrypted until it arrives at an intermediate server. In the case of analog phones, communication lines (PSTN) do not permit encryption of the line; in the case of cellular phones, the information is encrypted on its way to the relay station, but then is sent without encryption to the IVR platform; in the case of an IP phone, the information in always encrypted, but a system administrator could see all the transmitted information in the clear in the VoIP gateways, including audio messages and selected options. Therefore, the residual risk level will be high.

Threat 2: A system administrator of any intermediate infrastructure component (IVR platform …) would have access to the votes in transit, thus being able to see the voting options of the voters.

Complexity / Probability: EASY

It is easy for a system administrator of an intermediate server to access to the data in transit.

Impact: HIGH

An actor who intercepts the communications lines would see the votes cast during this time.

Mitigation:

- The service provider will be responsible for deploying the required software on top of the operating system (including application servers, databases, etc.), as well as of the operating system configuration and hardening (2.3.6.d).
- Whenever possible, use encryption in the communication channels (1.2.5.e).
- Deploy the appropriate procedures to detect any IVR administrator or other unauthorized users accessing the platform and the network during the voting period.

Risk: HIGH

Although the IVR platform will go through a process of security hardening, it is considered that there will be not enough effective controls to guarantee that an IVR platform administrator will not have access to the voting options in transit, as they are not encrypted. Therefore, the residual risk level will remain high.

Threat 3: Malicious software in the voting terminals can access the selected voting options by the voters.

Complexity / Probability: VERY COMPLEX

It would require an extremely high technical skill level, combined with very considerable effort to install malicious software on telephone devices to access/record the voting options. Currently, only certain mobile phones are targeted by a limited amount of malware, and only affecting the data channels, not the voice channel.

Impact: AVERAGE

Whoever compromises the telephone terminal could see the votes cast through this terminal.

Mitigation:

- *On-site telephone voting:* The service provider must describe its needs in terms of hardware, accessibility peripherals, COTS software, networking and security appliances in order to ensure the required availability and performance. Provide estimates for back up elements (2.3.3.b).
- *On-site telephone voting:* The service provider is responsible of deploying the required software on top of the operating system, as well as of the operating system configuration and hardening, and the accessibility peripherals configuration. (2.3.3.d).
- *Remote telephone voting:* The risk assessment performed has made the assumptions that personal telephones are standard telephones with no connections to sources of malware.

Risk: VERY LOW

The residual risk level will be very low because of the complexity of a malware phone attack to the elections and the controls that will be put in place.

9.1.3.2 VOTER COERCION & VOTE BUYING (VOTE INTEGRITY & RESULTS ACCURACY)

An individual or organization could bribe or force a voter to vote for a specific candidate through the following means:

- Voting is supervised by the coercer; and
- The voter is able, and can therefore be compelled, to show proof of his or her ballot selection;

Threat 1: The voter could be casting a vote under the surveillance of a vote buyer or coercer.

Probability: LOW

Bribing or coercing a voter is possible but it is not common in well-established democracies.

Impact: HIGH

Whoever buy votes or coerces could alter the accuracy of the results.

Mitigation:

- The system must generate voting receipts that do not allow voters to prove who they had voted for to a third party (2.1.13.a).
- The system must prevent anybody, even privileged managers or auditors, to correlate votes with voters (2.1.13.b).

Risk: MEDIUM

It is possible to bribe or coerce a voter in any scenario in which voting is done remotely with no poll worker supervision. This is common to any remote voting system.

***Note** that network voting systems allow the implementation of unique measures to mitigate this risk: to allow voters to vote several times, and to only count the last vote cast.*

Threat 2: A voter is able to demonstrate her voting options to a vote buyer / coercer.

Complexity / Probability: LOW

Buying someone's vote or coercing him or her to cast a vote with a specific intention is possible but it is not common in well established democracies.

Impact: HIGH

Whoever buy votes or coerces could alter the accuracy of the results.

Mitigation:

- The system must generate voting receipts that do not allow voters to prove who they had voted for to a third party (2.1.13.a).
- The voting receipt must preserve the vote's secrecy (i.e., the selected voting options should never be able to be deduced) (2.1.14.b).

- The system must prevent anybody, even privileged managers or auditors, to correlate votes with voters (2.1.13.b).

  Risk: VERY LOW

  Since the voting receipt does not contain information regarding the selected voting options, the voter would not be able to demonstrate his or her ballot selection.

9.1.3.3 VOTE MODIFICATION (VOTE INTEGRITY & RESULTS ACCURACY)

The vote contents could be modified to change the election results through the following means:

- Installation of malicious software on voting telephones; and
- Interception of the traffic between the telephone and the voting server.

Threat 1: Malicious software in the voting terminals can modify the voting options selected by the voters.

Complexity / Probability: VERY COMPLEX

It will require very high technical skills with a lot of effort to install malicious software (not so widespread) in telephone devices to access/record the voting options. Currently, only certain mobile phones are targeted by a limited amount of malware, and only affecting the data channels, not the voice channel.

Impact: HIGH

Individual ballots could be modified.

Mitigation:

- *On-site telephone voting:* The service provider must describe its needs in terms of hardware, accessibility peripherals, COTS software, networking and security appliances in order to ensure the required availability and performance. Provide estimates for back up elements (2.3.5.b).
- *On-site telephone voting:* The service provider is responsible for deploying the required software on top of the operating system, as well as of the operating system configuration and hardening, and the accessibility peripherals configuration (2.2.5.d).
- *Remote telephone voting:* The risk assessment performed has made the assumptions that personal telephones are standard telephones with no connections to sources of malware.

  Risk: VERY LOW

  The residual risk level will be very low because of the complexity of a malware phone attack to the elections and the controls that will be put in place.

Threat 2: An external attacker could be intercepting the communications between the voting terminal and the voting server, and modifying the voting options from a vote.

Complexity / Probability: MEDIUM

Intercept the communication lines it is not trivial: it requires appropriate knowledge, specific tools and specific access point to monitor the telephone network. However, the communications between the IVR and the secure voting servers are a bit easier to intercept.

Impact: HIGH

Individual ballots could be modified.

Mitigation:

There are no security controls strong enough to guarantee the integrity of the vote in transit, when the vote is cast by phone. Mitigations available include executing audits on the IVR infrastructure and deploying appropriate procedures to be followed by IVR operators and system administrators.

Risk: HIGH

The vote cannot be effectively protected to ensure its integrity or authenticity (i.e. digitally signed) until its arrival to a voting server, as the phone terminal does not allow this operation and trust must be placed on IVR administrators. Therefore, the residual risk level will be high.

9.1.3.4 VOTE DELETION (VOTE INTEGRITY & RESULTS ACCURACY)

An attacker could try to delete valid votes by intercepting the ballot and preventing it from reaching the voting servers.

Threat 1: An external attacker could intercept the vote after it leaves the voting telephone or IVR system and prevent it from reaching the voting server successfully, while still making the voter believe the ballot has been successfully cast.

Complexity / Probability: MEDIUM

Intercepting communication lines is not a trivial undertaking: it requires appropriate knowledge and specific tools.

Impact: HIGH

Individual ballots could be deleted.

Mitigation:

- The system must provide voters with a voting receipt once they have cast their vote. This receipt, will allow them to verify that their vote was present during the decryption and counting process (1.2.6.a).
- The system must allow voters to verify if his/her vote was present during the decryption and Tabulation process, by means of a voting receipt (2.1.8.a).

Risk: LOW

Since the vote will be confirmed through a voting receipt (verifiable once the voting period ends), the residual risk of deleting a vote in transit will be low.

9.1.3.5 VOTER UNCERTAINTY ON THE CAST BALLOT (VOTE INTEGRITY & RESULTS ACCURACY)

If a voter does not have a way to verify the correct reception and count of his or her vote, the voter could develop uncertainty about the voting process.

Threat 1: The voter could feel doubtful that his or her vote has been stored in the ballot box.

Complexity / Probability: HIGH

It is quite possible that a voter is uncertain that his or her telephone vote was correctly stored in the ballot box.

Impact: HIGH

The elections may lose credibility.

Mitigation:

- The system must provide voters with a voting receipt once they have cast their vote. This receipt, will allow them to verify that their vote was present during the decryption and counting process (1.2.6.a).
- The system must allow voters to verify if his/her vote was present during the decryption and Tabulation process, by means of a voting receipt (2.1.8.a).
- The verification process must allow the detection of manipulated or counterfeit receipts to prevent fraudulent claims by voters (2.1.8.c).

Risk: LOW

Since the voter will have a voting receipt and will have the possibility of checking that his/her ballot was used in the tally, the residual risk level will be low.

Threat 2: The voter could feel that his or her vote has not been cast properly.

Probability: HIGH

It is quite possible that a voter is uncertain that his or her telephone vote was correctly sent to and stored in the ballot box.

Impact: HIGH

The elections may not have enough credibility.

Mitigation:

- The system must provide voters with a voting receipt once they have cast their vote. This receipt, will allow them to verify that their vote was present during the decryption and counting process (1.2.6.a).
- The system must allow voters to verify if his/her vote was present during the decryption and Tabulation process, by means of a voting receipt (2.1.8.a).
- The verification process must allow the detection of manipulated or counterfeit receipts to prevent fraudulent claims by voters (2.1.8.c).

Risk: LOW

Since the voter will have a voting receipt and will have the possibility of checking that his/her ballot was used in the tally, the residual risk level will be low.

9.1.4 VOTE STORAGE & BALLOT BOX MANAGEMENT

The vote storage and ballot box management process includes the following categories of risk:

- Voter privacy compromise
- Unauthorized publication of intermediate results
- Ballot stuffing
- Vote modification
- Vote deletion
- Denial of service (election boycott)

9.1.4.1 VOTER PRIVACY COMPROMISE (VOTER PRIVACY & CONFIDENTIALITY)

A malicious insider could violate voter privacy by access the election servers directly, linking the voter with his or her ballot selection.

Threat 1: A system administrator with access to the election servers would be able to access the whole ballot box with all the cast votes.

Complexity / Probability: EASY

It would be easy for a system administrator with the right permissions to access the database storing the ballots.

Impact: VERY HIGH

Whoever accesses the ballot box would be able to see all the cast votes.

Mitigation:

- The system must guarantee that a cast ballot is secret in front of any third party, including system administrators and potential hackers that break through the conventional security measures protecting the voting platform (2.1.4.a).
- The system must guarantee that only the Network Voting Management Board can decrypt the votes, after the election, ideally in an isolated environment (e.g., without being connected to any communication network) (2.1.1.b).
- The system must guarantee that the key required to decrypt the votes is not available during the voting process until the Network Voting Management Board retrieves/reconstructs it (2.1.2.b).
- The system must guarantee that at least a pre-defined majority of Network Voting Management Board members are required in order to retrieve the election decryption key (2.1.2.c).

- The system must guarantee that votes are encrypted in a way that only the Network Voting Management Board can decrypt them (2.1.2.a, 2.1.4.c).
- The system must protect the votes (e.g., encryption) on the voter's terminal before being sent to the voting server (2.1.1.a, 2.1.4.b).
- The system must guarantee that two different votes with exactly the same content have different encryption formats (2.1.2.e).

  Risk: VERY LOW

  Since the vote will be stored in an encrypted form with no possibility of the system administrator accessing the decryption key, the residual risk level will be very low.

9.1.4.2 PUBLICATION OF NON-AUTHORIZED INTERMEDIATE RESULTS (VOTER PRIVACY & CONFIDENTIALITY)

Intermediate results could be disclosed before the election is closed, influencing those voters that have not exercised their right to vote yet. This could occur through the following means:

- Access to the voting servers;
- Interception of the votes in transit within the network voting infrastructure;
- Interception of the votes in transit from the IVR servers; and
- Tabulation of results before voting closes.

Threat 1: Someone with access to the voting servers would be able to calculate and publish intermediate results.

Complexity / Probability: EASY

It is easy for a system administrator with the right permissions to access the database storing the ballots.

Impact: HIGH

If someone calculates and publishes intermediate election results, she could be influencing those voters that have not exercised their right to vote yet, altering the final election outcome.

Mitigation:

- The system must guarantee that two different votes with exactly the same content have different encryption formats (2.1.2.e).
- The system must guarantee that a cast ballot is secret in front of any third party, including system administrators and potential hackers that break through the conventional security measures protecting the voting platform (2.1.4.a).
- The system must guarantee that only the Network Voting Management Board can decrypt the votes, after the election, ideally in an isolated environment (e.g., without being connected to any communication network) (2.1.1.b).

- The system must guarantee that the key required to decrypt the votes is not available during the voting process until the Network Voting Management Board retrieves/reconstructs it (2.1.2.b).
- The system must guarantee that at least a pre-defined majority of Network Voting Management Board members are required in order to retrieve the election decryption key (2.1.2.c).
- The system must guarantee that votes are encrypted in a way that only the Network Voting Management Board can decrypt them (2.1.2.a, 2.1.4.c).
- The system must protect the votes (e.g., encryption) on the voter's terminal before being sent to the voting server (2.1.1.a, 2.1.4.b).

Risk: VERY LOW

Since the vote will be encrypted from the vote selection until the decryption process, which will be executed at the end of the election, the residual risk level will be very low.

Threat 2: Someone with access to any intermediate infrastructure component in the network voting servers environment would have access to the votes in transit, and be able to calculate and publish intermediate results.

Complexity / Probability: EASY

It would be easy for a system administrator with the right permissions to access the database storing the ballots.

Impact: HIGH

If someone calculates and publishes intermediate election results could be influencing those voters that have not exercised their right to vote yet, altering the election results.

Mitigation:

- The system must guarantee that two different votes with exactly the same content have different encryption formats (2.1.2.e).
- The system must guarantee that a cast ballot is secret in front of any third party, including system administrators and potential hackers that break through the conventional security measures protecting the voting platform (2.1.4.a).
- The system must guarantee that only the Network Voting Management Board can decrypt the votes, after the election, ideally in an isolated environment (e.g., without being connected to any communication network) (2.1.1.b).
- The system must guarantee that the key required to decrypt the votes is not available during the voting process until the Network Voting Management Board retrieves/reconstructs it (2.1.2.b).
- The system must guarantee that at least a pre-defined majority of Network Voting Management Board members are required in order to retrieve the election decryption key (2.1.2.c).

- The system must guarantee that votes are encrypted in a way that only the Network Voting Management Board can decrypt them (2.1.2.a, 2.1.4.c).
- The system must protect the votes (e.g., encryption) on the voter's terminal before being sent to the voting server (2.1.1.a, 2.1.4.b).

Risk: VERY LOW

Since the vote will be encrypted from the vote selection until the decryption process, which will be executed at the end of the election, the residual risk level will be very low.

Threat 3: Someone accessing to any intermediate infrastructure component in the IVR platform would have access to the votes in transit, and be able to calculate and publish intermediate results.

Complexity / Probability: EASY

It would be easy for a system administrator with the right permissions to access the database storing the ballots and to intercept the unencrypted data in transit through the servers.

Impact: HIGH

If someone calculates and publishes intermediate election results could be influencing those voters that have not exercised their right to vote yet, altering the election final outcome.

Mitigation:

- The service provider will responsible of deploying the required software on top of the operating system (including application servers, databases, etc.), as well as of the operating system configuration and hardening (2.2.3.e).
- There is no effective mitigation to avoid IVR administrators to access the data in transit. Several procedures limiting system access must be put in place to increase the complexity of this risk happening.

Risk: HIGH

Although the IVR platform will go through a process of security hardening, it is considered that there will be not enough effective controls to guarantee that an IVR platform administrator will not have access to the ballots cast by the voters. Therefore, the residual risk level will remain high.

Threat 4: An electoral official could perform the Tabulation process before the end of the voting period and obtain intermediate results.

Complexity / Probability: EASY

An electoral official could easily try to perform the Tabulation process before the end of the voting period.

Impact: HIGH

If someone calculates and publishes intermediate election results could be influencing those voters that have not exercised their right to vote yet, altering the election outcome.

Mitigation:

The system must guarantee that only the Network Voting Management Board can decrypt the votes, after the election, ideally in an isolated environment (e.g., without being connected to any communication network) (2.1.1.b).

The system must guarantee that the key required to decrypt the votes is not available during the voting process until the Network Voting Management Board retrieves/reconstructs it (2.1.2.b).

The system must guarantee that at least a pre-defined majority of Network Voting Management Board members are required in order to retrieve the election decryption key (2.1.2.c).

The system must guarantee that votes are encrypted in a way that only the Network Voting Management Board can decrypt them (2.1.2.a, 2.1.4.c).

The system uses an Network Voting Management Board for decrypting the cast votes (2.1.7.a).

The system uses a N of M threshold scheme of Network Voting Management Board members for retrieving the key that allows the decryption of the votes (2.1.7.b).

It must be impossible for an individual member or a number of members below the threshold, to retrieve the election decryption key (2.1.7.c).

The system must support the use of tamper proof devices (e.g., PIN protected smartcards) for storing the information required by each Network Voting Management Board member in order to retrieve the election decryption key (2.1.7.d).

The threshold scheme is based on cryptographic means (e.g., secret sharing scheme) (2.1.7.e).

The decryption key is destroyed by the threshold scheme and does not exist until it is reconstructed by the Network Voting Management Board members at the end of the election (2.1.7.f).

Risk: VERY LOW

Since the vote will be encrypted until the decryption process, which will be executed at the end of the election by a qualified majority, the residual risk level will be very low.

9.1.4.3 BALLOT STUFFING (VOTE INTEGRITY & RESULTS ACCURACY)

An attacker can try to add to the ballot box votes from voters that did not participate in the voting process. This could be done through the following means:

A malicious insider could insert votes directly into the database;

An internal or external attacker could insert votes directly into the database; and

A prepared ballot box could be loaded into the voting server before voting begins.

Threat 1: Someone with access to the voting servers and with access to the ballot box could try to insert votes directly into the database.

Complexity / Probability: EASY

It is easy for a system administrator with the right permissions to access the database storing the ballots.

Impact: VERY HIGH

Whoever accesses the voting server would have access to the database directly to insert a new vote, altering the election results.

Mitigation:

The system must prevent the addition of counterfeit votes from both external users and system administrators (2.1.6.b, 2.1.5.d).

The system, for audit purposes, must allow to accurately trace the processes that concluded with the casting and storage of a vote in a ballot box (2.1.6.c).

Vote integrity should be protected by means of strong cryptography, such as digital signatures (2.1.5.e).

The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and Tabulation process (2.1.6.a).

Risk: VERY LOW

Since the integrity of digital ballot box will be protected and the votes will be digitally signed, the residual risk level will be very low.

Threat 2: An internal or external attacker could cast votes from an intermediate server or other voting system component (avoiding the filters that prevent such behaviour from voters).

Complexity / Probability: MEDIUM

It is not trivial to have access the intermediate servers. In this specific case, internal attacks are not being considered, as they are covered in the description of the previous attack.

Impact: HIGH

Whoever accesses an intermediate server could alter the accuracy of the results casting additional votes.

Mitigation:

The system must prevent the addition of counterfeit votes from both external users and system administrators (2.1.6.b, 2.1.5.d).

The system, for audit purposes, must allow to accurately trace the processes that concluded with the casting and storage of a vote in a ballot box (2.1.6.c).

The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and Tabulation process (2.1.6.a).

Vote integrity should be protected by means of strong cryptography, such as digital signatures (2.1.5.e).

