Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

# Security considerations for electronic poll book systems

MANAGEMENT

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

# Foreword

This document is an UNCLASSIFIED publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email, or phone our Service Coordination Centre:

**Service Coordination Centre**

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

# Effective date

This publication takes effect on February 7, 2022.

# Revision history

| Revision | Amendments | Date |
|---|---|---|
| 1 | First release. | February 7, 2022 |
| | | |
| | | |
| | | |

# Overview

This document provides guidance on cyber security considerations required to securely design, deploy, and operate electronic poll book systems. The document highlights traditional poll book functions and discusses new services that can be integrated to support modern elections.

It also provides recommendations on security configuration controls that election authorities may consider when evaluating, designing, or deploying electronic poll book systems.

ISBN 978-0-660-42356-2
CAT D97-4/10-101-2022E-PDF

# Table of contents

## List of figures

## List of tables

# Introduction

Modern elections are increasingly driven by information technology tools designed to optimize processes and increase transparency. Several nations, including Estonia, Norway, and Canada, have implemented different forms of electronic voting systems to manage democratic elections with varying success outcomes. The use of electronic poll books is common among most election modernization strategies. Electronic poll books offer a multi-function platform to introduce efficiencies and optimize election day activities.

Traditional poll books are typically paper based and used primarily for manual voter check-ins. While these are perceived as highly reliable, they are inadequate to effectively optimize election day activities. Paper poll books can lead to voter processing delays and human errors on election day and cannot support newer services such as real-time voter turnout tracking, to enable efficient poll resource management. Electronic poll books technologies can assist with addressing some of these challenges, as well as offering new opportunities for additional services to improve election day processes.

In this document, we discuss some of the benefits of using electronic poll books but focus primarily on security considerations for safeguarding its deployment.

## 1.1 Electronic voting system architecture, standards, and technologies

Though federal elections in Canada use minimal technology for ballot casting, there are still several back-end activities that rely on technological systems. For example, election day activities such as ballot results reporting and collation is delivered through information technology systems that take advantage of telecommunication systems and web technology.

There is an expectation that electoral bodies identify opportunities to improve components of the electoral process. The use of technology can help achieve these goals but may introduce unintended outcomes (e.g. introduce security vulnerabilities in the election process). Therefore, it is important to emphasize safe security practices to drive any modern election transformation strategy. In the sections below, we will review a general architecture for electronic voting systems, highlight electronic poll books, and discuss strategies to securely manage them.

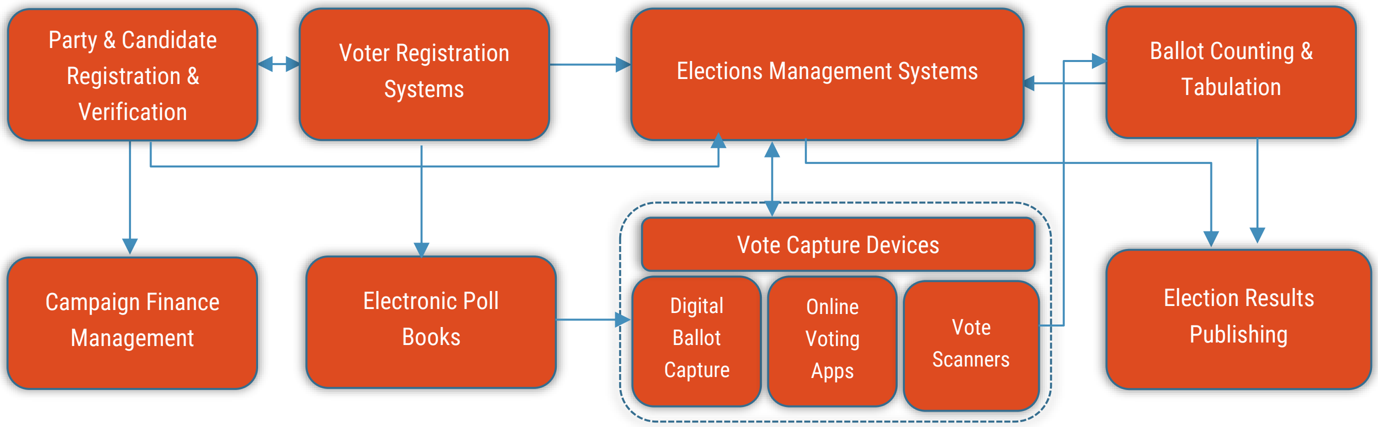
### 1.1.1 Electronic voting system architecture