Risk: VERY LOW

Since the authenticity of the votes stored in the digital ballot box will be guaranteed, the residual risk level will be very low.

Threat 3: Before the election starts, a malicious insider could load a prepared ballot box into the voting servers.

Complexity / Probability: EASY

It is easy for a system administrator with the right permissions to access the database storing the ballots and placing a prepared ballot box that already contains votes.

Impact: VERY HIGH

Whoever accesses the voting servers would have access to the whole ballot box, to allocate a ballot box containing counterfeit votes.

Mitigation:

The system must protect the integrity and authenticity of the election information used to configure the voting platform (1.1.1.b).

The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and Tabulation process (2.1.6.a).

The system must prevent the addition of counterfeit votes from both external users and system administrators (2.1.6.b, 2.1.5.d).

The system, for audit purposes, must allow to accurately trace the processes that concluded with the casting and storage of a vote in a ballot box (2.1.6.c).

Vote integrity should be protected by means of strong cryptography, such as digital signatures (2.1.5.e).

Risk: VERY LOW

Since the integrity and authenticity of the digital ballot box will be protected, and the votes shall be digitally signed by voters, the residual risk level will be very low.

9.1.4.4 VOTE MODIFICATION (VOTE INTEGRITY & RESULTS ACCURACY)

The vote contents could be modified to change the election results.

Threat 1: A system administrator or an external attacker could access the ballot box directly and modify the contents of a valid vote.

Complexity / Probability: EASY

It would be easy for a system administrator with the right permissions to access the database storing the ballots.

Impact: VERY HIGH

Anyone accessing the whole ballot box could modify all the votes, seriously altering the election results.

Mitigation:

Vote integrity should be protected by means of strong cryptography, such as digital signatures (2.1.5.e).

The system, for audit purposes, must allow to accurately trace the processes that concluded with the casting and storage of a vote in a ballot box (2.1.6.c).

The system must preserve during the whole electoral process the integrity of each individual cast vote (2.1.5.a).

The system must protect the privacy and integrity of the cast vote, along with the voter's identity by cryptographic means, so that that the vote cannot be tampered with during its transportation or storage (1.2.5.b).

The cast votes must be protected against both external and internal attacks (e.g. system administrators) by employing appropriate cryptographic measures that can be demonstrated in front of a security expert or auditor (1.2.5.d).

Risk: VERY LOW

Since the integrity and authenticity of the digital ballot box will be protected, and the votes shall be digitally signed by voters, the residual risk level will be very low.

9.1.4.5 VOTE DELETION (VOTE INTEGRITY & RESULTS ACCURACY)

An attacker could try to delete valid votes from the ballot box.

Threat 1: A system administrator or an external attacker could access the ballot box directly and remove a valid vote.

Complexity / Probability: EASY

It is easy for a system administrator with the right permissions to access the database storing the ballots.

Impact: VERY HIGH

Several ballots could be deleted, affecting election accuracy.

Mitigation:

- The system must implement adequate measures for detecting any attempt to delete a vote from the ballot box (2.1.6.d).
- The system, for audit purposes, must allow to accurately trace the processes that concluded with the casting and storage of a vote in a ballot box (2.1.6.c).
- The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and Tabulation process (2.1.6.a).
- The system must provide voters with a voting receipt once they have cast their vote. This receipt, will allow them to verify that their vote was present during the decryption and counting process (1.2.6.a).
- The system must allow voters to verify if his/her vote was present during the decryption and Tabulation process, by means of a voting receipt (2.1.8.a).

Risk: VERY LOW

Since the integrity of the digital ballot box will be protected, the residual risk level will be very low.

9.1.4.6 ELECTION BOYCOTT-DENIAL OF SERVICE (ELECTION SYSTEMS AVAILABILITY)

An attacker could disrupt the availability of the voting channel by performing a denial of service attack by flooding the system with requests.

Threat 1: The voting system could be flooded with false voting requests to overload the system and prevent valid votes from being received.

Complexity / Probability: EASY

Basic technical skills would be required to flood the voting system with simulated voting requests. These requests could take the form of login requests, page loads, or other requests that use server resources.

Impact: HIGH

Voting system could be unavailable at critical times.

Mitigation:

- The voting system must provide monitoring tools that ensure the detection of any anomalies during the voting process (1.2.8.a).
- The voting system must be available 99.95% during the voting period (2.2.1.a).
- The voting system must be able to support enough concurrent computer-based voters and enough telephone-based voters in parallel. (2.2.1.b). The number of lines will depend on the number of expected voters. If there are 2 telephones per voting centre, there should be at least 20 lines available.

- The voting terminals located in the polling stations must be able to operate during the whole voting period (2.2.1.c).
- The system should be able to run elections for thousands to millions of voters in an easy and cost-efficient way (2.4.1.a).
- The system must allow the addition of new components without having to stop the service, e.g. for supporting a larger number of voters (2.4.1.b).
- The system must be able to operate in two different environments in parallel: on-site (from polling places) and remotely (from anywhere) (2.4.2.d).
- The service provider is responsible of deploying the required software on top of the operating system (including application servers, databases, etc.), as well as of the operating system configuration and hardening (2.2.2.d).

Risk: LOW

Since there will be several controls to detect and stop a denial of service attack, and provided that the voting system will be available for at least six days, the residual risk level will be low.

Threat 2: The voting servers could be flooded with malicious requests to force server failure and prevent any network votes from being received.

Complexity / Probability: EASY

Basic technical skills will be required to flood the voting servers with malicious requests.

Impact: HIGH

Voting system could be unavailable at critical times.

Mitigation:

- The service provider is responsible of deploying the required software on top of the operating system (including application servers, databases, etc.), as well as of the operating system configuration and hardening (2.2.2.d).
- The voting system must provide monitoring tools that ensure the detection of any anomalies during the voting process (1.2.8.a).
- The voting system must be available 99.95% during the voting period (2.2.1.a).

Risk: LOW

Since there will be several controls to detect and stop a denial of service attack, and provided that the voting system will be available several days, the residual risk level will be low.

9.1.5 TABULATION

The tabulation process is exposed to several risk areas:

- Voter privacy compromise
- Ballot stuffing
- Vote modification
- Vote deletion
- Modification of voter results

9.1.5.1 VOTER PRIVACY COMPROMISE (VOTER PRIVACY & CONFIDENTIALITY)

An attacker could violate the voter's privacy and correlate a voter with their selected voting options.

Threat 1: An electoral official could have access to the votes on the Tabulation process, identifying the voting options of each voter.

Complexity / Probability: MEDIUM

It would be difficult for an electoral official to have direct access to the vote contents during the Tabulation process provided it is performed in front of multiple stakeholders.

Impact: HIGH

Anyone having access to Tabulation process would see all the votes.

Mitigation:

- The decryption and counting process must be carried out in an isolated environment that is not connected to the Internet (1.3.2.a).
- The decryption and Tabulation process must ensure that it is impossible to correlate the order of the decrypted votes with the order they were cast and therefore, prevent any link between the decrypted votes and the voters (e.g., by using a Mixing process) (1.3.2.g).
- The system must guarantee that it is impossible to correlate the order in which the votes were decrypted with the order in which they were cast (2.1.2.d).

Risk: VERY LOW

Since there is a process that ensures that is impossible to correlate the cast ballots and the voters, the residual risk level will be very low.

9.1.5.2 BALLOT STUFFING (VOTE INTEGRITY & RESULTS ACCURACY)

During the Tabulation process, a malicious insider could try to add votes from voters that did not participate in the voting process.

Threat 1: An electoral official could add counterfeit votes to the system during the Tabulation process.

Complexity / Probability: MEDIUM

It is not trivial for an electoral official to add counterfeit votes during the Tabulation process, provided it is performed in front of multiple stakeholders. The electoral official would also need certain advance technical knowledge to add counterfeit ballots in a network voting system.

Impact: VERY HIGH

Anyone adding counterfeit votes could alter the accuracy of the results.

Mitigation:

- The decryption and counting process must be carried out in an isolated environment that is not connected to the Internet (1.3.2.a).
- The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and Tabulation process (2.1.6.a).
- The system must prevent the addition of counterfeit votes from both external users and system administrators (2.1.6.b, 2.1.5.d).
- The system must allow independent auditors or the Network Voting Management Board to carry out new decryption and tabulation processes if required (1.3.5.a).
- The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes (1.3.5.b).
- The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes (1.3.5.c).

Risk: VERY LOW

Since the digital ballot box will be protected and isolated, and any operations on it will be tacked, the residual risk level will be very low.

9.1.5.3 VOTE MODIFICATION (VOTE INTEGRITY & RESULTS ACCURACY)

The vote contents could be modified to change the election results.

Threat 1: During the Tabulation process, an electoral official could replace valid votes with counterfeit votes, or even replace the whole ballot box with a counterfeit one.

Complexity / Probability: MEDIUM

It would be difficult for an electoral official to add counterfeit votes or even replace the whole ballot box during the Tabulation process, provided it is performed in front of multiple stakeholders. The electoral official would also need advance technical knowledge to add counterfeit ballots in a network voting system.

Impact: VERY HIGH

Anyone accessing the whole ballot box could modify any or all the votes.

Mitigation:

- The decryption and counting process must be carried out in an isolated environment that is not connected to the Internet (1.3.2.a).
- The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and Tabulation process (2.1.6.a).
- The system must allow independent auditors or the Network Voting Management Board to carry out new decryption and tabulation processes if required (1.3.5.a).
- The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes (1.3.5.b).
- The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes (1.3.5.c).

Risk: VERY LOW

Since the digital ballot box will be protected and isolated, and any operations on it will be tacked, the residual risk level will be very low.

9.1.5.4 VOTE DELETION (VOTE INTEGRITY & RESULTS ACCURACY)

A malicious insider could try to delete valid votes from the ballot box.

Threat 1: During the Tabulation process, an electoral official could remove votes from the system.

Complexity / Probability: MEDIUM

It would be difficult for an electoral official to remove votes during the Tabulation process, provided it is performed in front of multiple stakeholders. The electoral official would also need advance technical knowledge to remove ballots in a network voting system.

Impact: VERY HIGH

Anybody removing counterfeit votes could alter the accuracy of the results.

Mitigation:

- The decryption and counting process must be carried out in an isolated environment that is not connected to the Internet (1.3.2.a).
- The system must implement adequate measures for detecting any attempt to delete a vote from the ballot box (2.1.6.d).
- The system must provide voters with a voting receipt once they have cast their vote. This receipt will allow them to verify that their vote was present during the decryption and counting process (1.2.6.a).
- The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and Tabulation process (2.1.6.a).

- The system must allow independent auditors or the Network Voting Management Board to carry out new decryption and tabulation processes if required (1.3.5.a).
- The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes (1.3.5.b).
- The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes (1.3.5.c).

Risk: VERY LOW

Since the digital ballot box will be protected and isolated, and any operations on it will be tacked, the residual risk level will be very low.

9.1.5.5 MODIFICATION OF VOTING RESULTS (VOTE INTEGRITY & RESULTS ACCURACY)

The election results can be altered without modifying the votes or the ballot box, but by manipulating the Tabulation or counting processes.

Threat 1: An electoral official could alter the voting results during the counting process.

Complexity / Probability: MEDIUM

It would be difficult for an electoral official to alter the counting process, provided it is performed in front of multiple stakeholders.

Impact: VERY HIGH

Election results could be compromised.

Mitigation:

- The decryption and counting process must be carried out in an isolated environment that is not connected to the Internet (1.3.2.a).
- The system must allow independent auditors or the Network Voting Management Board to carry out new decryption and tabulation processes if required (1.3.5.a).
- The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes (1.3.5.b).
- The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes (1.3.5.c).
- The information transferred to Elections Ontario's EMS must be protected to ensure its integrity and authenticity (1.3.3.c).

Risk: VERY LOW

Since the counting process will be executed in an isolated environment, the integrity of the digital ballot box will be controlled and the tabulation results will be protected, the residual risk level will be very low.

Threat 2: The voting application could modify the voting results during the counting process.

Complexity / Probability: MEDIUM

It is would be difficult for a programmer with access to the voting application to modify the software to alter the voting results undetected, considering that the code should have gone through an audit process before the election and that the counting process is done in an isolated environment in front of several stakeholders.

Impact: VERY HIGH

Election results could be compromised.

Mitigation:

- Auditors must have access to the source code of the system if requested by Elections Ontario (1.4.2.a).
- The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and Tabulation process (2.1.6.a).
- The system must allow independent auditors or the Network Voting Management Board to carry out new decryption and tabulation processes if required (1.3.5.a).
- The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes (1.3.5.b).
- The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes (1.3.5.c).

Risk: LOW

In addition to the software certification/audit process, independent counting processes could be done to verify the obtained results.

Threat 3: An attacker (external or internal) could modify the election results after the counting process.

Complexity / Probability: MEDIUM

Modify the election results after the counting process is not trivial, considering that the counting process is done in an isolated environment in front of several stakeholders.

Impact: VERY HIGH

Election results could be compromised.

Mitigation:

- The decryption and counting process must be carried out in an isolated environment that is not connected to the Internet (1.3.2.a).
- The components of the voting system used for election configuration and ballot decryption/tabulation must run in an isolated environment composed of one or more servers/computers (2.2.4.a).
- The information transferred to Elections Ontario's EMS must be protected to ensure its integrity and authenticity (1.3.3.c).
- The system must allow independent auditors or the Network Voting Management Board to carry out new decryption and tabulation processes if required (1.3.5.a).
- The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes (1.3.5.b).
- The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes (1.3.5.c).

Risk: VERY LOW

Since the results of the counting process will be protected independent counting processes could be done to verify the obtained results, the residual risk level will be very low.

Threat 4: An attacker (external or internal) could modify the published election results.

Complexity / Probability: MEDIUM

Modify the election results after the counting process and once published would be difficult, unless the website is hosted in a rather insecure environment. A modification would imply a successful hacker attack that is able to replace web contents. Internal attacks are less feasible, as the attacker would be immediately detected

Impact: AVERAGE

The image of the Election authorities could be damaged.

Mitigation:

- The information transferred to Elections Ontario's EMS must be protected to ensure its integrity and authenticity (1.3.3.c).
- Dissemination channels (e.g. a public website) must be protected in front of external attacks

Risk: VERY LOW

Since the results of the counting process will be protected, and that the attack can be easily detected and solved, the residual risk level will be very low.

9.1.6 ELECTION AUDITING

Election auditing could be compromised due to inaccuracy or incompleteness of the data required to support an audit.

9.1.6.1 AUDITABILITY - INACCURATE AUDITABILITY

Not enough election traceability or audit data that is easy to tamper with may allow attackers to hide any unauthorized behaviour.

Attack: The voting systems are not registering enough audit information to verify the voting process or the Tabulation process.

Complexity / Probability: EASY

It could be possible to not register enough (or any) audit information during the voting process.

Impact: HIGH

Election results could be questioned because a valid audit is not possible.

Mitigation:

- The system logs and election information generated during the election must allow a meaningful audit of the election without requiring that auditors have access to any private key, or assuming the role of any privileged actor (2.1.10.b).
- The system must allow auditors to retrace any election process, in a meaningful manner, without compromising the election privacy or accuracy (2.1.10.a).
- The system must implement adequate cryptographic practices for verifying the accuracy and integrity of the log information to be used during the audit (2.1.10.c).
- The system must allow any independent auditor to check and certify the integrity of the application components at any time during the election (2.1.10.d).
- The service provider must describe its approach for an end-to-end auditable process (2.2.5.e).
- The system, for audit purposes, must allow to accurately trace the processes that concluded with the casting and storage of a vote in a ballot box (2.1.6.c).
- The system must facilitate a meaningful audit of the system by trusted third party auditors based on the stored election information and logs (1.4.2.c).
- Auditors must be able to check the integrity and authenticity of the election information and logs to detect any manipulation attempt of such audit information (1.4.2.e).

Risk: LOW

Since there will be controls to ensure the registration of information about the voting process and the Tabulation process, the residual risk level will be reduced to low.

Threat 1: The voting system components register counterfeit audit information to demonstrate that a fraudulent election was valid.

Complexity / Probability: MEDIUM

It would require some effort to modify or introduce false audit information into the application logs.

Impact: HIGH

Election results could be questioned because the logs information are inaccurate or falsified.

Mitigation:

- The system must implement adequate cryptographic practices for verifying the accuracy and integrity of the log information to be used during the audit (2.1.10.c).
- Auditors must be able to check the integrity and authenticity of the election information and logs to detect any manipulation attempt of such audit information (1.4.2.e).
- The service provider must describe its approach for an end-to-end auditable process (2.2.5.e).

Risk: VERY LOW

Since the external auditing of the election process will certainly review the audit information to ensure that there had not been fraudulent actions, the residual risk level will be very low.

Threat 2: The audit information could be modified by an attacker – without detection – to demonstrate that a fraudulent election was considered valid, or to revoke a valid election.

Complexity / Probability: MEDIUM

It would require reasonable technical skills for an attacker to modify the audit information.

Impact: HIGH

Election results could be compromised because of its lack of auditability.

Mitigation:

- The system must implement adequate cryptographic practices for verifying the accuracy and integrity of the log information to be used during the audit (2.1.10.c).
- Auditors must be able to check the integrity and authenticity of the election information and logs to detect any manipulation attempt of such audit information (1.4.2.e).
- The service provider must describe its approach for an end-to-end auditable process (2.2.5.e).

Risk: VERY LOW

Since the audit information (logs) will be protected and the system will not allow modifications to pass undetected, the residual risk level will be very low.

9.2 OPERATIONAL RISK ASSESSMENT

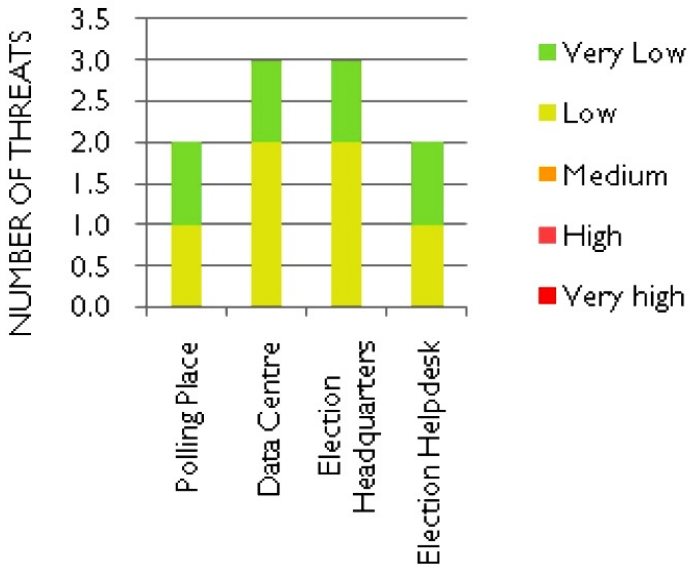
This section assesses a series of operational risks related to the recommended Network Voting model. Generic risks that apply to any standard project are not assessed. It is organized into four sections, one for each of the following areas of operation:

- Polling Places
- The data centre
- Elections Ontario's Head Office
- The Help Desk supporting the Network Voting initiative

The chart at right presents a summary of the operational risk assessment for the network voting model recommended by this Business case.

It displays the number of potential threats for each operational area, as well as the residual risk level that would be in place, given that provided that the appropriate mitigation steps are taken. As can be seen on the chart, all of the operational threats that have been identified can be mitigated to the point where they present only a low or very low risk.

Figure 12: Operational Risks



9.2.1 POLLING PLACE OPERATIONS

Threat: The terminals used for voting and/or managing the list of voters are not fully operative and cannot be used properly.

Probability: MEDIUM

There are many factors involved in the process of setting up polling places, including HW/SW, communications, procedures and infrastructure and therefore the likelihood of issues appearing will raise with the number of polling places.

Impact: MEDIUM

Unavailability of polling places can lead to voters not being able to cast their vote conveniently, forcing them to vote remotely or having to make long queues, which could damage the image of the NVS.

Mitigation:

- An experienced project team will be able to foresee issues and plan accordingly.
- Adequate testing needs to be carried out, including an end-to-end test if possible.
- Appropriate backup countermeasures (personnel, equipment, procedures, etc.) must be set up and tested.

Risk: LOW

The proposed mitigation measures make the residual risk level to be very low.

Threat: The electoral officials in charge of operating the different NVS components are unable to operate them correctly.

Probability: MEDIUM

Although the systems to be operated are not very complex, some necessary training must be delivered. The probability will increase with the number of polling places.

Impact: LOW

In most of the cases, this type of issues will affect only one poll worker or only one polling place, and therefore it should not be critical for the whole election.

Mitigation:

- Appropriate training and support must be provided to electoral officials. Appropriate backup teams are also required.
- Participation
- The NVS interfaces must be easy to use by electoral officials, to avoid confusing electoral officials during the operation of the systems and/or making their work harder and/or slower.

- Electoral officials interfacing with the NVS must be pre-selected considering some computer knowledge at user-level.

Risk: VERY LOW

The proposed mitigation measures make the residual risk level to be very low.

9.2.2 DATA CENTRE OPERATIONS

Threat: Certain required NVS central components, may it be hardware, software or communications related, are missing.

Probability: LOW

It is unlikely that some components are not present and that is not detected on time.

Impact: VERY HIGH

In the case that any component was missing, it could have a major impact on the NVS's performance, and it could eventually affect the whole election.

Mitigation:

- Appropriate planning and thorough testing is required (including a back-up plan). Periodic controls could be set up.
- Enough time is allocated for system procurement and deployment.
- Strong physical security measures must be set up for the Data Centre to prevent unauthorised personnel from accessing the NVS.
- A Monitoring System that reports any potential issue should be implemented.

Risk: VERY LOW

The proposed mitigation measures make the residual risk level to be very low.

Threat: Certain required NVS central components, whether hardware, software, or communications related, are functioning incorrectly, by themselves or when interacting with other elements.

Probability: HIGH

Data centres deployments are very complex, including the configuration of each component and their integration as a single system.

Impact: HIGH

In the case that any component was misconfigured or incorrectly integrated, it could have a major impact on the NVS's performance, and it could eventually affect the whole election.

Mitigation:

- Allocate enough time for system deployment and components integration.
- Thorough testing at different levels on the real production environment previously to the election.
- A back-up plan must be set up.
- A Monitoring System that reports any issue should be implemented.

Risk: LOW

The proposed mitigation measures make the residual risk level to be low.

Threat: Data centre technicians in charge of monitoring the correct operation of the NVS infrastructure behave (intentionally or unintentionally) in an incorrect way.

Probability: LOW

The data centre can be difficult to set up, but its daily operation should not be very complex.

Impact: VERYHIGH

Incorrect operation or procedures could potentially affect the whole election.

Mitigation:

- Data Centre technicians must receive appropriate training. Back-up personnel must be available.
- Clear procedures describing how to operate the data centre must be provided.
- Measures against possible corruption and coercion of personnel must be taken.
- A Monitoring System that reports any failure should be implemented.
- The NVS should feature audit tools to ensure that any wrong doing is detected, as well what caused it.

Risk: LOW

The proposed mitigation measures make the residual risk level to be low.

9.2.3 EO HEADQUARTERS OPERATIONS

Threat: The NVS components are not available or fully operative when required.

Probability: LOW

The Headquarters is a central place for the election and therefore it has high visibility. For that reason it is unlikely that any of its NVS components are overlooked or not thoroughly tested.

Impact: VERY HIGH

This situation could potentially affect the entire election during a long period of time.

Mitigation:

- Allocate enough time for system procurement and deployment.
- Appropriate planning and thorough testing is required (including a back-up plan).
- Strong physical security measures must be set up for the Head Quarters to prevent unauthorised personnel from accessing the NVS.

Risk: LOW

The proposed mitigation measures make the residual risk level to be low.

Threat: Certain critical data required to configure/operate the NVS is incorrect or not available on time.

Probability: LOW

How to provide critical data shall be defined early in the project, and it should not be a complex process to carry out.

Impact: VERY HIGH

There is data that can be critical for the election, and without it the election cannot take place.

Mitigation:

- Accurate definition of the format and the procedures for the data to be used by EO.
- Accurate definition of data exchanges.
- Accurate testing with data as much real (in contents, format and volumes) as possible before the election.

Risk: LOW

The proposed mitigation measures make the residual risk level to be low.

Threat: The technicians in charge of operating the NVS components located in the headquarters do not operate them correctly (intentionally or unintentionally).

Probability: LOW

The Headquarters is a central place for the election and therefore it has high visibility. For that reason it is unlikely that any personnel operating the NVS there do not do it correctly.

Impact: VERY HIGH

This situation could potentially affect the entire election, stopping it for a long period of time.

Mitigation:

- Appropriate training and support must be provided to Headquarters' personnel. Appropriate backup teams are also required.
- Clear procedures describing how to operate the NVS must be provided.
- Measures against possible corruption and coercion of personnel must be taken.
- A Monitoring System that reports any failure should be implemented.
- The NVS should feature audit tools to ensure that any wrong doing is detected, as well what caused it.

Risk: VERY LOW

The proposed mitigation measures make the residual risk level to be very low.

9.2.4 HELP DESK OPERATIONS

Threat: Help desk is unable to provide suitable support to Election Officials employing the NVS at the polling places.

Probability: VERY LOW

The number of different issues that can happen on the polling places is limited, and they should not be complex to solve. Furthermore, the personnel staffing the Help Desk will be well trained and have access to additional levels of support (from EO, or from the vendor's technical staff). Therefore, it is unlikely that the Help Desk could not provide appropriate support.

Impact: LOW

Mitigation:

- Appropriate dimensioning and training must be provided to the support team. Enough backup personnel is also required.
- Second and third support level of support (appropriately sized, trained and with backup personnel) must be available.
- All the help guides and procedures (including escalation) must be set up.
- Appropriate help desk tools provided to the support team.

Risk: VERY LOW

The proposed mitigation measures make the residual risk level to be very low.

Threat: Help desk is unable to provide suitable support to voters employing the NVS remotely.

Probability: MEDIUM

Individual voters can have many different issues with different nature, and sometimes it will be difficult for help desk personnel to identify them and provide a solution.

Impact: LOW

It can happen that in the end a few voters cannot use the remote voting interface, but they can always visit a polling place.

Mitigation:

- Appropriate dimensioning and training must be provided to the support team. Enough backup personnel is also required.
- Second and third support level of support (appropriately sized, trained and with backup personnel) must be available.
- All the help guides and procedures (including escalation) must be set up.
- Allow voting during multiple days, so remote voters that cannot vote from a place, can try a different place (e.g. another computer) or even visit a polling place.

Risk: LOW

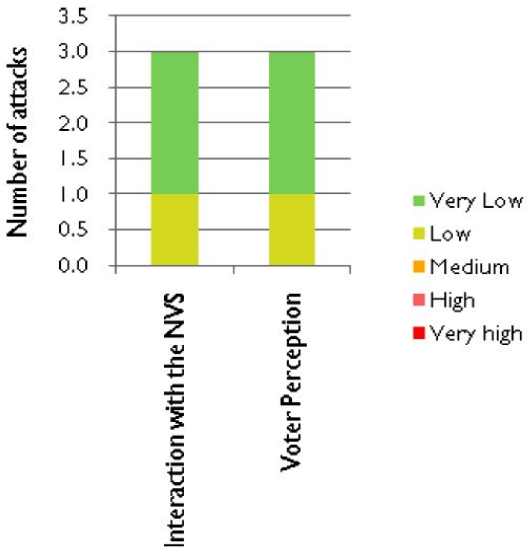
The proposed mitigation measures make the residual risk level to be low.

9.3 VOTER RISK ASSESSMENT

The risks assessed in this section are related to voters, and include their interaction with the network voting system at different stages, their perceptions of the system in particular, and their perception of network voting in general.

The chart at right presents a summary of the voter risk assessment for a network voting model recommended by this Business Case. It displays the number of potential threats, as well as the residual risk level that would be in place given that provided that the appropriate mitigation steps are taken. As can be seen on the chart, all of the operational threats that have been identified can be mitigated to the point where they present only a low or very low risk.

Figure 13: Voter Risk Assessment



9.3.1 INTERACTION WITH THE NETWORK VOTING SYSTEM

Threat: The interaction with the NVS is not easy and intuitive for voters.

Probability: MEDIUM

If the authentication process and/or the voting process are complicated, it can lead to complex actions to be taken by voters and their disfranchisement.

Impact: MEDIUM

Public perception of EO and the NVS could be not as good as desired.

Mitigation:

- The system should provide a user-friendly voter interface, so that the voting process is intuitive and no previous training for using the network voting system is necessary (2.3.1.a).
- The system must support the use of the main Internet browsers and operating systems, and of standard telephones (2.3.1.b).
- The system must include easy to understand instructions for voters (2.3.1.c).
- The system must warn voters if, during the voting process, they make a selection that could invalidate their vote (e.g., under voting, over voting) (2.3.1.d).
- Voters must select their voting options by directly selecting the candidate instead of using a code or indirect selection method (2.3.1.e).

Risk: LOW

The proposed mitigation measures make the residual risk level to be low

Threat: The NVS system provides insufficient accessibility features that impede certain voters to vote on their own without the help of a third party.

Probability: MEDIUM

The lack of assistive devices and/or an incompatible voting interface would undermine the voting capability of electors with certain disabilities.

Impact: MEDIUM

This situation will only affect specific group of voters.

Mitigation:

- The system must support the use of multiple languages without compromising the voter's privacy (2.3.2.a).
- The system must be compliant with WGAI accessibility standards for remove voting (2.3.2.b).
- The system must support visual impaired voters using screen readers (JAWS) and screen magnifiers (2.3.2.c).
- The system must support motor disabled voters using sip & puff or equivalent technologies (2.3.2.d).
- The voting interfaces should be validated by representatives of the collectives of voters with disabilities that would use them (visually-impaired voters, disabled people, etc.).

Risk: VERY LOW

The proposed mitigation measures make the residual risk level to be very low.

Threat: The registration process required to use the network voting channel is too complex to make a critical mass of voters to participate.

Probability: MEDIUM

The registration process would have an inherent complexity for some voters, but it should not affect a majority.

Impact: LOW

In the case of the Threat happening, the percentage of voters using the NVS would be low, but the election transparency and integrity would not be compromised.

Mitigation:

- The registration process must be simple and straightforward. In the case that it requires personal data from the voters, that data should be easily known by them.
- The data from voters stored in the database must be reviewed to ensure that it is not too old or contains too many errors.
- If the process relies on third parties (such as the postal service) a backup process must be set up for any issues related to it (e.g. delivery to the wrong addressee, etc.).
- There should be alternate registration or even voting channels that do not require a specific registration process (e.g. voting from polling places by showing a standard ID).

Risk: VERY LOW

The proposed mitigation measures make the residual risk level to be very low.

9.3.2 VOTER PERCEPTION

Threat: Voters may distrust the NVS and believe that it does not fulfill the required principles to be followed by an electoral process. This situation would reduce the number of e-voters.

Probability: MEDIUM

There are some anti-Network voting activist groups but they are not the majority of the population.

Impact: LOW

Perception of the NVS can be affected, reducing the participation rate. However, it should not have a major impact on the election itself.

Mitigation:

- A detailed communication plan must be created to ensure every voter knows how the system addresses any potential issue.
- Electoral authorities must behave transparently by answering any question received from voters and other stakeholders.
- The NVS to be employed must be easy to explain to the citizens, and all the information about the security measures it implements must be publicly available.

Risk: LOW

The proposed mitigation measures make the residual risk level to be low.

Threat: Certain voters may try, and perceive incorrectly, that they can deceive the NVS.

Probability: VERY LOW

Not many people will try to attack the system and misunderstand the system's behaviour.

Impact: LOW

In the case the Threat happened, perception of the NVS by individual voters would be affected, but it would not be in a large scale, because in that case someone else would prove the perception was wrong.

Mitigation:

- The NVS must provide accurate feedback to voters to ensure they do not have a wrong understanding of what they do (they do not think they have been able to vote twice or more times, that their vote has not been cast, etc.).
- Procedures to verify that a vote has been cast should be implemented.

Risk: VERY LOW

The proposed mitigation measures make the residual risk level to be very low.

Threat: A majority of voters are not aware of the availability of network voting channels.

Probability: MEDIUM

It is possible that the existence of a new network voting channels is not well publicised and awareness remains low.

Impact: LOW

If a majority of voters are not aware of the network voting channels, the percentage of voters using the NVS would be low but the election itself would not be compromised.

Mitigation:

- A dissemination plan (including advertising, media campaigns, etc.) must be designed and carried out on time.
- Key stakeholders should be actively consulted during project delivery.
- Different stakeholders and notable actors in Ontario should be made aware of the project so they can do parallel communications.

Risk: VERY LOW

The proposed mitigation measures make the residual risk level to be very low.

10. SUCCESS CRITERIA

This section provides a set of key criteria that will be critical to the success of the Network Voting pilot, including a set of metrics that will help assess the outcomes of a Network Voting pilot.

THE SUCCESS OF the Network Voting pilot will be based on three related sets of criteria:

1. the pilot must implement a system that preserves and records evidence of a continuous '**chain of trust'** that controls custody of the ballot data;
2. an experienced project team must execute an effective **implementation approach**; and
3. the pilot must support the core Network Voting **principles** defined in Section 3, above.

10.1 CHAIN OF TRUST

The success and integrity of an election depends on eliminating the possibility that ballots have been tampered with during or after the act of casting them. In a Network Voting system, tampering could occur through the installation of malicious code at some point in the ballot custody chain. To prove election integrity, Elections Ontario must be able to demonstrate that only authorized parties and software have come into contact with the digital ballot data. A strong emphasis must be placed on audit. Independent auditors must be able to review the source code, verify the build and deployment, audit system logs during the election event, and finally to review both the counting process and the results.

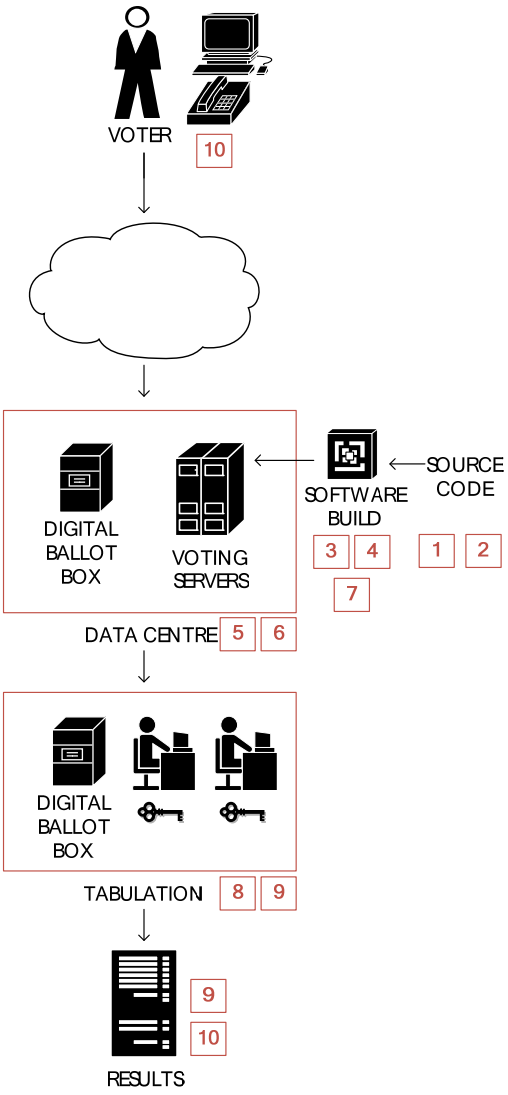
In case of an allegation of tampering, the resolution of the issue would be based on forensics: experts will need to validate the integrity of the chain of trust based on available evidence. If the implementation of the Network Voting system does not both support the Chain of Trust and provide auditable evidence, then the process is open to question.

The best approach to prevent the existence of malicious code in an Internet voting system, either present from origin or added later, is to employ measures that allow it to be detected or prevented. The Chain of Trust is a compilation of all the following measures:

1. Source code audit to verify that the code will perform only what it should do.
2. Digital signature of the audited source code to protect its authenticity and integrity.
3. Trusted build of the voting executable code in front of auditors (based on audited source code).
4. Signature of the executable code to protect its authenticity and integrity

5. Deployment of the executable software in a clean system
6. Logical sealing of the system to detect any additions later
7. Logic & accuracy testing of the voting system to validate it works properly
8. Continuous audit of the voting system while used in an election, by reviewing and validating logs and other data. The logs must be protected from external manipulations by using special cryptographic measures.
9. Post-election audit that validates that the system behaved correctly by reviewing the logical sealing and the protected logs. Possibility of recounts.
10. Individual voter verification that their ballots were used in the final tally (by using special receipts)

Figure 14: Chain of Trust



If these processes are applied correctly, combined with a secure network voting solution and the appropriate procedures, it can be demonstrated that the election behaved correctly and no tampering occurred

10.2 IMPLEMENTATION APPROACH

Elections Ontario must recognize that the pilot project will have multiple sources or risk and implement a strategy to manage it. Risks related to project implementation (including requirements fit, quality, and schedule risks) can be managed through the engagement of an experience project team, who must execute an effective implementation approach that focuses on the following:

- Procurement of secure, high-availability hosting;
- Procurement of a COTS that provides strong end-to-end security, and a vendor experience in large scale binding elections;
- Thorough user and performance testing;
- Demonstrations and stakeholder review;
- Dedicated participation of subject matter experts from Elections Ontario to ensure customized solution is a tight fit; and
- Continued consultation with an emphasis on widening the scope of stakeholders consulted.

An equally important success factor will be Elections Ontario's ability to communicate the security and integrity of the process through a detailed outreach campaign that demonstrates both that there are valid concerns and that they have been addressed. Processes already in place for communications and outreach will be leveraged.

Critically, the supplier selected to provide the network voting system should have demonstrated experience in similar implementations, including experience with more than one election in which the customer was a public administration, the electoral roll included a minimum of 150,000 potential voters, and there was a combination of remote and on-site voting.

The system supplier should also be able to demonstrate that their product has passed reliable and demonstrable audits and/or certifications, including audits that prove the support for key election principles, the integrity of the data, the strength of the cryptography used, and the auditability of the source code.

10.3 MEASURING OUTCOMES

In order to provide a report on the suitability of Network Voting technologies for application in the province of Ontario, Elections Ontario will need to be able to evaluate the outcome of the pilot against a meaningful set of objectives. In order provide the best link to Elections Ontario's strategic objectives; the recommended metrics are based on the list of core principles for evaluation of Network Voting. See Section 3 for a discussion of how these eight principles were selected.