Electronic voting system architecture describes the information systems components involved in electronic voting and how these components interact with each other. These systems may include:

- Public websites
- Party registration systems
- Voter registrations systems
- Election management systems
- Internet voting systems
- Ballot counting systems
- Results publishing systems

These systems, often running disparate technologies, are interconnected and communicate across diverse network protocols. Based on *A Handbook for Elections Infrastructure Security* published by the Center for Internet Security (CIS), a generic modern electronic voting systems architecture is as shown in Figure 1. [1]

**Figure 1: Generic elections systems architecture**


Party & Candidate Registration & Verification
Voter Registration Systems
Elections Management Systems
Ballot Counting & Tabulation
Campaign Finance Management
Electronic Poll Books
Vote Capture Devices
Digital Ballot Capture
Online Voting Apps
Vote Scanners
Election Results Publishing

| Key | Description |
|---|---|
| → | Data flow path |
| 🟧 | Electronic system component |

As it specifically relates to electronic voting systems, one or more of these core capabilities can be implemented through the aid of both software and hardware computing systems. Some of these components may communicate via the Internet or over private communication networks.

# 2 Electronic poll books

Poll books, also called lists of electors, contain personal information on approved electors for a particular polling area. This list contains approved voter information that polling staff rely on at each location. An electronic poll book is an electronic device running a software application that manages the list of approved voters for an electoral region. Polling staff use the poll book data to look up and validate individuals who present themselves to vote. There are two major models for the deployment of poll books – standalone and networked model solutions.

## 2.1 Deployment model for electronic poll books

Electronic poll books can be deployed in a standalone or a networked deployment model. Below, we review some of the characteristics of each deployment model.

**Table 1: Standalone vs networked model**

| | Standalone model | Networked model |
|---|---|---|
| ***General description*** | This involves the deployment and operation of the poll book with no network connectivity. Ahead of an election, voter registration data is migrated to the poll books to manage election day activities. | This involves the deployment of the poll books with partial or full network connectivity, typically communicating with a central election management network over the public Internet. Networked poll book deployments provide an added advantage of being able to support real-time services. |
| ***Wi-Fi and internet connectivity*** | In this model, the poll book device is not connected to a Wi-Fi network or the internet when in a production environment. | The poll book device may or may not be connected to a Wi-Fi network or the internet for election day activities. |
| ***Data migration*** | Data migration, including the electronic voter register, is completed ahead of election day. The data is transferred via an interface (e.g., USB, Wi-Fi). Data migration is disabled for election day activities. | This model supports both offline and online data migration models. Data can either be migrated continuously over a network or via scheduled data transfer on election day. |
| ***Election day activities*** | Deployments cannot facilitate "vote anywhere" capabilities during an election. | Some deployments may be able to facilitate "vote anywhere" capabilities, allowing the elector to vote outside of their local riding. |
| ***Software updates*** | Once the poll book device is deployed, real-time software or system updates will not be available. | Real-time software or system updates can be supported even after deployment for election day activities. |

### 2.1.1 Benefits of electronic poll books

Some of the benefits of electronic poll book solutions include:

- Improves the efficiency of the accreditation and validation process;
- Reduces or avoids manual errors through automation of voter check-ins and reporting;
- Redirect voters to their appropriate polling station;
- Reduces voter fraud by easily identifying incidents of voters associated with multiple ballots; and,

- Supports the delivery of additional services such as election day voter registration, voter identity validation, and real-time reporting.