The following table suggests ways that success or failure to uphold each principle could be assessed and measured. During the implementation of the project, specific measurement points and target values can be defined where appropriate.

	PRINCIPLE	METRICS
1	Accessibility[1.2] / Usability[1.1]	The 2007 survey showed that people with disabilities experienced more barriers to voting than others. Success of the pilot can be measured via a post-election survey or exit poll to measure problems with barriers: • Issue the 2007 survey questions with additional question(s) about experience with network voting. • Compare with baseline for same electoral district (assume raw data by ED to be available from most recent survey) Gather qualitative feedback from expert groups. This will provide a specific metric to show that people with various disabilities were more or less satisfied.
2	One vote per voter[2.1]	A post-event audit can prove that Network Voting has not introduced additional risk by: • comparing the number of electors who voted with the number of votes cast; and • demonstrating that there is only 1 vote in the system for each elector who voted. It is desirable to prove this is true not only within the network voting system but across mechanisms. • Need to account for ballots cast using network mechanisms and on-site paper ballots • Accuracy of this measurement will require a comprehensive and authoritative (online) voter list.
3	Voter authentication and authorization[2.4]	The event can be audited to prove that the process meets or improves on the process currently in place. • Demonstrate that the system provided an secure authentication system • May include scrutiny of updates to voters list • Accuracy of this measurement will require a comprehensive and authoritative (online) voter list.

	PRINCIPLE	METRICS
4	Only count votes from valid voters[2.6]	The event can be audited (pre and post) to prove that the process meets or improves on the process currently in place. • Tie (an encrypted) ballot to a voter. Each ballot must be associated with a voter who voted. • System must provide mechanisms that support points being audited (tampering, 'private' link between voters and ballots, digital signatures on ballots, etc.)
5	Individual verifiability[3.2]	In addition to usability mechanisms that give users accessible feedback in real time, publishing audit results post-election can also support verifiability. Success of these and other mechanisms can be measured via a post-election survey.
6	Voter privacy[4.3]	The system can be audited post-event to demonstrate that the voter's identity has been separated from the voter's readable ballot.
7	Results validation[6.4]	The system can be audited post-event to demonstrate that the results can be reconstructed independently. The scope of these recalculations can vary, as can the extent to which the process is replicated. • Handling of ballots for this purpose may constitute 'recounts' and may therefore require special authority.
8	Service availability[7.1]	The availability of the service can be measured technically in two ways: • Reports of production performance and availability, including response time and uptime statistics. • The availability of service at each polling station (internet connectivity, availability of workstations and assistive devices) SLAs will be needed for all metrics.

11. COST ESTIMATES

11.1 ESTIMATED PILOT COSTS

The estimated cost for a pilot of the two recommended channels is $1,745,500.00, of which approximately half is made up of the cost of the COTS product. This figure is the total expenditure required to customize and test the COTS product, license 100,000 voters at $2.00 each, conduct voting, count the ballots, and audit the entire process. It does not include internal resource costs.

*Two remote channels

*No poll book

*Two registration packages

Costs for a pilot (remote only)	
Custom off the Shelf (COTS)	$837,000.00
Polling Location Costs	$0.00
Central Infrastructure	$162,000.00
Implementation Costs	$217,500.00
Project Resource Costs	$429,000.00
Other project costs	$100,000.00
TOTAL	$1,745,500.00

The COTS line item includes the cost of 100,000 one-time voter licenses, as well as the cost of the professional services required to customize and implement a commercial-off-the-shelf network voting product. The Polling Location Costs would include the cost of poll book and voting hardware and the supporting infrastructure, which would amount to roughly $5,000 per location if implemented. Since on-site voting is not currently recommended for the Pilot, and an electronic poll book is not necessary, this line item is left at zero. The Central Infrastructure line item includes the costs of managed hosting for one year, as well as dedicated decryption and outing hardware. The Implementation costs include the costs of mailing two registration packages ($156,000) and providing help desk and support staff ($30,000) . The project resource line item represents the cost of staffing a dedicated delivery team responsible for project management, quality assurance, and integration with Elections Ontario’s business. The final line item contains the estimated cost for communication and outreach.

However, the majority of these costs would not recur if a second by-election were to be held in the same year. The largest recurring item is the COTS cost, which is primarily composed of voter licensing and election support costs. The remaining recurring expenditure is the cost associated with the event implementation (approving and rolling out the system, support staff, and secure mailing). As a result, a second by-election with 100,000 electors and 10 polling locations would incur an additional total of approximately $649,500.00.

11.2 POTENTIAL GENERAL ELECTION COSTS

While it is difficult to project the costs accurately for a general election, it is worth noting that a key factor is likely to change: the per-user licensing fee charged by a COTS vendor will drop to as little as $0.25 per user. If computer voting were rolled out to the maximum number of locations (approximately 600), then the total cost of a general election would be $9,295,500.00.

Costs for a General Election	initial	recurring	total
COTS	$ 478,500.00	$ 2,331,500.00	$ 2,810,000.00
Polling Location Costs	$ 2,910,000.00	$ 261,000.00	$ 3,171,000.00
Central infrastructure	$ 162,000.00	$ -	$ 162,000.00
Implementation Costs	$ 12,000.00	$ 2,611,500.00	$ 2,623,500.00
Project Resource Costs	$ 429,000.00	$ -	$ 429,000.00
Other costs	$ 50,000.00	$ 50,000.00	$ 100,000.00
Total	**$ 4,041,500.00**	**$ 5,254,000.00**	**$ 9,295,500.00**

Note that due to a much lower per-voter license cost, the costs are more evenly distributed among the COTS, Location Costs, and Implementation line items. The recurring Implementation costs are high primarily due to the recurring need for secure mail and support staff.

Caveat

Key cost factors must be investigated further: the need to re-invest in project resources may change depending on the outcomes of the pilot, and the central infrastructure needs may increase in order to support the additional voter traffic. A major variable exists with regards to the vendor costs. The costs in this study are based on a review of industry pricing and may change substantially in the context of a competitive bid or a contract negotiation.

Detailed Estimate by line item

	Quantity	Unit	Unit Cost	Total
1. COTS solution cost (Customization & Integration)				**$ 837,000.00**
NV system	**28**	**750**	**1000**	**$ 783,000.00**
Software license	**100000**		**2**	**$ 200,000.00**
Related services				**$ 583,000.00**
Sofware customisation (including on-line registration system)	6	HCM	$ 16,500.00	$ 99,000.00
Integration with EO systems (EMS, Voter registration, IVR)	2	HCM	$ 16,500.00	$ 33,000.00
Deployment in the data centre, including OS hardening	3	HCM	$ 16,500.00	$ 49,500.00
Testing (at different levels)	2	HCM	$ 16,500.00	$ 33,000.00
UAT support	2	HCM	$ 16,500.00	$ 33,000.00
Support during electoral process, including configuration	2.5	HCM	$ 16,500.00	$ 41,250.00
Support to auditing process	1	HCM	$ 22,000.00	$ 22,000.00
Post-election support	0.5	HCM	$ 16,500.00	$ 8,250.00
Specialized e-voting consulting	3	HCM	$ 22,000.00	$ 66,000.00
Project management implementation	6	HCM	$ 22,000.00	$ 132,000.00
Project management election	3	HCM	$ 22,000.00	$ 66,000.00
Third party auditor	3	HCM	$ 18,000.00	**$ 54,000.00**
2. Polling Location Hardware				**$ -**
	per location	*totals*	*unit cost*	
Furniture				
Desks/tables (reuse of existing assets)				$ -
Privacy screens (reuse of existing assets)				$ -
Voting telephones (incl. redundant equipment)				**$ -**
Telephones	0	0	$ 20.00	$ -
Head sets for telephones	0	0	$ 20.00	$ -
Disposable ear covers for head sets	0	0	$ 0.25	$ -
Voting Computers (+redundant equipment)	0			**$ -**
Touchscreen Computers	0	0	$ 850.00	$ -
Sip and puff	0	0	$ 750.00	$ -
Paddles/joysticks	0	0	$ 250.00	$ -
Keyboard and mouse	0	0	$ 50.00	$ -
Screen reader s/w	0	0	$ 800.00	$ -
Head sets for computers	0	0	$ 25.00	$ -
Disposable ear covers for head sets	0	0	$ 0.25	$ -
Smart card reader	0	0	$ 25.00	$ -
Printer (for receipts)	0	0	$ 150.00	$ -
Poll book	0			**$ -**
Computer/Monitor	0	0	$ 600.00	$ -
Printer	0	0	$ 150.00	$ -
Smart card writer	0	0	$ 25.00	$ -
Smart cards	0	0	$ 20.00	$ -
Location Costs (Infrastructure)	0			**$ -**
Phone lines	0	0	$ 130.00	$ -
Network connections to polling stations (redundant)	0	0	$ 135.00	$ -
Network connections to polling stations (redundant)2	0	0	$ 300.00	$ -
Backup power	0	0	$ 500.00	$ -
Switches, routers	0	0	$ 150.00	$ -
Cables	0	0	$ 5.00	$ -
3. Central infrastructure				**$ 162,000.00**
Call centre infrastructure				$ 30,000.00
Data centre costs (managed service for 1 year, includes High Availability)				$ 125,000.00
Infrastructure for Decryption and Counting				$ 7,000.00

4. Implementation Costs				**$ 217,500.00**
System rollout				**$ 22,000.00**
H/W certification (phones, voting computers, ePB computers)	0	HCM	$ 22,000.00	$ -
candidate review / approve ballots	0.25	HCM	$ 22,000.00	$ 5,500.00
system demo (for candidate and stakeholder review)	0.75	HCM	$ 22,000.00	$ 16,500.00
Deployment and decomissioning	0	HCM	$ 22,000.00	$ -
Registration package (to include the voter's unique NV identifier)				**$ 156,000.00**
Secure Mailing Envelopes	100000		0.15	$ 15,000.00
Printing				$ 8,000.00
postage	-		0.59	$ 55,000.00
2nd mailing (at a percentage rate to reflect uptake)	100%			$ 78,000.00
Support Staff				**$ 30,000.00**
Call centre (1st line)	2	HCM	$ 10,000.00	$ 20,000.00
Help desk (2nd line)	1	HCM	$ 10,000.00	$ 10,000.00
Field Teams	0	HCM	$ 10,000.00	$ -
Poll Staff				**$ -**
Poll Clerk (net increase of 1 for 2 weeks x 10 locations)	0	HCM	$ 5,000.00	$ -
Training				**$ 9,500.00**
Poll workers	0	HCM	$ 10,000.00	$ -
Support teams	0	HCM	$ 10,000.00	$ -
Call centre	0.25	HCM	$ 10,000.00	$ 2,500.00
Help desk	0.25	HCM	$ 10,000.00	$ 2,500.00
Returning office staff	0.1	HCM	$ 10,000.00	$ 1,000.00
Revisions office staff	0.1	HCM	$ 10,000.00	$ 1,000.00
EO staff (head office) training	0.25	HCM	$ 10,000.00	$ 2,500.00
5. Project Resource Costs (4.5 month project)				**$ 429,000.00**
Project initiation (1 PM)	3	HCM	$ 22,000.00	$ 66,000.00
Project management and planning (1 PM) during implementation	4.5	HCM	$ 22,000.00	$ 99,000.00
Project management and planning (1 PM) for election	0	HCM	$ 22,000.00	$ -
Design and development (BA, SA,)	5	HCM	$ 22,000.00	$ 110,000.00
Technical architect (validating security and infrastructure design)	3	HCM	$ 22,000.00	$ 66,000.00
Integration with voter list - EMS (programmer analyst)	2	HCM	$ 22,000.00	$ 44,000.00
System Testing (1 manager)	0	HCM	$ 22,000.00	$ -
UAT/Focus group testing (AAC)	2	days	$ 22,000.00	$ 44,000.00
6. Other project costs				**$ 100,000.00**
Travel: site visits, conferences				$ 50,000.00
Outreach				**$ 50,000.00**
TV, print ads (no net increase)				
Stakeholder consultation (Phase II) Surveys and research specific to Network Voting				$ 50,000.00
eBlast - outreach (no net increase)				
GRAND TOTAL				**$ 1,745,500.00**

12. CONCLUSIONS & RECOMMENDATIONS

THIS BUSINESS CASE has reviewed and evaluated the four short-listed network voting scenarios:

1. on-site computer voting
2. on-site telephone voting
3. remote computer voting
4. remote telephone voting

All four scenarios are capable of operating well within most the documented constraints that would be in place for a pilot. However, the on-site channels will introduce more operational complexity and organizational change than Elections Ontario may be willing to accept for a short-term pilot implementation. Given that investing in change required to handle the added complexity would deliver only the marginal benefit of providing network voting options to only the subset of electors who would not otherwise be able to access telephone or internet, Elections Ontario may wish to consider eliminating the on-site channels from the pilot.

12.1 IMPLEMENTATION OPTIONS

The evaluation has also included identified implementation options in two key areas: voter authentication and voters list management.

Voter Authentication Options

The assessment concluded that, while using government identification to support electors' identity claims is the most secure method, the fact that only Driver's Licence data is available to Elections Ontario will prevent electors who do not drive from registering using the standard process. Elections Ontario may therefore wish to allow these accessibility concerns to outweigh the need for security in this case. A registration process that uses a less secure form of identity support (address and date of birth) but introduces the incremental security benefit of a second letter will allow all Ontarians to access the same process. Elections Ontario must also accept that, while it may be more accessible, it adds additional delays to the process that will make network voting more difficult and reduce overall adoption, thereby reducing the sample size used to support the report to the Legislature in 2013.

Voters List Management Options

If Elections Ontario eliminates the on-site channels for the reasons discussed above, an online real-time poll book will not be strictly necessary. Instead, Elections Ontario can implement process controls to prevent the possibility of multiple votes across multiple channels. These controls would principally include a registration cut-off that allows time for the paper poll books to be printed and distributed before the advance polling period begins. These poll books would indicate which voters had registered to vote online so that poll workers could prevent them from casting ballots in person and support the principle of one vote per voter.

12.2 CONCLUSIONS

While all four of the short-listed channels would be capable of operating within Elections Ontario's constraints and would offer advantages and benefits to a wide range of Ontario's electors, there are key factors that may shift the cost/benefit equation. Specifically, the benefits of onsite network voting, while they deliver a marginal increase in voter convenience and accessibility, may not be worth the required investment for a pilot. While these channels may be piloted for a relatively low capital expenditure, especially if only one location is provided, the cost to Elections Ontario is high in terms of complexity and the need for organizational change.

This complexity would include changes to personnel (new poll worker skill sets), processes (managing real-time electronic elector list), and systems (new interfaces with existing electoral management systems). Given that the scope of this business case is to recommend viable options only for a pilot, this level of change may not be worth the investment. The key objective of the pilot, which is to evaluate the feasibility of network voting in order to report confidently on a future direction for Ontario, can be achieved without the expense of implementing onsite voting.

Once the scope of the pilot has been determined, Elections Ontario must also choose whether to still implement an electronic poll book and how to configure the registration process: for security or for accessibility.

12.3 RECOMMENDATIONS

1. The objectives of the pilot can be achieved by implementing remote channels only. Given the complexity and cost of implementing onsite network channels, and the marginal benefits to accessibility of doing so, it would not be worth the investment for the pilot.
2. Voter authentication is one of eight key principles that must be supported during the pilot. However, the related process is the source of several key security risks, including the risk of voter impersonation. Part of the mitigation for these risks is the incorporation of personal voter data into the registration process in order to support the voter's identity claim. Currently, the most secure option is government identification in the form of Drivers Licence Number.

Authentication by Drivers Licence is not Universally Accessible

While verifying a user's identity using this form of identification is the best means currently available, it has a direct impact on voters who cannot obtain a driver's licence. While this compromise could be considered acceptable for the pilot, Elections Ontario would need to pursue a more universal form of identification or other personal data for future elections.

Pursue a More Universal Authentication Model

Opportunities for a more universal authentication method exist and should be pursued. Elections Ontario should explore two directions simultaneously:

- obtaining a personal data element for verifying electors during registration that is more universal that a Drivers Licence Number; and
- integrating with and leveraging a third-party authentication mechanism, such as ServiceOntario.

For the purposes of the pilot, Elections Ontario may wish to consider a registration process that uses a weaker but more accessible process, such as the three-stage postal process described as an alternative in Section 6.

An Electronic Poll Book is not a Dependency for Remote Voting Pilot

3. If both remote and on-site network voting were implemented, the threats created by having multiple parallel voting mechanisms (paper, computer, and telephone) and differing types of authentication (physical and password), would put two key principles are at risk: the ability to ensure that only one vote is counted for each voter and the need to only count votes cast by valid voters. The mitigation strategy would need to include an online, real-time poll book that manages network voting and paper channels simultaneously. Without an electronic poll book, voters could vote twice: once online and once in person.

   However, by removing the on-site network channels, the risk of multiple votes per voter is reduced and the cost and complexity of an electronic poll book is harder to justify. In this scenario, the risk can be controlled by restricting registered network voters to the remote channels. Their names would not appear on the paper poll books and they would be unable to vote by paper during the advance polling period

Telephone Voting is a Risk Area, but Increases Access to Voting

4. The telephone voting channel presents inherent risks that are among the most difficult to manage or mitigate successfully. These risks stem from the fact that telephone voting uses an infrastructure that cannot be secured in the same way as computer voting can be. The public telephone lines are not secure, which opens up the possibility of privacy threats. Votes then pass unencrypted through the IVR environment, where they could be intercepted, deciphered, and even modified. However, the inclusion of telephone voting greatly increases the ease of access to network voting to segments of the population who have no access to or comfort with computers and the Internet. These risks can be mitigated to an extent, primarily by securing the IVR environment and implementing intrusion detection systems. Removing telephone voting would weaken support for principles, but also reduce risk, cost, and complexity.

Elections Ontario must Control the Hosting Environment

5. Elections Ontario's ability to control the network voting environment as much as possible will play a big part in establishing and maintaining the Chain of Trust. Elections Ontario should therefore procure the hosting environment (including web + IVR environments) under terms separate from the procurement of the COTS solution and the successful vendor will need to specify their detailed hardware and infrastructure requirements. Otherwise, the RFP must specify that the hosting server is physically dedicated for the election project, in order to allow servers to be sealed in support of the chain of trust and support the audit process.

   The recommended network voting approach, therefore, is to implement remote voting in the form of telephone and internet voting in an upcoming by-election. Doing so according to the general model described in Section 6, but without implementation of onsite channels, will result in a pilot that is able to operate within Elections Ontario's business constraints, support core electoral principles, and achieve the strategic direction and objectives.

APPENDIX A: DETAILED REQUIREMENTS

1. FUNCTIONAL REQUIREMENTS

1.1 PRE-ELECTION REQUIREMENTS

1.1.1 PRE-ELECTION INFORMATION MANAGEMENT

Requirements related to the access of existing electoral system's information (e.g., interfaces for introducing information, ELMS / EMS support, types of elections supported, counting methods supported, etc.)

a. The system must be able to automate the import of electoral information extracted from Elections Ontario's systems. This information can include, but will not be limited to:
   - Start and end dates and times for the voting period
   - Electoral district information
   - Ballot information (candidate names)

b. The system must protect the integrity and authenticity of the election information used to configure the voting platform.

1.1.2 ELECTORAL ROLL, REGISTRATION & CREDENTIAL MANAGEMENT

Requirements related to voter information and credential management (e.g., creating the Elector ID for each elector, distributing credentials, managing registration, etc.).

a. The system must be able to automate the import of external electoral roll information from EMS / ELMS

b. The system must be able to generate a unique Elector ID for each eligible voter

c. The system must be able to export data to supply the existing Notice of Registration Card (NRC) process (driven by the EMS/ELMS system) with sufficient data to populate and distribute the Elector IDs via mail.

d. The system must provide a web interface that allows voters to register for network voting
   i. Voters must be able to enter the Elector ID received on the NRC into a secure web site (the address of which is provided on the NRC)
   ii. Voters must be able to enter into the web site additional personal data in order to assist Elections Ontario in verifying their identity. This may take the form of date of birth plus a piece of government issued identification.

iii. Once authenticated, and in the same session, the web site must provide voters with a unique and strong numeric password OR allow the voter to choose their own, providing it meets required security standards

e. The system must provide am interactive voice response (IVR) interface that allows voters to register for network voting

i. Voters must be able to enter the Elector ID received on the NRC by calling a toll-free number printed on the NRC and using an IVR interface

ii. Voters must be able to enter into IVR interface additional personal data in order to assist Elections Ontario in verifying their identity. This may take the form of date of birth plus a piece of government issued identification.

iii. Once authenticated, and in the same session, the IVR must provide voters with a unique and strong numeric password OR allow the voter to choose their own, providing it meets required security standards

f. The system must be able to interface with EO's EMS to support real-time online poll book features.

1.1.3 CENTRAL NETWORK VOTING MANAGEMENT BOARD

Requirements related to the existence of an Network Voting Management Board that must certify the Election information.

a. The system must allow the secure configuration of the Network Voting Management Board in a way that a threshold of members is required to carry out the decryption and final tally/tabulation of votes. This is intended to prevent a single member acting on his/her own.

b. The system must require the presence of the Network Voting Management Board to certify any change on the election configuration.

c. Any election information must be certified by the Network Voting Management Board by means of non-repudiation practices (e.g., digital signatures).

i. Election information includes: list of voters[18], list of candidates/ballots, and data related to opening times, etc.

ii. Election information should be digitally signed so any auditor can validate that the configured voting system reflects the data provided by EO.

d. The previous processes must be performed in an isolated server with no network access for maximum security protection.

1.1.4 PRE-ELECTION AUDIT

The election information used by the voting platform during the voting and counting process must be auditable in order to detect any manipulation attempt. Election information is understood as any information in electronic format that is used by the voting platform or independent auditors to verify the correct configuration of the election. That includes the contents of the electoral roll, the ballot templates, the election identification, the Network Voting Management Board members, etc.

a. The system must check that the election information has been electronically certified by the Network Voting Management Board before starting the voting and counting processes

b. The system must allow any independent auditor to check if the election information used by the voting platform has been certified by the Network Voting Management Board

Furthermore, the different software components of the voting platform must also be certified to detect any attempt of tampering. This must facilitate independent auditors and voters to check if the components used are the same as the ones audited.

c. Independent auditors must be able to audit and certify the application components used for voting. This audit should at least include:

   i. the revision of the security measures implemented in the software (e.g. cryptographic protocols and algorithms);

   ii. the revision of the source code, including the implementation of the security measures mentioned above;

   iii. a functional testing; and

   iv. an accuracy testing.

d. Voters must be able to check the integrity and authenticity of any voting component executed on the voting device before using it (e.g., verification of the digital signature of a Java applet when using a computer to vote)

e. Any independent auditor must be able to certify the integrity and authenticity of the system components installed in the voting platform

f. Any action performed by an independent auditor must not affect voter privacy nor election integrity.

1.1.5 VOTER CREDENTIAL GENERATION

a. The voting platform must interface with Elections Ontario's EMS to obtain the list of voters that will receive a postal card

b. The voting platform must provide the required voter credentials to the EMS (the login), so it can be printed in the cards to be sent to all the voters

c. The voting platform must keep all related passwords, protected in such a way that only authorized personnel from Elections Ontario can have access to them. System administrators can not have access to the passwords

1.1.6 REMOTE REGISTRATION

a. The voting platform must provide a web interface for voters to obtain their password online, once they introduce the ID received by post and other personal information

b. A similar interface must be available to voters using the telephone (audio interface through the IVR provided by Elections Ontario)

1.2 VOTING PROCESS REQUIREMENTS

1.2.1 ACCESS TO THE VOTING PLATFORM

Requirements related to the access to the voting platform. (e.g., voter's computers supported, installation-free, etc.)

For remote computer-based voting:

a. The voting platform must allow voters to cast their ballots from computers running widely used operating systems and browsers.

b. Voters must not be required to manually install any specific election software or hardware on their computers in order to access the voting process unless it is required for security and/or accessibility purposes

c. Voters shall not be restricted to always using the same voting computer (or IP address) for accessing the voting platform. That is, they could register from one location and vote from another.

d. Voters must be able to verify the authenticity of the voting platform they are accessing using their browser.

For on-site voting:

e. Voters must be able to identify themselves to a poll worker by using legally accepted identification. The system must offer an interface to the poll worker to validate voter's eligibility (e.g. the voters is on the voter list and has not voted before).

f. The system must provide some type of token (e.g. smartcard or PIN on a piece of paper) to the voter, so he can vote using one of the available voting terminals (computers or telephones) in the polling place.

For on-site computer-based voting:

g. The voting platform must allow voters to cast their ballots using accessible and user friendly computerized devices located in the polling place, including the following assistive technologies:
    i. Screen reader software
    ii. Sip and puff input devices
    iii. Joysticks
    iv. Touch screens

For telephone-based voting:

h. The voting platform must allow voters to cast their ballots using standard telephone sets, may it be analogical or digital, including land-line telephones, Voice over IP (VoiP) and mobile telephones.

1.2.2 VOTER AUTHENTICATION

Requirements related to voter authentication.

Remote authentication:

a. The system must require voters to use specific credentials to access the voting system
b. Voter credentials shall be combined with personal data to grant access to the voting system for casting a ballot.
c. Voters shall be able to access the voting system multiple times from different locations and devices provided they do not cast a ballot.

On-site authentication:

d. Voters shall be able to identify themselves in front of a poll worker using any legally accepted ID. If eligible to vote, the voter will obtain a token for accessing the voting system.
e. The voting system (on-site) shall accept the token and validate its authenticity to grant access to the voter.

1.2.3 BALLOT FORMAT (VOTING OPTIONS)

a. The voting option must appear in a clear and understandable format, without being codified or requiring the use of a code book to reveal the real value of the options.
b. Voters must be able to clearly distinguish the different voting options (candidates)
c. Voting options must support the use of multiple languages, currently specified as English and French.

d. The ballot layout must support either a fixed (alphabetical) or random order of candidate names.

1.2.4 SELECTION & CONFIRMATION OF VOTING OPTIONS

The online ballot screen or IVR menu must be usable enough that voters can clearly distinguish their selections and be warned from making inadvertent selections or other errors. However, the voting option function should allow under voting.

a. The system should prevent and warn voters if they make involuntary errors that could invalidate their vote (e.g., it should prevent over voting and warn against unintentional under voting)

b. The system should clearly distinguish selected voting options from non-selected ones

c. The system must allow voters to cast blank ballots

d. The system must allow voters to verify their voting options before casting their vote

e. The system must provide the voter with the option of modifying his/her vote before casting it

f. The system must provide the voter with the option of intentionally declining the ballot. The declined ballot should be recorded in the system.

g. The IVR system must provide the voter with the option increasing or decreasing the speed and volume of playback, and to repeat menu options.

h. The IVR system must clearly confirm ballot selections and allow voters to cancel and re-enter as needed

1.2.5 CASTING THE BALLOT

a. The system must clearly tell the voter when the ballot is cast, and whether it has been correctly stored in the voting system or not.

b. For computer voting, the system must protect the privacy and integrity of the cast vote, along with the voter's identity by cryptographic means, so that that the vote cannot be tampered with during its transportation or storage

c. For computer voting, the system must allow voters to protect their votes on their voting computer before casting it, instead of only protecting the votes when received in the voting servers.

d. The cast votes must be protected against both external and internal attacks (e.g. system administrators) by employing appropriate cryptographic measures that can be demonstrated in front of a security expert or auditor

e. Whenever possible, use encryption in the communication channels

f. For telephone voting, the system must implement appropriate procedures to mitigate internal or external attacks that could affect voter's privacy and/or ballot integrity.

1.2.6 VOTER VERIFIABILITY

The system must allow network voters to verify that their votes were received by Elections Ontario at the end of the election, and were therefore included in the final count.

a. The system must provide voters with a voting receipt once they have cast their vote. This receipt will allow them to verify that their vote was present during the decryption and counting process

b. The voting receipt must include proof of authenticity to avoid false claims from voters (e.g. a digital signature).

c. If requested, the system must allow voters to prove that their vote was present during the final count.

d. Any voter verification method must not facilitate coercion or vote buying practices by including readable evidence of the voter's actual selection.

e. The voting receipt must not allow to link voters with their cast ballots or the receipt so that their privacy is ensured.

1.2.7 VOTER MANAGEMENT DURING THE VOTING PROCESS

The network voting system must support the following requirements related to managing voters during the voting process.

a. The System must allow authorized users to invalidate voters before and during the voting process (e.g. if the voter's authentication mechanism has been compromised and it has to be blocked). If the invalidation is done on a voter who already cast a ballot, it must be tagged as invalid and not used in the final count.

b. The System must allow authorized users to perform the following actions

   i. add new voters to the election if required by law

   ii. generate new Network Voting credentials

   iii. reissue lost credentials

   iv. delete a voter and cancel their credentials

   v. update a voter's record in cases where their Electoral District has changed.

c. Any of the previous actions shall not affect voter's privacy or election integrity.

1.2.8 ELECTION MONITORING

It should be possible to demonstrate to stakeholders, auditors, etc. that the network voting system was not the subject of intrusion or data manipulation. To do this, it should provide monitoring tools.

a. The voting system must provide monitoring tools that ensure the detection of any anomalies during the voting process

b. The system must ensure that the monitoring tools are tamper proof and provide non-repudiation of the recorded audit information

c. The voting system must guarantee that the monitoring tools cannot compromise the voter's privacy and election accuracy

1.3 COUNTING AND RESULTS PUBLICATION

1.3.1 CLOSING THE VOTING PROCESS

It must be possible to initiate a clear and unambiguous closure to the voting period.

a. The system must automatically close the election at the time specified by Elections Ontario during the election setup and not allow this date and time to be overridden.

b. Voters must not be allowed to access the system and cast their votes once the voting process has closed

c. The system must give voters who are in the process of casting their vote extra time to finish the process.

d. The system must prevent internal or external attackers (including actors with privilege access rights to the system) from adding votes from voters that have not participated, once the election is closed

e. The system must protect the integrity and authenticity of the digital ballot box (containing all the votes cast by the voters) after the voting process has been closed (e.g., digitally signing the ballot box)

1.3.2 DECRYPTION AND TABULATION OF THE ELECTRONIC BALLOT BOXES

Once the voting period has ended, the network voting results (including both computer and telephone channels) must be decrypted and counted.

a. The decryption and counting process must be carried out in an isolated environment that is not connected to any network

b. The transfer of the ballot box(es) from the voting servers to the isolated environment must ensure the ballot box integrity and authenticity

c. The authenticity and integrity of the collected ballot boxes must be verified before accepting them

d. The ballot boxes must contain all the votes cast during the election process (i.e., if multiple voting is required, all the votes cast by the voters must be included in the collected ballot box)

e. The decryption and tallying process can only be initiated by a pre-defined majority of the Network Voting Management Board members, who must meet to reconstruct the decryption key.

f. The decryption and tallying process must verify that all the votes contained in the ballot boxes are cast by eligible voters

g. The decryption and tallying process must prevent multiple votes from the same voter being decrypted, including prevention of counting votes tagged as invalid by an authorized user (as in cases of an impersonation claim).

h. The decryption and tallying process must ensure that it is impossible to correlate the order of the decrypted votes with the order they were cast and therefore, prevent any link between the decrypted votes and the voters (e.g., by using a Mixing process)

i. The Network Voting Management Board must certify the list of decrypted votes (e.g., digitally sign it)

j. The decryption and tallying process must guarantee that it is impossible to correlate any voter verification information (e.g., voting receipts) with the voting options selected within the ballot.

1.3.3 CONSOLIDATION OF THE ELECTION RESULTS

a. The decrypted ballots obtained from the previous process shall be transferred to Elections Ontario's EMS (Election Management System) for its consolidation with the results obtained from the other voting channels (postal and on-site paper).

b. The information transferred to Elections Ontario's EMS must be protected to ensure its integrity and authenticity.

c. The detailed contents of the data to be transferred and its format will be agreed with Elections Ontario in order to minimize changes in its EMS.

1.3.4 CERTIFYING AND PUBLISHING THE ELECTRONIC RESULTS

a. The system must generate the results of the network voting channel from the certified list of decrypted votes.

b. The system must publish the results from the network voting channel with the information that allows the voter to verify his/her vote. The system must include a simple interface that allows Elections Ontario to gather the information and display it in its website (e.g. a web service).

c. The system must be able to generate results reports including the following

- all accepted/valid ballots for each candidate by ED/PD
- all declined
- all unmarked
- all invalid
- total number of votes case (accepted, declined, unmarked, and invalid) by channel (Telephone, Computer) and location (onsite, remote).

d. For each Electoral District, the system must export and distribute a results report that includes vote counts for each candidate to the Results Coordinator for the Electoral District.

1.3.5 AUDITING THE COUNTING PROCESS

a. The system must allow independent auditors or the Network Voting Management Board to carry out new decryption and tabulation processes if required.

b. The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes. Auditors should be able to operate with the decrypted votes and obtain human-readable results that can be compared to the ones generated by the system.

c. The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes, including the authenticity of the software, the integrity of the system, the integrity and authenticity of the generated logs, etc.

1.4 RESULTS VERIFICATION

1.4.1 VOTER VERIFICATION OF THE RESULTS

a. The system must generate a voting receipt that allows voters to verify that their vote reached the Network Voting Management Board and was present during the decryption and tallying process

b. This voting receipt must allow voters to fill a valid claim in the case that they detect that their vote was not processed

c. The system must provide an easy interface for the voters to check their voting receipts. This interface should be available through Elections Ontario website.

1.4.2 INDEPENDENT AUDIT OF THE ELECTION

a. Auditors must have access to the source code of the system if requested by Elections Ontario

b. The vendor must provide the required procedures/ technologies/ mechanism to ensure an end-to-end auditable process, from the network voting system construction to the election results validation

c. The system must facilitate a meaningful audit of the system by trusted third party auditors based on the stored election information and logs

d. The system must allow a full audit without compromising election integrity and voter privacy

e. Auditors must be able to check the integrity and authenticity of the election information and logs to detect any manipulation attempt of such audit information.

2. PRINCIPLES & NON-FUNCTIONAL REQUIREMENTS

2.1 UNIVERSAL PRINCIPLES

2.1.1 USABILITY

The voting process must be easy to understand and execute by any voter. Voters shall not need any special technical, cultural or legislative skills to cast a ballot.

a. The system should provide a user-friendly voter interface, so that the voting process is intuitive and no previous training for using the network voting system is necessary

b. The system must support the use of the main Internet browsers and operating systems, and of standard telephones

c. The system must include easy to understand instructions for voters

d. The system must warn voters if, during the voting process, they make a selection that could invalidate their vote (e.g., under voting, over voting, etc.)

e. Voters must select their voting options by directly selecting the candidate instead of using a code or indirect selection method

2.1.2 ACCESSIBILITY

The voting process must be equally accessible to all eligible voters, including voters with disabilities. In any case, the voting process shall be performed by the voter without requiring any assistance for making their selections.

a. The system must support the use of multiple languages without compromising the voter's privacy

b. The system must be compliant with WGAI accessibility standards for remove voting and conform to WCAG 2.0 Level AA

c. The system must support visual impaired voters using screen readers (JAWS, NVDA, VoiceOver, etc.) and screen magnifiers

d. The system must support motor disabled voters requiring use of an audio ballot (through the telephone or using a screen reader), and sip-and-puff and paddle/joystick input devices.

e. The IVR interface must allow voters to adjust the following factors

    i. Speed of the content and the ability to adjust the speed of playback

    ii. Ability to adjust the volume level of the playback

iii. Ability to repeat or rewind menus and other content, as well as user selections

iv. Duration of the timeout imposed on user selections

2.1.3 REACHABILITY (LOCATION)

The means required to vote must be easily reachable by any voter, independently of the voter's physical location during the voting period.

2.1.4 ONE VOTE PER VOTER

Only one vote per voter is counted for obtaining the election results. This shall be fulfilled even in the case the voter is allowed to cast multiple votes.

2.1.5 NO PRIVILEGED VOTERS

There must be no voter (individual or a group) with any technical, logical or decisional advantage respect to other voters. Each vote has the same value regardless the voter who cast it.

2.1.6 NO PRIVILEGED ACTORS

There must be no person or entity involved in the management or implementation of the electoral process capable of influencing the electoral process and/or gathering non-public information.

2.1.7 VOTER AUTHENTICATION AND AUTHORIZATION

The electoral process shall ensure before allowing a voter to cast a vote, that the identity of the voter is the same as claimed, that the elector is eligible to vote, and that she has not exceeded the allowed voting intents.

For remote authentication:

a. Voter credentials shall be combined with personal data to grant access to the voting system for casting a ballot.

b. The system must require voters to use specific credentials to access the voting system

c. Voters shall be able to access the voting system multiple times from different locations and devices provided they do not cast a ballot.

For on-site authentication:

d. Voters shall be able to identify themselves in front of a poll worker using any legally accepted ID. If eligible to vote, the voter will obtain a token for accessing the voting system.

e. The voting system (on-site) shall accept the token and validate its authenticity to grant access to the voter.

2.1.8 RIGHT TO BE ON THE VOTERS LIST

The electoral process shall ensure that all eligible voters are included in the Voters List and provide means to voters to claim their right to vote if they are not present in it.

2.1.9 ONLY COUNT VOTES FROM VALID VOTERS

The electoral process shall ensure that the votes used in the counting process are the ones cast by valid eligible voters.

a. The system must guarantee that only eligible voters can log into the voting platform

b. Before accepting a cast vote, the system must verify the identity of the voter who casts the vote

c. The system must prevent a voter from casting more votes than the ones permitted

d. The system must allow verifying, at any time during the election, that the votes within the ballot box belong to eligible voters

e. The system must guarantee the non-repudiation of the cast votes

f. The system must prevent the addition of counterfeit ballots in the ballot box from both external users and system administrators.

g. The system must use unique digital certificates for authenticating voters

h. The system must use unique voter digital certificates for digitally signing the votes cast

2.1.10 FAIR BALLOT LAYOUT

Voting process shall ensure that all the voting options, parties and candidates have the same right to be in the ballot. The ballot design or distribution of voting options shall not favour any party or candidate. This principle should be preserved independently of the voting channel used by the voter to cast the vote.

a. The voting option must appear in a clear and understandable format, without being codified or requiring the use of a code book to reveal the real value of the options.

b. Voters must be able to clearly distinguish the different voting options (candidates)

c. Voting options must support the use of multiple languages, currently specified as English and French.

d. The ballot layout must support either a fixed (alphabetical) or random order of candidate names.