## 2.2 Threats against electronic poll book systems

Deploying technology to support or replace manual electoral processes can be beneficial. However, inadvertent threats and vulnerabilities may be introduced as well. These threats may be associated with the physical manipulation of the poll book device, configuration of hardware system components, software code flaws, supply chain attacks or vulnerabilities associated with the network communication infrastructure. The use of electronic poll book applications during an election, either in a standalone or networked model, will most likely increase the attack surface. Therefore, proactively identifying these potential threats and implementing appropriate safeguards to protect affected systems is crucial.

Please note that the list enumerated below do not represent an exhaustive list. We recommend that organizations carry out threat modeling within requisite threat-risk assessments to identify and adequately map threats associated with their deployment requirements.

1. **Data integrity attacks**: Electronic poll book systems will hold sensitive data including information on voters, polling processes, and elections systems. Data corruption, inadvertent data destruction, human error, and spoofing attacks are examples of threats that may impact the integrity of your data.
2. **Cryptographic attacks:** Cryptographic controls, such as encryption, are used to protect the confidentiality and integrity of data at rest and in transit on electronic poll book systems. Weaknesses in the implementation of cryptographic algorithm may lead to exploitation by threats actors to compromise the cryptographic protections around the data. Cryptographic software vulnerabilities, poor key management, and misconfigurations are key security challenges that require closer attention. Developments in quantum technology and increasing computational strength is also a growing threat. For more information on quantum threats, we recommend reviewing the following publications*: Preparing Your Organization for The Quantum Threat to Cryptography (ITSAP.00.017)* [2] and *Addressing the Quantum Computing Threat to Cryptography (ITSE.00.017)* [3]
3. **Wireless attacks**: The convenience of wireless networks makes them a favourable solution for organizations. Wireless networks can also make organizations an attractive target for threat actors.  Unsecured wireless networks introduce the potential for wardriving, person-in-the-middle (PITM), and network traffic sniffing attacks. Default settings on wireless devices can also introduce vulnerabilities that can be exploited. Nonsegregated networks can increase the impact of damage to computing assets when a successful attack occurs. Hackers can easily pivot from one network segment to the other.
4. **Distributed denial of service (DDoS)**: The infrastructure supporting electronic poll book systems could be subjected to targeted DDoS attacks if appropriate protections are not in place. Threat actors can deploy malware to disrupt operations and flood servers, thereby leading to availability issues and resource exhaustion, hindering access to the electronic poll book infrastructure. These disruptive attacks can be used to repress votes when attacks are focused on a segment of the voting public.
5. **Malware attacks**: Threat actors or hackers can use phishing, social engineering, supply chain attacks and other sophisticated techniques to infect electronic poll book systems with malware. Threat actors may use malware tools to enable initial entry and facilitate additional comprehensive attacks.

6. **Data breaches**: Human error or threat actor-initiated attacks can lead to personal or sensitive information disclosure. Unintentional actions of election stakeholders can lead to a data breach, which could compromise the confidentiality and integrity of an electronic poll book system. Confidential information such as cryptographic keys, ballot data, passwords, and voter details can be accessed by unauthorized parties.
7. **System vulnerabilities**: Vulnerabilities (software or hardware) present within infrastructure components could be exploited to manipulate or update voter information. System related vulnerabilities can be exploited to compromise the integrity of the poll book system. Each component of the electronic voting infrastructure could be potentially vulnerable.

# 3 Security considerations for electronic poll books

The security of your organization's electronic poll book infrastructure relies primarily on the effectiveness of the controls in place to secure your hardware, software, network, and data. Security controls deployed must work in tandem and complement each other to address potential gaps and threats associated with your deployment.

Electronic Poll books should be deployed as a single purpose system.

The recommendations discussed below are considerations to minimize the risks associated with the use of electronic poll book systems in elections. The recommendations do not represent an exhaustive list of security considerations. Your organization should consider conducting a threat risk assessment to ensure security measures implemented are tailored to the threats associated with your electronic poll book infrastructure.