2.1.11 NO COST FOR VOTERS

Voters must not incur in specific costs for exercising their right to vote. Neither the online or telephone channels should cause the voter to incur a cost that is directly related to voting.

2.1.12 FAIR VOTERS LIST GENERATION

The electoral process shall use a Voters List honestly generated based only on data from valid voters. All valid voters must be included in this Voters List.

2.1.13 NO COERCION OR VOTE SELLING

The voting process must prevent voter coercion and vote selling. This is usually achieved by not providing any information to the voter or any other third party that could be used by a coercer or vote buyer to discern the voter intent of the vote cast by the voter.

a. The system must generate voting receipts that do not allow voters to prove who they had voted for to a third party

b. The system must prevent anybody, even privileged managers or auditors, to correlate votes with voters

2.1.14 INDIVIDUAL VERIFIABILITY

The voting process shall provide means to the voters for verifying that their votes have been properly deposited inside the ballot box (vote recorded as cast).

a. The system must allow voters to verify if his/her vote was present during the decryption and tallying process, by means of a voting receipt

b. The voting receipt must preserve the vote's secrecy (i.e., the selected voting options should never be able to be deduced)

c. The verification process must allow the detection of manipulated or counterfeit receipts to prevent fraudulent claims by voters

2.1.15 INTEGRITY

The voting process shall ensure that the outcome of the election represents the opinion of the participating voters and therefore, it is obtained only from votes cast by valid voters. Furthermore, the voting process shall ensure that votes from valid voters have not been manipulated or the ballot box stuffed.

a. The system must preserve during the whole electoral process the integrity of each individual cast vote

b. The system must allow checking the integrity of each individual vote stored in the ballot box

c. The vote's integrity is protected by the voter when casting his/her vote using a computer

d. The system must prevent any attempt to add counterfeit ballots into the digital ballot box

e. Vote integrity should be protected by means of strong encryption, such as digital signatures

2.1.16 PERSONAL DATA PRIVACY

This information related to voters shall only be used for the specific purpose of the election and cannot be accessed by any unauthorized actor. Voters must be protected against identity theft.

2.1.17 BALLOT SECRECY

The voting process shall preserve the secrecy of the cast votes until they need to be processed in the counting process.

a. The system must guarantee that a cast ballot is secret in front of any third party, including system administrators and potential hackers that break through the conventional security measures protecting the voting platform.

b. Votes must be encrypted on the voter's terminal before being cast when using the computer-based channel

c. Votes can only be decrypted by the Network Voting Management Board

d. The system must prevent the decryption of the ballots before the election is closed to avoid leaking information on partial results

e. Any audit process supported by the system to verify the accuracy of the election must no compromise the voter privacy

2.1.18 VOTER PRIVACY

The voting process shall prevent at any stage of the election the correlation between voters and the contents of the ballots cast by such voters.

a. The system must guarantee that votes are encrypted in a way that only the Network Voting Management Board can decrypt them

b. The system must guarantee that the key required to decrypt the votes is not available during the voting process until the Network Voting Management Board retrieves/reconstructs it

c. The system must guarantee that at least a pre-defined majority of Network Voting Management Board members are required in order to retrieve the election decryption key

d. The system must guarantee that it is impossible to correlate the order in which the votes were decrypted with the order in which they were cast

e. The system must guarantee that two different votes with exactly the same content have different encryption formats

f. Any audit process supported by the system to verify the accuracy of the election must not compromise voter privacy

2.1.19 NO INTERMEDIATE RESULTS

The voting process shall prevent any access to the contents of the cast votes until the counting process.

a. The system must guarantee that only the Network Voting Management Board can decrypt the votes, after the election, ideally in an isolated environment

b. The system must encrypt the votes on the voter's terminal before sending them to the voting server

2.1.20 SECURE DATA DECOMMISSIONING

The voting process shall provide secure decommissioning practices of any voting material, records and data that could compromise the privacy of voters. Electoral data, including data captured and stored by the network voting system, must be stored securely for and decommissioned after a defined length of time

2.2 PROCEDURAL PRINCIPLES

2.2.1 VOTER TRAINING

The electoral process should provide voters means for learning and understanding the voting process before the actual election. A detailed communication campaign will provide effective outreach and support to the community of electors.

2.2.2 INFORMATION/DIFFUSION

Information related to the electoral process (schedule, technology, procedures, audit results...) shall be made publicly available. Information shall be accurate and available enough time before the election. A detailed communication campaign will provide effective outreach and support to the community of electors.

2.2.3 EASY TO EXPLAIN / UNDERSTAND BY VOTERS

The electoral process shall be as simple and easy to explain as possible. A detailed communication campaign will provide effective outreach and support to the community of electors.

2.2.4 SOURCE CODE AUDITABILITY

The source code and binaries of any software used for managing the election processes or data, shall be available for auditing and, if required, certification. The audit process shall be performed by independent auditors to ensure that the electoral process behaves properly.

2.2.5 PROCESS AUDITABILITY

The procedures followed during the election process shall be well documented and auditable in order to ensure that they accomplish with the expected requirements.

a. The system must allow auditors to retrace any election process, in a meaningful manner, without compromising the election privacy or accuracy

b. The system logs and election information generated during the election must allow a meaningful audit of the election without requiring that auditors have access to any private key, or assuming the role of any privileged actor

c. The system must implement adequate cryptographic practices for verifying the accuracy and integrity of the log information to be used during the audit

d. The system must allow any independent auditor to check and certify the integrity of the application components at any time during the election

e. The service provider must describe its approach for an end-to-end auditable process

2.2.6 CERTIFICATION

The voting process and any logical of physical components related to it shall be designed to facilitate any certification of their design principals. The certification will confirm that the network voting election process is able to accomplish what the specifications claim.

2.2.7 RESULTS VALIDATION

The voting process shall provide a means for verifying if the results clearly represent the intention of the voters that participated in the voting process. This verification shall also ensure that only votes from valid voters have been used in the counting process to prevent fraud practices that could compromise the election accuracy.

2.2.8 ELECTION MONITOR

The elections process shall support the election monitor of all the transactions carried out during the process. This monitor process shall be sound and shall guarantee that voter secrecy is preserved at all times.

2.2.9 REVIEW LOGS/FORENSICS

The election process shall leave traces of the activities carried out during the process (e.g. logs). These traces shall be available for being analyzed during and after the election in order to ensure that the electoral process behaves properly.

2.2.10 POTENTIAL PARTIAL RERUNS

The election process shall allow the resume of an active election from the same stage in which it was paused / stopped without losing any information that was already recorded.

2.2.11 SERVICE AVAILABILITY

The election process and any of its critical components or entities (e.g., electoral roll information, cast votes, voting channel…) shall be available during the whole election period to voters, election managers, observers or any other actor involved in the process.

2.2.12 NO SINGLE POINT OF TRUST

The election process shall not trust any single entity (person or system) for implementing any critical step. Entity privileges shall be restricted by segregation of duties policies, to require the collaboration of multiple entities for implementing critical processes.

2.2.13 PLATFORM INTEGRITY

The election process shall provide means for protecting the integrity and authenticity of the entities and components that participate in the process. These means shall be verifiable during the election process, to ensure their correct operation. Audit procedures can be done before and after the election process.

2.2.14 ACCESS CONTROL

The election process shall provide means for controlling and registering the access of entities to the different steps and components used in the process.

2.2.15 BALLOT BOX INTEGRITY

The election process shall provide means for preserving and detecting any manipulation of the ballot box.

a. The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and tallying process

b. The system must prevent the addition of counterfeit votes from both external users and system administrators

c. The system, for audit purposes, must allow to accurately trace the processes that concluded with the casting and storage of a vote in a ballot box

d. The system must implement adequate measures for detecting any attempt to delete a vote from the ballot box

2.2.16 LOGS INTEGRITY

The election process shall provide means for preserving and detecting any manipulation of the activity logs or registers recorded during the process.

2.2.17 VOTERS LIST INTEGRITY

The election process shall provide means for preserving and detecting any manipulation of the electoral roll information.

2.2.18 ELECTION CONFIGURATION INTEGRITY

The election process shall provide means for preserving and detecting any manipulation of the election configuration information used to setup the election.

2.2.19 BALLOT INTEGRITY

The election process shall provide means for preserving and detecting any manipulation of any individual ballot cast by a valid voter.

2.3 NON-FUNCTIONAL REQUIREMENTS

2.3.1 VOTE DECRYPTION

a. The system uses an Network Voting Management Board for decrypting the cast votes

b. The system uses a N of M threshold scheme of Network Voting Management Board members for retrieving the key that allows the decryption of the votes

c. It must be impossible for an individual member or a number of members below the threshold, to retrieve the election decryption key

d. The system must support the use of tamper proof devices (e.g., PIN protected smartcards) for storing the information required by each Network Voting Management Board member in order to retrieve the election decryption key

e. The threshold scheme is based on cryptographic means (e.g., secret sharing scheme)

f. The decryption key is destroyed by the threshold scheme and does not exist until it is reconstructed by the Network Voting Management Board members at the end of the election

2.3.2 SERVICE AVAILABILITY AND PERFORMANCE

Explain which are the required service level agreements in terms of availability and performance

a. The voting system must be available 99.95% during the voting period

b. The voting system must be able to support at least 100 concurrent computer-based voters and 100 telephone-based voters in parallel

c. The voting terminals located in the polling stations must be able to operate during the whole voting period.

d. The decryption and tabulation of ballots must be able to provide the results in less than 30 minutes for up to 50,000 votes.

2.3.3 NETWORK VOTING SYSTEM HOSTING REQUIREMENTS

This section contains the requirements for hosting the voting system in the infrastructure provided by Elections Ontario

a. Elections Ontario will provide the hosting infrastructure for the network voting system, as well as Internet connectivity

b. The service provider must describe its needs in terms of hardware, COTS software, networking and security appliances in order to ensure the required availability and performance.

c. Elections Ontario will be responsible of providing the agreed hardware, COTS software, networking and security appliances, as well as 24x7 monitoring services up to operating system level.

d. The service provider is responsible for deploying the required software on top of the operating system (including application servers, databases, etc.), as well as of the operating system configuration and hardening.

2.3.4 INTERACTIVE VOICE RESPONSE REQUIREMENTS

This section contains the requirements for interfacing with the IVR system provided by Elections Ontario

a. The voting system must use the IVR software and facilities provided by Elections Ontario

b. The service provider must describe its needs in terms of hardware, COTS software, networking and security appliances in order to interface Elections Ontario IVR with the voting system ensuring the required availability and performance.

c. Elections Ontario will be responsible of providing the agreed hardware, COTS software, networking and security appliances, as well as 24x7 monitoring services up to operating system level.

d. Elections Ontario will provide the required number of telephonic lines.

e. The service provider is responsible of deploying the required software on top of the operating system (including application servers, databases, etc.), as well as of the operating system configuration and hardening.

2.3.5 ISOLATED DECRYPTION AND TABULATION SYSTEM

This section contains the requirements for the isolated system using for election configuration and final decryption and tabulation

a. The components of the voting system used for election configuration and ballot decryption/tabulation must run in an isolated environment composed of one or more servers/computers.

b. The service provider must describe its needs in terms of hardware and COTS software to ensure the proper availability and performance of the system.

c. Elections Ontario will be responsible of providing the agreed hardware and COTS software.

d. The service provider is responsible of deploying the required software on top of the operating system (including application servers, databases, etc.), as well as of the operating system configuration and hardening.

e. The service provider must also describe its needs for the exchange of data between the isolated system and the voting servers located in the hosted environment. Elections Ontario will provide the required Internet access.

2.3.6 POLLING STATIONS INFRASTRUCTURE REQUIREMENTS

This section contains the requirements for deploying voting terminals in the polling stations

a. Elections Ontario will provide the required technological infrastructure for the network voting system elements deployed in the polling stations, as well as its Internet and telephonic connectivity

b. The service provider must describe its needs in terms of hardware, accessibility peripherals, COTS software, networking and security appliances in order to ensure the required availability and performance. Provide estimates for back up elements.

c. Elections Ontario will be responsible of providing the agreed hardware, COTS software, networking and security appliances, as well as technical support.

d. The service provider is responsible of deploying the required software on top of the operating system, as well as of the operating system configuration and hardening, and the accessibility peripherals configuration.

2.3.7 SCALABILITY

Requirements related to the system scalability

a. The system should be able to run elections for thousands to millions of voters in an easy and cost-efficient way

b. The system must allow the addition of new components without having to stop the service, e.g. for supporting a larger number of voters

2.3.8 FLEXIBILITY

Requirements related to the system flexibility

a. The system must support all the characteristics of Ontario's electoral process

b. The system must be customizable in several features, such as look & feel, language, help and information pages, etc. following Elections Ontario's requirements

c. The system must be able to support in parallel two different voting channels: based on computers and based on voice (telephones)

d. The system must be able to operate in two different environments in parallel: on-site (from polling places) and remotely (from anywhere).

e. The system must support several mechanisms for authenticating voters. These mechanisms should be able to work in parallel, so that the participation rate can be maximized. The selected mechanisms for this project are on-site authentication based on physical IDs and remote authentication based on voter credentials (PIN)

f. System management tools must be customizable to tailor Elections Ontario's requirements, such as the capability to access the participation rate in real time, to audit the system, or to cancel/revoke certain votes following the agreed procedures

g. The system must allow easy integrations with Elections Ontario current systems, including its Elections Management System.

2.3.9 TECHNICAL STANDARDS

a. The system provider must include a list of the cryptographic and security standards fulfilled by the proposed voting system.

b. Employed cryptographic algorithms must be based on international and open standards

c. The voting system should be compatible with the Election Markup Language (EML)

2.3.10 FREE OF IP CONFLICTS

The system supplier must guarantee that the solution has no Intellectual Property conflicts with third parties.

Appendix B: Risk List

This appendix provides a detailed list of the risks identified for the short-listed scenarios:

- Security risks;
- Operational risks; and
- Voter risks

2.4 SECURITY RISKS

The security risks that must be managed and mitigated can be divided into four categories:

- Voter privacy and confidentiality;
- Vote integrity and accuracy of results;
- Election system availability; and
- Auditability.

Voter Privacy & Confidentiality

RISKS	POSSIBLE ATTACKS
Voter privacy compromise An attacker could break the voter's privacy, relating a voter with their voting options and, thereby, breaking the vote's secrecy.	• An external attacker could intercept the communications between the voting terminal and the voting servers, in order to access the vote's content. • A system administrator with access to the election servers would be able to access the whole ballot box containing all the votes. • A system administrator of any intermediate infrastructure component (IVR platform, intermediate servers, etc) could have access to the votes in transit (containing the voting options selected by the voters). • Malicious software in the voting terminals can have access to the

RISKS	POSSIBLE ATTACKS
	voting options selected by the voters. • An electoral official could have access to the votes on the tallying process, identifying the voting options of each voter.
Publication of non-authorized intermediate results The intermediate results could be disclosed before the election is closed, influencing those voters that have not exercised their right to vote yet.	• Someone with access to the voting servers could be able to calculate and publish intermediate results. • Someone with access to any intermediate infrastructure component (IVR platform, intermediate servers, etc) could have access to the votes in transit, and calculate and publish intermediate results. • An electoral official could perform the tallying process before the election end-time, to obtain intermediate results.

Vote Integrity & Accuracy of Results

RISKS	POSSIBLE ATTACKS
Ballot stuffing An attacker can try to add in the ballot box votes from voters that did not participate in the voting process.	• Someone with access to the voting servers could have access to the ballot box, and could try to cast votes directly to the database. • An internal or external attacker could cast votes from an intermediate server of the voting solution (avoiding previous filters). • Someone before the election starts could allocate a non-empty ballot box in the voting servers.

RISKS	POSSIBLE ATTACKS
	• An electoral official during the tallying process could be adding counterfeit votes.
Voter coercion and vote buying. One person or organization could buy or force a voter to vote for specific voting options.	• A voter could cast a vote under surveillance of a vote buyer or coercer. • A voter is able to demonstrate their selected voting options to a vote buyer / coercer.
Vote modification The vote contents could be modified to change the election results	• Malicious software in the voting terminals can modify the voting options selected by a voter. • An external attacker could intercept the communications between the voting terminal and the voting server, and modify a vote. • A system administrator or an external attacker could be able to access directly the ballot box and modify the content of a valid vote. • During the tallying process, an electoral official could replace valid votes with counterfeit votes, or even replace the whole ballot box with a counterfeit one.
Vote deletion An attacker could try to delete valid votes from the ballot box.	• A system administrator or an external attacker could be able to access directly the ballot box and remove a valid vote. • An external attacker could intercept and stop a vote between the voting terminal and the voting server, making the voter believe that the vote has been cast. • During the tallying process, an electoral official could remove votes.
Voter uncertainty on the cast ballot A voter does not have any means of	• A voter could have the feeling that their vote has not been cast

RISKS	POSSIBLE ATTACKS
verifying the correct reception and count of their vote. Therefore, the voter could have a negative feeling about the voting process.	properly. • A voter could have the feeling that their vote has not arrived to the ballot box.
Modification of voting results The election results can be altered without accessing the votes or the ballot box, by manipulating the tallying or counting processes.	• A malicious insider could alter the voting results during the counting process. • The voting application could alter the voting results during the counting process. • An attacker (external or internal) could modify the election results after the counting process. • An attacker (external or internal) could modify the published election results.

Election System Availability

RISKS	POSSIBLE ATTACKS
Election boycott-denial of service An attacker could disrupt the availability of the voting channel by performing a denial of service attack.	• The voting system could be inundated with false voting requests to avoid valid votes to be processed due to system overload. • The voting servers could be inundated with malicious requests to force a servers' failure.
VOTER AUTHENTICITY	
Voter impersonation A voter or an attacker could try to cast a vote on behalf of another person.	• An attacker could steal a voter's credentials and cast a valid vote on behalf of the authorized voter. • An attacker could steal all voter credentials from the voting servers, and send valid votes in a massive way - on behalf of the authorized voters.

RISKS	POSSIBLE ATTACKS
	• An attacker could try to obtain valid voter's credentials (by guessing them, or through brute force attacks) and cast a valid vote on behalf of the authorized voter.
Unauthorized voters casting votes Non-eligible voters could try to cast a vote for a specific election.	• A non-eligible voter could try to cast a vote. • An attacker – as a non-eligible voter – could try to cast a vote by skipping the authentication process. • A voter could be granted access to the system to cast a vote in a specific contest, and try to cast a vote in a contest they are not granted access to cast a vote. • An attacker could try to modify the electoral roll managed by the voting application, to be included as an eligible voter.

Auditability

RISKS	POSSIBLE ATTACKS
Inaccurate auditability Not enough election traceability or audit data easy to tamper with may allow attackers to hide any unauthorized behavior.	• The voting systems do not register enough audit information to verify the voting process or the tallying process. • The voting systems register false audit information to demonstrate that a fraudulent election is right. • The audit information could be modified by an attacker – without detection, to demonstrate that a fraudulent election were right, or revoke a valid election.

2.5 OPERATIONAL RISKS

This section introduces a series of operational risks related to the Network Voting System. Generic risks that apply to any standard project are not included.