1. **Establish a guiding framework and a set of principles for the use of digital technologies.** Implementing a guiding framework with appropriate legal guard rails for the use of digital technologies in the electoral process represents a significant foundational step. Putting in place a legislative mandate and appropriate supporting guiding principles will ensure that the new digital systems stay consistent with existing electoral processes, as well as making sure that our core democratic values are preserved. Values such as voter anonymity, fairness, integrity and transparency represent fundamental pillars upon which your digital elections strategy, including the use of electronic poll books, should be dependent on. A guiding framework for digital elections can also be useful for evaluating the adequacy of proposed electronic solutions and third-party services.
2. **Choose solutions developed using best practice security standards.** The security standards supported in any digital poll book solution will most likely influence the choice of controls available to be deployed. Ensure that the electronic poll book solution chosen conforms to best practices and secure development standards. Poll book solutions developed based on secure coding best practices will help promote security, reliability, and resiliency of the entire system. Conformance to application development standards such as the Open Web Application Security Project (OWASP) Secure Coding Guidelines, Center for Internet Security (CIS) Critical Security Controls, and MITRE Secure Code Practices, will ensure unsafe software development practices are avoided. The benefit of choosing solutions with best practice standards include interoperability, resiliency, and security. Other standards to consider for alignment include Federal Information Processing Standards (FIPS), and International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) Standards.
3. **Select products with verifiable and traceable supply chains.** Ensuring that products or solutions supporting our democratic processes have verifiable and traceable supply chain associations is fundamental. Some nation-state actors are known to take advantage of access to global supply chain paths to compromise systems during development. Management should institute a Supply Chain Risk Management (SCRM) program for oversight and integration with purchase processes. Build SCRM requirements into your processes. Conduct periodic assessments and due diligence of vendors and suppliers to evaluate any changes to their ownership structure or relationships. The Canadian Centre for Cyber Security (Cyber Centre) provides supply chain risk assessment services to support Canadian critical infrastructure sectors, which Democratic Institutions is a sub-sector. Election management bodies can reach for assistance to evaluate critical components of their digital election infrastructure. Please refer to the Cyber Centre's publication on *Supply Chain Threats and Commercial Espionage* [4] for more information.

4. **Implement end-to-end cryptographic protections and data security controls.** The security of all sensitive data such as electronic voter records should be a critical objective of every electronic poll book solution. Data encryption and data integrity controls to safeguard electronic poll book data is strongly recommended.  To address data confidentiality and integrity risks, data in transit or at rest on the electronic poll book media should be encrypted. Cryptographic protections available within modern operating systems to safeguard data in memory should be enabled. Only applications using approved FIPS 140-2/140-3 algorithms should be used to encrypt data. Please refer to our Cryptographic Module Validation Program (CMVP) [5] webpage for the most recent guidance on approved cryptographic standards. Session and encryption keys and passwords should be properly managed to avoid compromise. Whether your poll book application runs on or off-the-cloud, you may also consider other advanced data security controls such as data masking, data classification and tokenization techniques to safeguard specific sensitive data fields and values. Tokenization is an automated process of replacing sensitive data elements with non-sensitive data. For more information on tokenization techniques, please refer to the Cyber Centre's publications: *Guidance on Cloud Service Cryptography (ITSP.50.106)* [6] and *Guidance on Using Tokenization for Cloud-Based Services (ITSP.50.108)* [7].
5. **Implement network security controls to secure communications.** Connect your electronic poll book devices to approved wireless or wired networks only. Implement network segmentation and segregation controls around the poll book network. Implement virtual routing and forwarding (VRF) for logically segmenting Layer 3 traffic, VLANs for Layer 2 traffic, and host-based firewalls to restrict and manage traffic to or from the poll book network. Ensure application filtering controls are in place to prevent malicious requests from compromised poll book devices. Use Virtual Private Networks (VPNs) to secure communications from the poll book to other devices on the network. Select VPN encryption solutions based on only approved algorithms and avoid the use of obsolete protocols. To learn more about VPNs, please see our publication on *Virtual Private Networks (ITSAP.80.10)* [8]. In addition, consider implementing mutual authentication or two-way authentication mechanisms to ensure that all devices are authenticated. Zero trust security principles should be considered when designing and integrating components of your poll book network. Avoid implicit trust of network components. Continuously authenticate and authorize network assets and services. Restrict physical access to network access points to protect against physical attacks.
6. **Implement multifactor authentication and strong password policies.** To mitigate the risk of unauthorized access and password attacks, implement multifactor authentication (MFA) on your devices and poll book application. Set and enforce secure password policies such as the use of strong passwords and do not allow shared accounts on the devices. Change default usernames and passwords related to the hardware device and the poll book application before deployment to the field. In scenarios where biometrics-based authentication is implemented, liveness detection controls should be supported. Liveness detection techniques involves the ability to detect if a biometric dataset presented is from a real person or spoofed (image photo, video, or audio recording). Implement account lockout measures or remote wipe capabilities on devices to protect data after multiple authentication failures. For more information on authentication, passwords and biometrics security, please refer to the Cyber Centre's publications *Biometrics (ITSAP.00.019)* [9], *Best Practices for Passphrases and Passwords (ITSAP.30.032*) [10] and *Secure Your Accounts and Devices with Multi-Factor Authentication (ITSAP.30.030)* [11].
7. **Restrict access rights to only those required to complete tasks.** Access control mechanisms should be implemented. Poll worker access permissions should be consistent with expected tasks. Excessive user rights should be avoided. Embrace secure principles such as least privilege by default and avoid using administrative