Polling Place Risks

RISK	POTENTIAL ATTACK
Required NVS technology not operative at the polling places The terminals used for voting and/or to manage the list of voters are not operative and cannot be used at the polling places	• Complex logistical process could lead to delays on delivery of the required components at the polling places • Software or hardware malfunction makes inoperable the NVS • Connectivity issues impede the NVS technology at the polling places to connect to the data center. This connectivity issue could range from a total interruption to sporadic but constant cuts that make the system inoperable. • Power outages could cause the NVS to be unavailable at the polling places • Sabotage on the polling place facilities (e.g. door cannot be opened, fire, etc.) and/or NVS components (removal of required components such as the screen, thieves, etc.) could lead to a non-available NVS. • Incorrect set up due to late delivery, employment of sub-qualified personnel, etc. could lead to an incorrect NVS set up at the polling place, rending marginally to not operative the NVS.
Electoral officials incorrectly operate the NVS at the polling places The electoral officials in charge of	• Insufficient training on such personnel, not detected on time, could lead to an incorrect operation of the NVS. The impact could include negative perception of EO

RISK	POTENTIAL ATTACK
operating the different NVS components are unable to operate it correctly	and the NVS, to violation of election principles. • Insufficient support provided to electoral officials. This may be caused by a poorly sized or inadequately trained support team. This could lead to incorrect resolution of electoral officials' problems when operating the NVS. The resulting inadvertent misuse of the system could result in election principles being affected. • NVS interfaces for electoral officials are not user-friendly, thus confusing electoral officials during the operation of the systems and/or making their work harder and/or slower. • Insufficient trained back-up personnel could lead to employ electoral officials not appropriately trained on using the NVS. This need could happen in case of strike, illnesses, natural disaster, etc. that could affect certain number of electoral officials at the same time.

Data Centre Risks

RISK	POTENTIAL ATTACK
Missing NVS components Certain required NVS central components, may it be hardware, software or communications related, are missing	• Delays on delivery of the required elements to the data centre • Sabotage on certain components, from internal or external attackers.
NVS functioning incorrectly Certain required NVS central components, may it be hardware,	• Sabotage on the configuration of any element in the data centre (external or internal) would affect the availability of the whole NVS.

RISK	POTENTIAL ATTACK
software or communications related, are functioning incorrectly, by themselves or when interacting with other elements	• Incorrect set up due to late delivery, employment of sub-qualified personnel, the inherent complexity of the data centre deployments, etc. could lead to an incorrect NVS set up at its central facilities, thus affecting the whole election. • Integration between the different components not performed correctly (e.g. due incorrect implementations, inappropriate requirements, connectivity issues…) could affect the election.
Technicians operate the NVS incorrectly Data centre technicians in charge of monitoring the correct operation of the NVS infrastructure behave (intentionally or unintentionally) in an incorrect way	• Insufficient knowledge on critical-mission systems could lead to an incorrect data centre operation affecting the NVS's availability. • Insufficient training on the deployed system could lead to its incorrect operation and maintenance, thus affecting the NVS's availability and auditability. • Corruption or coercion on data centre technicians could lead them to, on purpose, incorrectly operate the NVS in order to affect election outcome and/or its public image. • Inappropriate definition of required procedures to operate the data centre could lead to an incorrect system management and to incorrect decisions when unexpected situations happen.

EO Headquarters Risks

RISK	POTENTIAL ATTACK
Required NVS components not operative The NVS components operated by EO are not operative when required, affecting the whole election	• Logistical/procurement delays could lead to missing elements required to operate the NVS. • Software or hardware malfunction makes inoperable the NVS. • Connectivity issues impede the NVS technology at the headquarters to connect to the data center. This connectivity issue could range from a total interruption to sporadic but constant cuts that make the system inoperable. • Power outages could make the NVS unavailable at the headquarters • Sabotage on the headquarters facilities (e.g. door cannot be opened, fire, etc.) and/or NVS components (removal of required components such as the screen, thieves, etc.) would lead to a non-available NVS. • Incorrect set up due to late delivery, employment of sub-qualified personnel, etc. could lead to an incorrect NVS set up at the headquarters, rending marginally to not operative the NVS.
Electoral data availability Certain critical data required to configure/operate the NVS is missing or not available on time	• The data is not in the correct format defined before the election, thus affecting the NVS capability to process it automatically and potentially requiring manual operation which could affect election integrity, introduce manual errors in the election (e.g. missing candidates, etc.) and/or delays. • The required data is available too late for the NVS, delaying the opening of the electronic voting

RISK	POTENTIAL ATTACK
	period. • The data set is incomplete and has some missing information which can affect the election, thus producing delays and/or requesting manual operations which can introduce errors.
Incorrect NVS operation The technicians in charge of operating the NVS components located in the headquarters behave (intentionally or unintentionally) in an incorrect way	• Insufficient knowledge on critical-mission systems could lead to an incorrect operation of the NVS at the headquarters, affecting the NVS's configuration and delaying the start of the voting period and/or the final delivery of results. • Insufficient training on the deployed system could lead to its incorrect operation and maintenance, thus affecting the NVS's auditability and performance. • Corruption or coercion on headquarters technicians could lead them to, on purpose, incorrectly operate the NVS in order to affect election outcome and/or its public image. • Inappropriate definition of required procedures to operate the NVS's components at the headquarters could lead to an incorrect system operation on critical operations and to incorrect decisions when unexpected situations happen.

EO Help Desk Risks

RISK	POTENTIAL ATTACK
Incorrect support to Election Officials Help desk is unable to provide suitable support to Election Officials employing the NVS at the polling places	• Insufficient training provided to help-desk staff. • Insufficient trained back up personnel to cover situations where trained personnel are not available to cover help needs. • Second and third support levels not appropriate and/or undersized to provide effective help to the first level of support. • Insufficiently defined procedures and help guides do not allow help-desk staff to efficiently support election officials, having to scale up basic issues.
Incorrect support to voters Help desk is unable to provide suitable support to voters employing the NVS remotely	• Insufficient training provided to help-desk staff. • Insufficient trained back up personnel to cover situations where trained personnel are not available to cover help needs. • Second and third support levels not appropriate and/or undersized to provide effective help to the first level support. • Insufficiently defined procedures and help guides do not allow help-desk staff to efficiently support voters, having to scale up basic issues.

2.6 VOTER RISKS

The risks explained below are related to voters, and include their interaction with the NVS at different stages, their perceptions of the system in particular, and network voting in general.

Interaction with the network voting system

GENERIC RISK	THREATS
NVS is not user-friendly The interaction with the NVS is not easy an intuitive for voters, thus frustrating voting attempts and affecting public perception of EO and the NVS.	• Non-usable user interfaces which affect the capacity of the voters (or a subset of voters, e.g. elderly citizens) to satisfactorily cast a ballot without requesting assistance or dedicating much more time than expected. • Certain languages commonly employed by some group of voters are not included in the NVS voting interface, thus affecting the voting capacity of such voters. • The inherent dependency on third party software (e.g. web browsers) to create the voting user interface could lead to certain versions displaying the ballots in an odd way (e.g. contents displaced, options hidden), thus affecting the voting experience. • Legal constraints on ballot design limit the usability options in the electronic ballot layout. • Lack of appropriate help information can frustrate voters trying to cast an electronic ballot. • Voters employing old computers which are not compatible with the NVS. If the information about incompatibility is not clearly available to voters, it can lead to frustrating voting attempts.

GENERIC RISK	THREATS
	• Complex ballots and/or voting procedures that must be replicated in the NVS affect the voters' capacity to vote intuitively with no external support, thus affecting their perception of the NVS in particular and EO in general.
NVS does not provide appropriate accessibility features The NVS system provides insufficient accessibility features that impede certain voters to vote on their own with no external assistance	• There are some accessibility features, which should cover certain types of disabilities, that are missing, thus affecting the voters with such disabilities. • The accessibility features supported by the NVS are not correctly implemented, or implemented in a way that is not user-friendly for the voters affected by such disabilities (e.g. relying on a Braille keyboard when only a minority of blind voters knows Braille). • The voters use some accessibility accessories which are not supported by the NVS. • Legal constraints on ballot design limit the accessibility options in the electronic ballot layout.
Too cumbersome registration process The registration process required to use the network voting channel is too complex to make a critical mass of voters to participate	• The process requires too many and/or too complex steps which mitigates voters' willingness to participate • The process requires voters to have access to certain personal information not available to them • The data related to the voters required to execute the registration process has too many errors which affect the outcome. • The process relies on third parties, such as the postal service, which can introduce errors (e.g. delivery to the wrong addressee)

Voter Perception

GENERIC RISK	THREATS
Voter distrust of the NVS Voters may distrust the NVS, considering that it does not fulfill the required principles to be followed by an electoral process. This situation will make the voter an anti-eVoting advocate and will reduce the number of e-voters.	• Obvious security flaws (technical and/or procedural) affect the voter's confidence on the NVS and the election. • Anti-eVoting activists campaign very loudly against the NVS and/or EO's network voting initiative, getting attention from the media and the citizens. • Unfounded scams and hoaxes on the NVS make voters distrust the NVS. • Voters natural distrust on technologies affect their first approach to the NVS.
Voters deceiving the NVS Certain voters may try, and perceive incorrectly, that they can deceive the NVS	• Voters believe they have been able to vote twice or more times and that such different votes will be counted. • Voters claim to have never voted before, arguing that the NVS is flawed, to try to vote again on a polling place or even remotely. • Voters intentionally try to affect the NVS when voting remotely, by using "hacks" such as going back on the screen with the browser, and trying to cast a new ballot, etc.
Voter is not aware of the new voting channel The majority of voters addressed to use the NVS are not aware of this new possibility, or are aware too late	• Incorrect dissemination plan, which does not reach the target voters appropriately. • Dissemination activities are executed too late. • Insufficient dissemination activities.

Appendix C: Stakeholder Consultation Detail

At the meeting of the AAC held in Toronto on 26 January, the following questions were presented to the members of the committee who answered them in a round-table fashion:

1. Suppose Elections Ontario wanted to invite electors with disabilities exclusively to participate in our network voting test run. How feasible is that? What should Elections Ontario take into consideration about attempts to seek to confirm who is and who is not an elector with a disability?
2. Please discuss the importance of the following attributes, ranking them if possible and explaining why you ranked each as you did:
   - Privacy
   - Confidence in the system/security
   - Convenience and ease of use
   - Personal independence
   - Other
3. Thinking of different methods of network voting (internet voting, telephone voting, or other options such as smart phones or text messaging), please discuss the pros and cons for each option from the perspective of electors with disabilities.
4. How can the Committee best support the Network Voting project through to 2012 (e.g., participate in user acceptance testing, etc.)?
5. Who else among electors with disabilities should we consult with about network voting now or in future phases?
6. What assistive technologies or other supports might need to be utilized to make network voting possible for electors with disabilities (e.g., accessible EO website for electors that are blind; easy-to-understand directions for persons with cognitive disabilities; etc.)? (Are there needs of disabled electors that will require a different network voting solution than that for the broader population?)

Appendix D: Accessibility Factors for Web & IVR Content

BACKGROUND

The Accessibility Directorate of Ontario has drafted a regulation[19] that will require Government web sites to conform to WCAG 2.0 Level AA, in graduated degrees, beginning on January 2012. It does not prescribe any specific standards with respect to the accessibility of Interactive Voice Response (IVR) systems.

WEB ACCESSIBILITYFACTORS

The WCAG 2.0, published by the W3C, provides a detailed set of guidelines for web site content. These guidelines are aimed at making content accessible to all users, primarily disabled users. Although some of the design practices that support an accessible experience are specific, many of these practices are consistent with good web design. At a high level, the WCAG 2.0 specifies the following:

WCAG GUIDELINES

Content must be perceivable, meaning that it must be easy to read and that text alternatives are provided for video or audio content.

Content must be operable, meaning that functionality is available from the keyboard, users have enough time to read and understand the content (including considerations for authenticated sessions), and users have multiple ways to locate their position within the web site's navigation.

Content must be understandable, meaning that it is readable and free from unnecessary jargon or abbreviations, and does not require a reading ability beyond lower secondary education, and pages are predictable in terms of focus and context.

Content must be compatible, meaning that it can be interpreted by assistive technologies and, most importantly, that HTML (tags, ID attributes) is implemented according to specification.

SCREEN READERS

Users with visual impairments may rely on screen readers to access web pages. These assistive tools interpret the page's HTML code and reproduce it as speech. There are a number of ways that web pages can help a screen reader present an accurate and understandable interpretation of a web page. The use of tables for page layout, for example, may cause a screen reader to present content in a confusing or incorrect order and should be avoided.

In addition to considerations for blind users, colour-blind users can have difficulty navigating sites that rely on specific colours to present content or meaning, and users with low vision should have the ability to increase the text size or choose a high-contrast display option. Users with motor impairment may need to use the keyboard to navigate instead of a mouse, making it necessary for the site design to support keyboard-based navigation and selection.

IVR ACCESSIBILITY FACTORS

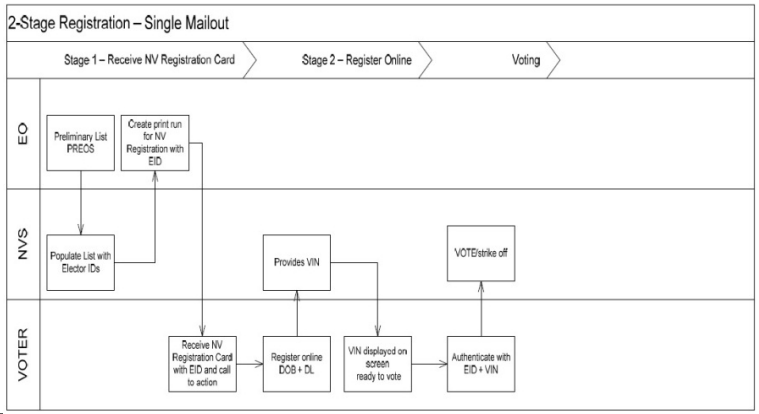
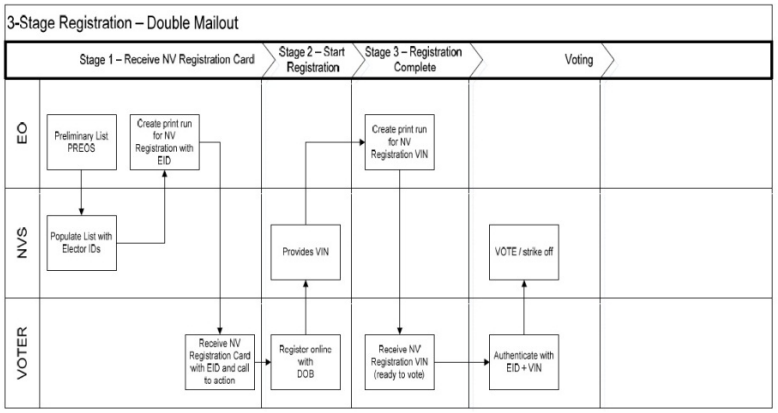
For any user, the usability of the IVR interface relies on the user's ability to hear and understand the menus and other recorded content. Usability also depends on the user being able to make selections from the menu options provided. Factors that affect the accessibility and usability of these actions include the following:

- Audio quality (including clarity of the recorded speech and a quiet background)
- Speed of the content and the ability to adjust the speed of playback
- Ability to adjust the volume level of the playback
- Ability to repeat or rewind menus and other content, as well as user selections
- Duration of the timeout imposed on user selections

These usability factors improve the overall user experience and also improve accessibility to users who have difficulty hearing or processing content, as well as those who have difficulty making selections due to visual or motor impairment. While blind users are able to obtain information aurally that would be inaccessible on a screen via text presentation, the IVR system must allow sufficient time for the user to make a selection from the menu.

Accessibility for the hard of hearing can be provided by the usability controls described above, provided that the volume level can be made loud enough. Accessing IVR systems for users who rely on TTY requires that the users TTY equipment is capable of producing DTMF tones, which is a limitation of some devices. From a usability perspective, the IVR system must allow sufficient time for the user to enter a selection without timing out.

APPENDIX E: AUTHENTICATION COMPARISON

	1	2
	2-stage process- Single Mail Out	**3-Stage process – Double Mail Out**
FLOW		
DESCRIPTION	• Two stages • system or voter can generate VIN/password • used by other jurisdictions in multiple elections(ex. Geneva since 2003)	• Three stages • system must generate VIN/password • used by Ontario municipalities in 2010 elections (Markham, Peterborough)
ADVANTAGES	• verifies voter identity using multiple methods • residence at mailing address • proof of identity (DOB + DL) • Voter is ready to vote immediately after proving identity online • registration can continue throughout the voting	• voter proves their identity using only their residence at mailing address and DOB • perceived mitigation of impersonation risk by stakeholders • some additional deterrent to impersonation risk (more difficult to intercept 2 pieces of mail than to intercept 1)

	1	2
	2-stage process- Single Mail Out	**3-Stage process – Double Mail Out**
	process • gives voters more flexibility • allows time for exception handling (electors with no DL) • Simple process facilitates adoption	• all voters will be processed in the same way • minor net security improvement ; checking identity using the same method twice (residence at mailing address) adds very little additional security, but can add perception of greater security
DISADVANTAGES	• simplicity of process may create perception of weaker security • electors without DL must be handled differently • Some options may require physical transactions • Some options may require voters to send proof of identity as in the special ballot case.	• longer elapsed time • shorter window for registration / early cutoff before start of advance poll to allow time for 2nd mail out to arrive • limited time available for handling exceptions • time for delivery of 2nd card will reduce adoption, especially for electors living in areas without home delivery • increased complexity for voter and EO • increased call centre volumes • increase postal cost / print cost and personnel overhead
RISKS	low-medium risk of impersonation if someone has access to mail and to DL number	• low risk of impersonation if someone has access to mail • complexity of process will reduce adoption / cause confusion • delays in receiving card will reduce adoption
EXCEPTIONS	• If no DL, then voters can prove identity on site at an	• losing the Election ID will require two extra mailings,

	1	2
	2-stage process- Single Mail Out	**3-Stage process – Double Mail Out**
	Returning Office or by mailing proof of identity (which will add time)	adding again to the elapsed time (starts the process over) • losing a password will require a third mailing, adding again to the elapsed time
ALTERNATIVES	• Voters could create their own passwords (subject to complexity rules) • password could be delivered through SMS • could restrict each user (Elector ID) to accessing the registration page only once	• Stage 3: delivery of second credential via an alternate channel (not mail, ie SMS) adds more deterrent to impersonation • could restrict each user (Elector ID) to accessing the registration page only once • adding DL to this process adds the same disadvantages as in the original process and forces extra exception handling, which will be very difficult to achieve given the shorter time frame

Appendix F: Poll Book Comparison

	1	2
	Network Voting with electronic poll book (ePB)	**Network Voting without electronic poll book (ePB)**
ASSUMPTIONS	ePollBook is required if remote and onsite network voting is implemented	EPollBook is not required if only remote network voting is implemented
FLOWS	**Onsite Voting Flow** 1. Voter presents ID at polling location 2. If voting by paper, the poll worker strikes the voter electronically using the ePB 3. If voting via computer, the poll worker uses the poll book to encode a token with the ID/password that is stored in the voting system. 4. The voter inserts the card at the computer, which reads the Elector ID and password. 5. The voter selects the voting options and casts a ballot 6. The NVS processes the vote, and strikes the voter electronically **Remote Voting Flow** 1. Voter authenticates online using Elector ID and password 2. Network voting system processes the vote and strikes the voter	**Onsite Voting Flow** 1. Printed list is distributed to polling locations, indicating voters that have registered to vote remotely. 2. Voter presents ID at polling location and poll worker checks eligibility on printed list 3. The poll worker will give a ballot only to voters who are not registered to vote online 4. The poll worker strikes the voter from the paper list. **Remote Voting Flow** 1. Voter registers to vote remotely (using telephone or computer) before the advance polling period begins. 2. Voter authenticates online using Elector ID and password 3. Network voting system processes the vote and strikes the voter. 4. Voter is not able to vote a second time using either remote channel.

	1	2
	Network Voting with electronic poll book (ePB)	**Network Voting without electronic poll book (ePB)**
	3. Voter is not able to vote a second time using either remote channel. 4. ePB is updated in real time 5. If the voter presents at a polling station, the poll worker will see that the voter has voted already **Revisions Flow** 1. EO staff add or remove voters from the list using the ePB 2. The updates are synchronized in real time with the network voting system	**Revisions Flow** 1. EO staff correct and update the voters list using the current back end systems and processes 2. The updates are synchronized as needed with the network voting system using manual processes. 3. A final sync is run between the network voting system and ELMS/EMS after the event.
DESCRIPTION	An electronic poll book is required in a scenario that combines remote password voting and on-site computer voting using physical ID. Since the onsite voter proves his or her identity to a poll worker using a physical mechanism, an electronic mechanism is required to connect the individual to the identity (Elector ID) stored in the network voting system. This lets the system determine eligibility (that the voter is in the list and has not voted before). The electronic poll book is a system that: • provides a link between onsite person and registered identity in NVS	In a scenario that uses only remote network voting combined with paper ballots, an online poll book is not strictly required, provided that another means can be implemented to prevent voters from voting online and then voting on paper, or vice versa. Each channel (network and paper) will effectively manage its own list in parallel and any need to synchronize will be handled manually as exceptions and will not be in real time. • ELMS or EMS will provide the back end voters list 'of record' and will generate the paper lists used at the polling locations. • ELMS or EMS will also provide the network voting system with the list of electors (PREO). The

	1	2
	Network Voting with electronic poll book (ePB)	**Network Voting without electronic poll book (ePB)**
	• integrates with the back end voters list (EMS) (including revisions) and the online system. • Provides real-time strike off (of all channels simultaneously, including paper) Note that the network voting system also maintains an electronic electoral roll that is the list of voters who are permitted to vote using the network channels. It can function independently of EO's voters list and is designed to provide a) real-time strike off of network voters; and b) linking of voters to encrypted ballots. It is **not optional**, and should be included in the network voting product.	network voting system will then assign a unique identifier to each elector (the Elector ID) • Electors who wish to vote remotely will register online or by phone and associate additional credentials with their Elector ID • Voter registration must end in advance of the advance poll date so that printed lists can be generated and distributed • Electors who register for the remote network voting channels will then be 'locked in' to network voting and would be unable to vote by paper. (*exceptions are possible for electors to request that their NV credentials be cancelled so that they can vote by paper). • The voters list at polling locations will not be automatically synchronized with the online network voting list The network voting system's electronic electoral roll contains the real-time list of voters who are permitted to vote using the network channels. It functions independently of EO's voters list and is designed to provide a) real-time strike off of network voters; and b) linking of voters to encrypted ballots. It is **not optional**, and should be included in the network voting product.
ADVANTAGES	• Supports principle of one vote per voter by preventing multiple votes	• Supports principle of one vote per voter by preventing multiple votes (one by paper, one by

	1	2
	Network Voting with electronic poll book (ePB)	**Network Voting without electronic poll book (ePB)**
	• Allows on-site voting using physical identification (i.e. the simpler option for voters) • Allows real-time synchronization of voters list (ELMS/EMS) with network voting system (easy way to handle voters list maintenance)	remote computer or telephone) • Does not require on-site computers and hardware and therefore reduces cost and complexity
DISADVANTAGES	• Adds cost and complexity to polling operations • requires on-site computers and hardware • requires training of poll staff • Add cost to vendor implementation, depending on • extent of integration with existing EO systems (ELMS/EMS) • technology options for integration (web services, file upload)	• Without an ePB, the online network voting system will not be synced with the backend voters list (ELMS/EMS) • Voters list maintenance must therefore be carried out in other ways: • A) freeze network voting list based on the preliminary voters list. (PREO). This is a reasonable measure to take for a pilot, as the volume of edits is likely low (<5% of total names); or • B) update NV list (deletions, changes to ED) manually as revision occur (e.g. by using an NVS back office interface or by uploading data files)
RISKS	Integration with EO processes and systems could add complexity to customization and rollout phases of project – including operational aspects at the polling stations	• Without locking in voters, there is a high risk that voters could vote twice (once remotely, once on site). Although this risk exists now with paper advance polls, the risk will have a much higher public profile with network voting and should be managed differently • Voters could register for network voting and then either decide not to or be prevented from doing so.

	1	2
	Network Voting with electronic poll book (ePB)	**Network Voting without electronic poll book (ePB)**
		If they remain 'locked in', they could be unable to vote at all
EXCEPTIONS	Additions and deletions to the voters list are handled in real time	To manage risk, electors who registered for network voting but haven't could be 'released' after the network voting period is over so that they can still vote by paper on election day Additions to the NV list would not be allowed once the NV online list is produced. Voters who must be deleted from the online list once it is in the NV system can be removed manually through an administrative interface
ALTERNATIVES	Required online functionality could reside in EO systems, the vendor solution, or a hybrid could be designed This would be a decision driven by: Vendor's ability to integrate and customize EO's ability to integrate and customize A simpler integration NVS/EMS is possible if no real time updates for new voters are required: Integration can be as simple as importing files before voting starts at once per day with the updates.	If locking voters in to the network voting channel is not acceptable, the ELMS/EMS list could be synchronized regularly (daily) with the NV online system by reviewing the list of paper strike-offs and striking them electronically from the network voting list. Alternatively, network votes cast by voters who also voted in person by paper could be removed as often as daily, or after the election. While this approach still supports the principle of one vote per voter, it will leave the impression that multiple voting is somehow possible and give the *appearance* that the principle is not being supported.

Appendix G: Definitions of Principles

The following list of principles was used as the basis for the process described in Section 3, above (Principles: Evaluating Network Voting). It is from this complete list that the final list of core network voting principles was derived. The list is divided into two groups: Universal Principles and Procedural Principles.

UNIVERSAL PRINCIPLES

BASIC PRINCIPLE	DETAILED PRINCIPLE	DESCRIPTION
1. Universality	1.1. Usability	The voting process is easy to understand and execute by any voter. Voters shall not need any special technical, cultural or legislative skills to cast a ballot.
	1.2. Accessibility	The voting process is equally accessible to all eligible voters, including voters with disabilities. In any case, the voting process shall be performed by the voter without requiring any assistance for making their selections.
	1.3. Reachability (location)	The means required to vote are easily reachable by any voter, independently of the voter's physical location during the voting period.
2. Equality	2.1. One vote per voter	Only one vote per voter is counted for obtaining the election results. This shall be fulfilled even in the case the voter is allowed to cast multiple votes.
	2.2. No privileged voters	There must be no voter (individual or a group) with any technical, logical or decisional advantage respect to other voters. Each vote has the same value regardless the voter who cast it.
	2.3. No privileged actors	There must be no person or entity involved in the management or implementation of the electoral process capable of influencing the electoral process and/or gathering non-public information.
	2.4. Voter authentication and authorization	The electoral process shall ensure before allowing a voter to cast a vote, that the identity of the voter is the same as claimed, that the elector is eligible to vote, and that she has not exceeded the allowed voting intents.
	2.5. Right to be on the Voters List	The electoral process shall ensure that all eligible voters are included in the Voters List and provide means to voters to claim their right to vote if they are not present in it.

BASIC PRINCIPLE	DETAILED PRINCIPLE	DESCRIPTION
	2.6. Only count votes from valid voters	The electoral process shall ensure that the votes used in the counting process are the ones cast by valid eligible voters.
	2.7. Fair ballot layout	Voting process shall ensure that all the voting options, parties and candidates have the same right to be in the ballot. The ballot design or distribution of voting options shall not favor any party or candidate. This principle should be preserved independently of the voting channel used by the voter to cast the vote.
	2.8. No cost for voters	Voters must not incur specific costs for exercising their right to vote.
	2.9. Fair Voters List generation	The electoral process shall use a Voters List honestly generated based only on data from valid voters. All valid voters must be included in this Voters List.
3. Freedom	3.1. No coercion or vote selling	The voting process must prevent voter coercion and vote selling. This is usually achieved by not providing any information to the voter or any other third party that could be used by a coercer or vote buyer to discern the voter intent of the vote cast by the voter.
	3.2. Individual verifiability	The voting process shall provide means to the voters for verifying that their votes have been properly deposited inside the ballot box (vote recorded as cast).
	3.3. Integrity	The voting process shall ensure that the outcome of the election represents the opinion of the participating voters and therefore, it is obtained only from votes cast by valid voters. Furthermore, the voting process shall ensure that votes from valid voters have not been manipulated or the ballot box stuffed.
4. Secrecy	4.1. Personal data privacy	This information related to voters shall only be used for the specific purpose of the election and cannot be accessed by any unauthorized actor.
	4.2. Ballot secrecy	The voting process shall preserve the secrecy of the cast votes until they need to be processed in the counting process.
	4.3. Voter privacy	The voting process shall prevent at any stage of the election the correlation between voters and the contents of the ballots cast by such voters.
	4.4. No intermediate results	The voting process shall prevent any access to the contents of the cast votes until the counting process.
	4.5. Secure data decommissioning	The voting process shall provide secure decommissioning practices of any voting material, records and data that could compromise the privacy of voters.

PROCEDURAL PRINCIPLES

BASIC PRINCIPLE	DETAILED PRINCIPLE	DESCRIPTION
5. Transparency	5.1. Voter training	The electoral process should provide voters means for learning and understanding the voting process before the actual election.
	5.2. Information/diffusion	Information related to the electoral process (schedule, technology, procedures, audit results., etc.) shall be made publicly available. Information shall be accurate and available enough time before the election.
	5.3. Easy to explain / understand by voters	The electoral process shall be as simple and easy to explain as possible.
6. Verifiability and accountability	6.1. Source code auditability	The source code and binaries of any software used for managing the election processes or data, shall be available for auditing and, if required, certification. Audit process shall be performed by independent auditors to ensure that the electoral process behaves properly.
	6.2. Process auditability	The behaviour of the procedures of the election process shall be well documented and auditable in order to ensure that they accomplish with the expected requirements.
	6.3. Certification	The voting process and any logical of physical components related to it shall be designed to facilitate any certification of their design principals. The certification will confirm if the election process can accomplish with the claimed specifications.
	6.4. Results validation	The voting process shall provide means for verifying if the results clearly represent the intention of the voters that participated in the voting process. This verification shall also ensure that only votes from valid voters have been used in the counting process to prevent fraud practices that could compromise the election accuracy.
	6.5. Election Monitor	The elections process shall support the election monitor of all the transactions carried out during the process. This monitor process shall be sound and shall guarantee that voter secrecy is preserved at any time.
	6.6. Review logs/forensics	The election process shall leave traces of the activities carried out during the process (e.g. logs). These traces shall be available for being analyzed during and after the election in order to ensure that the electoral process behaves properly.
	6.7. Potential partial reruns	The election process shall allow the resume of an active election from the same stage in which it was paused / stopped without losing any information that was already recorded.

BASIC PRINCIPLE	DETAILED PRINCIPLE	DESCRIPTION
7. Reliability and security	7.1. Service availability	The election process and any of its critical components or entities (e.g., electoral roll information, cast votes, voting channel, etc.) shall be available during the whole election period to voters, election managers, observers or any other actor involved in the process.
	7.2. No single point of trust	The election process shall not trust any single entity (person or system) for implementing any critical step. Entity privileges shall be restricted by segregation of duties policies, to require the collaboration of multiple entities for implementing critical processes.
	7.3. Platform integrity	The election process shall provide means for protecting the integrity and authenticity of the entities and components that participate in the process. These means shall be verifiable during the election process, to ensure their correct behaviour. Audit procedures can be done before and after the election process.
	7.4. Access control	The election process shall provide means for controlling and registering the access of entities to the different steps and components used in the process.
	7.5. Ballot box integrity	The election process shall provide means for preserving and detecting any manipulation of the ballot box.
	7.6. Logs integrity	The election process shall provide means for preserving and detecting any manipulation of the activity logs or registers recorded during the process.
	7.7. Voters List integrity	The election process shall provide means for preserving and detecting any manipulation of the electoral roll information.
	7.8. Election configuration integrity	The election process shall provide means for preserving and detecting any manipulation of the election configuration information used to setup the election.
	7.9. Ballot Integrity	The election process shall provide means for preserving and detecting any manipulation of any individual ballot cast by a valid voter.

Glossary of Terms

A	Authentication process	The process of confirming voter identify and authorizing access to the voting system.
D	Data Centre	The technical infrastructure used to host servers, usually connected to the Internet. There are several categories of data centres based on the levels of security, availability, performance, etc. they offer. A network voting system will require servers to be hosted in a reliable data centre.
	Denial-of-service attack (DoS)	An attempt to make a computer resource (such as a web site) unavailable to its intended users. A common method of attack involves saturating the target machine with requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable
E	Elector	In the context of this document, the word ‘elector’ is used to denote any Ontarian who has the right to vote, whether or not they actually do interact with any voting system or process. See ‘voter’ for differentiation.
	Electoral Authority	The entity in charge of planning, organizing, and executing an electoral process in a given territory. In the context of this document, it refers to Elections Ontario.
	Electronic voting	Electronic voting (e-voting) is a term encompassing several different types of voting. It includes electronic means of both casting and counting votes. Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.
	End-to-end security (encryption)	A way to ensure that the ballots cast by voters are protected from their origin, so that only the electoral authorities can process the ballots. (I.e. no external hacker or internal voting system technician can affect the ballot integrity or the voter's privacy).
I	Internet voting	Also known as i-voting, internet voting is a specific implementation of remote electronic voting, whereby the vote takes place over the Internet such as via a web site. The term is sometimes used

		interchangeably with Remote Electronic Voting. That usage is deprecated and is now used only to refer to a specific subset of remote electronic voting.
	IVR - Interactive Voice Response	A system that provides an audio interface to voters so they can cast ballots over a conventional telephone.
L	Login	A series of characters, usually easy to remember and/or linked to some data related to the voter, used to identify the voter in a network voting system. It is usually coupled with a password to authenticate the voter.
M	Man in the middle attack (MITM)	A form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones. A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other
N	Network Sniffing	Also known as ‘packet analyzer, a network sniffer is a program that intercepts and logs network traffic in an attempt to analyze activity. A sniffer can have many legitimate uses, including intrusion detection and system monitoring, or it could be used to spy on users and collect sensitive information.
	Network voting	Any type of electronic voting that involves casting and sending the ballots in electronic format to a central facility.
	Network Voting Management Board	The group of persons responsible for supervising the processing (counting) of the electronic ballots.
O	On-site electronic voting	This term is used to define the voting process that take place in supervised locations (e.g. polling places) by means of electronic devices. These devices can be isolated or connected to a network.
P	Password	A combination of characters, usually alphanumerical, that is only known to the voter and that is used by the voting system to authenticate voters. Usually passwords are accompanied by a unique "login" per voter. Sometimes, login and passwords can be combined in a single series of characters known as VIN.

	PIN	Personal Identification Number, usually employed by voters to access a mobile phone or smartcard. Note that a PIN is different from a VIN.
	Poll worker	Personnel that work in a polling station during the electoral process, who are responsible for identifying voters and facilitating the voting process.
	PSTN	The Public Switched Telephone Network.
R	Remote electronic voting	The preferred term for voting that takes place by electronic means from any location, without direct supervision from electoral authorities. This could include the use of the Internet, text message, interactive digital TV, or touch tone telephone.
S	SMS Gateway	The technical infrastructure used to send and receive short text messages in high quantities. Usually there are specialized companies offering this service which can operate with the different cellular networks.
	SSO - Single Sign On	A mechanism that allows users to access a system after having been authenticated in a different one.
	Spoofing	A legitimate web page is reproduced on a server under control of the attacker. The intent is to fool the users into thinking that they are connected to the trusted site.
T	Telephone voting	A specific case of network voting, whereby the vote is cast using a telephone and the voter interface is based on voice, a menu system, and numerical input.
V	VIN	Voter Identification Number, a combination of characters that can be used to authenticate a voter. A VIN is usually used in replacement of login/password couples.
	VOIP	Voice Over Internet Protocol, which is a communications protocol that allows voice communication to be transmitted over the Internet.
	Voter	In the context of this document, the word ‘voter’ refers to a person who is interacting with a voting system or process and is therefore actively exercising their right as an elector. An ‘elector’ becomes a ‘voter’ when he or she accepts a ballot at a voting location or authenticates using the network voting system. See ‘Elector’ for differentiation.
	Voter	The mechanism used by a network voting system to grant access to a

Authorization	voter to the system, so he or she is able to cast a ballot. Usually authorization follows voter identification, although in network voting the same mechanism can provide both voter identification and authorization.
Voting credentials	Voting credentials are the pieces of information used by an elector to authenticate him or herself at the time of voting.
Voter Identification	The mechanism used to validate that a voter is who he or she claims to be. Sometimes the same mechanism is used to identify and authorise a voter, but this is not always the case.

---

[1] http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90e06_e.htm#BK12

[2] http://www.elections.on.ca/en-CA/AboutUs/Mission.htm

[3] http://www.ontario.ca/en/login/ONT03_026063.html

[4] http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90e06_e.htm

[5] Elections Canada: Survey of Electors Following the 40th General Election
Ipsos Reid Post-Election Survey, 2007

[6] http://www.statcan.gc.ca/daily-quotidien/100510/t100510a1-eng.htm

[7] http://www40.statcan.gc.ca/l01/cst01/comm32a-eng.htm

[8] http://www40.statcan.gc.ca/l01/cst01/comm29a-eng.htm

[9] http://www.statcan.gc.ca/daily-quotidien/100510/dq100510a-eng.htm

[10] http://www.statcan.gc.ca/daily-quotidien/070504/dq070504a-eng.htm

[11] http://webaim.org/blog/screen-reader-user-survey-3-results/

[12] Statistic provided at Municipal iVoting Learning Summit, Toronto, 15 December 2010

[13] Peterborough 2010: 16% of votes cast were network votes

[14] *The principles used as the basis for this analysis were based on those recommended by the Council of Europe.* http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/Key_Documents/Rec%282004%2911_Eng_Evoting_and_Expl_Memo_en.pdf

[15] For example, Ontario's Enhanced Drivers License contains a RFID chip that stores only a unique identification number that denotes Canadian citizenship. It is designed as a passport alternative for the Canada-US border.

[16] The One-key service being launched by ServiceOntario will likely be a very good future candidate for this approach.

[17] These controls are linked to the requirements section of the Network Voting System (see Appendix A: Detailed Requirements).

[18] Information must include at least the number of voters, so credentials can be generated, i.e. the NVS would not need real names if the EMS covers it

[19] *The proposed Integrated Accessibility Regulation was posted for public review from 1 February to 18 March 2011. Part II, Section 14 deals with accessible web sites.*