accounts for non-administrative tasks. Remove access privileges to poll book systems when users no longer require them. For more information on securing accounts, please refer to *Managing and Controlling Administrative Privileges (ITSAP.10.094)* [12]. Inactivity lock-out screens and account lock-out controls should be considered for implementation.

8. **Disable data communication interfaces or services not in-use.** Communication interfaces on poll book devices, such as network interfaces, USB, and Bluetooth, which are not being used for data transfer should be disabled. Implement system hardening controls to ensure system services not used are locked down. Harden poll book devices and network communication devices by disabling insecure services and weak protocols such as Telnet and SSL version 3.0. Adopt procedures to ensure electronic poll book system components are deployed using secure configuration settings and standardized processes. Implement configuration change controls to restrict or prevent unapproved system changes.

9. **Setup poll book systems as single purpose systems.** Where possible, it is recommended that electronic poll books be setup as a single purpose system to reduce the probable attack surface. Additional system functions such as web browsing, email services and others should be prevented on the devices. Implement security controls to lock down the poll book devices to ensure only poll book or approved tasks can be carried out on the device. Consider implementing supporting control mechanisms to trigger alarms if the poll book deviates from its expected functionality.

10. **Conduct periodic threat and risk assessment of electronic poll book systems.** The need to regularly ascertain the security of the system is crucial, especially before the deployment for an election. Conduct a threat and risk assessment to identify and understand risks associated with election technologies being deployed. A threat and risk assessment of the poll book system will help focus efforts to address key risks. Collect threat intelligence to improve situational awareness and keep abreast of current threats. As much as possible, testing and assessments should be conducted as close to production configurations, such as devices enabled with Wi-Fi connectivity, internet access and connectivity with other applications. Testing scenarios for networked or standalone systems should also reflect the production deployment of such systems.

11. **Ensure business contingency plans include system backups, paper and back-up power options.** Ensure poll book devices are fully charged before deployment to polling stations on election day. Devices should be plugged into proper power outlets. Ensure your business continuity and recovery plans offer power backup contingencies in case of power outages. If devices are expected to run in power-saving mode, ensure applications and deployment are fully tested as part of contingency exercises. Implement a system backup solution to store and recover system data. Ensure data backups are stored offline and disconnected from the organization's network/devices/systems to prevent ransomware and other malware spreading to them. Test your backups as part of your contingency planning activities. The electronic poll book may be rendered inaccessible or unusable during the election-event, so it is necessary to include a paper-based backup system in your incident recovery procedure. Polling staff should be adequately trained on how to activate the use of paper-based poll books, especially during an election event. While running the poll book system in an offline mode may be considered as a service recovery option (i.e., for online systems), paper backups should always be included in all contingency plans.

12. **Maintain strict poll book device inventory controls and keep chain of custody records.** It is important to ensure the movement and location of poll book devices are managed properly. Proper procedures should be implemented

to physically track and safeguard poll book devices. Procedures including physical storage controls, written acknowledgements, and supporting processes should be implemented. Poll book devices with data (encrypted or non-encrypted) should not be carried across international borders as different legislations may apply on its content. Staff members and poll workers should be adequately trained on how to adhere with chain of custody procedures. Remote device wiping capabilities should be available in a case of a device theft.

13. **Implement protections and defences against malicious code.** An electronic poll book connected to the internet increases the risk of malicious code or malware. Anti-malware and anti-virus systems should be installed to detect and neutralize malicious software on the device. To prevent the execution of malicious code, consider system hardening controls such as implementing application execution restrictions, blocking the execution of unauthorized scripts, and locking down administrative accounts from access to the internet. Software updates should be installed promptly, and deprecated software components removed.

14. **Maintain a secure baseline configuration.** To ensure consistency and legislative compliance, your organization should develop and document a set of mandatory security requirements for the building, deployment, and operation of electronic poll books. In some cases, there may be a need to develop an enhanced set of requirements to address specific threat scenarios or business needs for specific use cases. These baselines should be regularly updated as necessary, especially when vulnerabilities impacting any of its core components are identified. Test and re-certify baselines when modified or new updates applied.

15. **Implement secure device sanitization procedures for decommissioned poll books.** As part of the disposal or decommissioning process, electronic media on poll book devices should be properly sanitized. Data sanitization procedures appropriate for the electronic media format should be selected. For example, degaussing may be appropriate for magnetic media drives but not suitable for media storage using solid state drives. It is important to tailor your decommission processes to the specific components involved. For more, please refer to the Cyber Centre’s publication on *Sanitization and Disposal of Electronic Devices (ITSAP.40.006)* [13].

16. **Continuously authenticate and validate poll book devices.** Monitor device health and system activity continuously, and trigger required actions when status changes. Implement security policies to identify risks on an ongoing basis. Device firmware, boot process, and operating system changes are some important parameters to track to ascertain compliance and secure configuration state. Results from an anti-virus system scan and other behaviour heuristic checks are additional parameters that can equally be tracked. Ensure poll book devices meet expected secure health status before being granted access to the central elections management network.

17. **Activate application isolation and sandboxing controls.** To safeguard the poll book application and restrict interactions with its data and resources, application isolation and sandboxing mechanisms can be implemented. Application isolation controls will restrict unauthorized operations on the poll book application and its data. Most modern operating systems support running applications in containerized or sandbox environments. Additionally, running third-party software applications within a sandbox environment on the poll book device will help restrict its impact to other parts of the poll book system should it be compromised. Techniques such as the use of digital code signatures and runtime application control policies are additional measures to consider to safeguard the system’s integrity and prevent untrusted code from running.

18. **Update software promptly and remove obsolete applications.** Obsolete or unmaintained applications can expose poll book systems to several vulnerabilities. Ensure updates addressing vulnerabilities are tracked and software patches tested and applied in a timely manner. For more, please refer to *How Updates Secure Your Device (ITSAP.10.096)*. [14] Software updates to poll book devices with no direct network connection, as well as software and hardware linked to poll systems, should be scheduled. Ample time should be provided to fully install all required updates before devices are deployed for an election.

19. **Enable system activity audit logging and monitoring.** Application system-level logging and network activity logs should be enabled. Where possible, the audit logging and monitoring strategy should consider real-time collection of logs to ensure the integrity of the logs is preserved.

20. **Implement policies and procedures for managing privacy breaches.** Implement policies and procedures to protect personal information on electronic poll book devices. Setup procedures for investigating, responding to, and reporting on privacy breach incidents. Ensure you have consent to collect, use and disclose user information. Inform affected users of breaches that may impact their personal information.

# 4 Conclusion

Electronic poll books can be immensely useful for managing and enhancing election day activities, but if not deployed in a secure manner, they may introduce additional risks to the election process. They present great opportunities for improving the efficient delivery of voter check-in processes, among many other benefits. Due to the potential to hold vast amounts of sensitive voter information and data, electronic poll books will represent attractive targets for threat actors. Security controls implemented should be tailored to the unique needs of each election management body.

Security solutions chosen should be geared towards maintaining the confidentiality, integrity, and availability objective of the election process. Best practices and modern technologies should be at the core of designing, building, and operating these systems. Each jurisdiction should assess its deployment scenarios and implement appropriate controls to safeguard its system. Importantly, poll books represent just one component of the electronic voting architecture. The security of its deployment depends in part, on securely integrating with the rest of the digital election eco-system.

# 5 Supporting Content

## 5.1 List of Abbreviations

| Term | Definition |
|---|---|
| CSE | Communications Security Establishment |
| GC | Government of Canada |
| IT | Information Technology |
| ITS | Information Technology Security |

## 5.2 Glossary

| Term | Definition |
|---|---|
| Elector | A person who is a Canadian citizen at least 18 years old, and therefore eligible to vote. |
| Poll book | A list of approved electors for a particular polling area. |
| Privacy breach | A privacy breach is when personal information is inappropriately collected, accessed, used, retained, disclosed, or disposed, and where there is an assessed impact on the individual's privacy. |
| Sensitive information | Information that if lost, compromised, or disclosed, could result in harm, embarrassment, or inconvenience to the individual or an entity. |
| Threat and risk assessment | A process of identifying system assets and how these assets can be compromised, assessing the level of risk that threats pose to assets, and recommending security measures to mitigate threats. |
| Tokenization | Tokenization relies on a process in which sensitive data elements are substituted with non-sensitive equivalents, referred to as tokens, which have no extrinsic or exploitable meaning or value. |
| Virtual Private Networks (VPN) | A private communications network usually used within a company, or by several different companies or organisations to communicate over a wider network. VPN communications are typically encrypted or encoded to protect the traffic from other users on the public network carrying the VPN. |
| Virtual routing and forwarding (VRF) | Virtual routing and forwarding (VRF) is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. |

## 5.3 References

| Number | Reference |
|---|---|
| 1 | Center for Internet Security. *A Handbook for Elections Infrastructure Security*. February 2018. |
| 2 | Canadian Centre for Cyber Security. *Preparing Your Organization for The Quantum Threat to Cryptography (ITSAP.00.017)*. February 2021. |
| 3 | Canadian Centre for Cyber Security. *Addressing the Quantum Computing Threat to Cryptography (ITSE.00.017). May 2020.* |
| 4 | Canadian Centre for Cyber Security. *Supply Chain Threats and Commercial Espionage*. December 2018. |
| 5 | Canadian Centre for Cyber Security. *Cryptographic Module Validation Program (CMVP)*. |
| 6 | Canadian Centre for Cyber Security. *Guidance on Cloud Service Cryptography (ITSP.50.106)*. May 2020. |
| 7 | Canadian Centre for Cyber Security. *Using Tokenization for Cloud-Based Services (ITSP.50.108)*. October 2021. |
| 8 | Canadian Centre for Cyber Security. *Virtual Private Networks (ITSAP.80.101)*. October 2019. |
| 9 | Canadian Centre for Cyber Security. *Biometrics (ITSAP.00.019)*. February 2020. |
| 10 | Canadian Centre for Cyber Security. *Best Practices for Passphrases and Passwords (ITSAP.30.032)*. September 2019. |
| 11 | Canadian Centre for Cyber Security. *Secure Your Accounts and Devices With Multi-Factor Authentication (ITSAP.30.030)*. June 2020. |
| 12 | Canadian Centre for Cyber Security. *Managing and Controlling Administrative Privileges (ITSAP.10.094)*. July 2020. |
| 13 | Canadian Centre for Cyber Security. *Sanitization and Disposal of Electronic Devices (ITSAP.40.006)*. October 2020. |
| 14 | Canadian Centre for Cyber Security. *How Updates Secure Your Device (ITSAP.10.096)*. March 2021. |