Communications Security Establishment

Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Cyber Security Playbook for Elections Authorities

MANAGEMENT

FOREWORD

ITSM.10.021 Cyber Security Playbook for Elections Authorities is an UNCLASSIFIED publication that is issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre).

EFFECTIVE DATE

This publication takes effect on August 26, 2020.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	August 26, 2020

OVERVIEW

This cyber security playbook guides elections authorities on anticipating, mitigating, and responding to threats that are specific to Canada’s democratic processes. This playbook introduces baseline cyber security measures and best practices that you can implement to improve your organization’s security profile. This playbook also provides a set of standards to reference as elections authorities continue to improve current systems and implement new ones.

The guidance in this document is based on information gathered from various sources and is only intended to provide a set of recommendations that you can implement in addition to your organizational policies and practices.

This document does not provide exhaustive guidance on the measures you should take to protect your organization against cyber threats. You should develop your own playbook, basing it on the security considerations introduced here and your organization’s business needs and security requirements.

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

Elections authorities across Canada need to take measures to protect democratic processes and systems. If electoral data is compromised, democratic institutions may not be able to achieve their mandates, and the public's confidence in election results and democratic processes is jeopardized. In 2016, electoral security changed when it became widely reported that attempts were made to disrupt election processes in the United States (US). Additionally, issues related to ballot integrity, voter registration systems, and measures taken to ensure voter eligibility have been emphasized.

Recently, there have been reports of cyber attacks that coincide with elections around the world. Although threat actors used a variety of techniques, most of the reported attacks were distributed denial of service (DDoS) attacks against government and media websites. In a DDoS attack, a threat actor tries to disrupt a website or system by flooding it with traffic. The attacks seem to have been designed to steal data or alter election results and disrupt the publication of these results.

There have also been reports of threat activity, sometimes facilitated by cyber activity, designed to influence voters or undermine public confidence in election results and the electoral process. These attempts are highlighted by the US government's reports of malicious cyber activity during the 2016 presidential election, as well as recent claims of fraudulent news stories that intend to influence public opinion.

Note that this document does not provide exhaustive guidance on the measures you should take to protect your organization against cyber threats. This playbook is just one of the many pieces of a cyber security program, and it builds on the guidance found in *ITSM.10.021 Cyber Security Guidance for Elections Authorities* [1].

1.1 IT SECURITY RISK MANAGEMENT

ITSG-33 IT Security Risk Management: A Lifecycle Approach [2] describes the roles, responsibilities, and activities that organizations should implement to manage their IT security risks. ITSG-33 [2] addresses the following key principles:

- **Determine asset sensitivity**: Identify your organization's assets, classify and categorize your assets based on their sensitivity levels and applicable legislative and regulatory requirements[1], and create an inventory that lists where your assets reside.
- **Identify major threats**: Determine who or what the greatest threat to data is. Is your organization most concerned about state actors, organized crime, individual hackers, or accidental disclosure? The more sophisticated the attacker, the more sophisticated your data security must be to defend against these attacks.
- **Understand vulnerabilities that impact your technology**: Organizations such as MITRE keep a list of common vulnerabilities and exposures (CVE) in technologies. Review this list, or similar publicly accessible lists, and cross-check known vulnerabilities against your organization's technology.
- **Determine appropriate security controls**: Use the security control catalogue (Annex 3A of ITSG-33 [2]) to determine the security controls that you need to implement, based on asset sensitivity, threats, and vulnerabilities.

[1] Treasury Board of Canada Secretariat (TBS) dictates that GC organizations treat personally identifiable information (PII) at the medium sensitivity level. TBS also recommends that you do not store highly sensitive information (i.e. individual votes) in the cloud.

1.2 PREVENTATIVE SECURITY MEASURES

There is a tendency to think of IT security as a remedy when networks, systems, or information is compromised. However, IT security is not just about responding to an attack; it is the continuous process of preventing, identifying, and responding to threats. To address threats and vulnerabilities, we recommend that you take preventative measures by implementing security controls that address your business and security requirements. For example, to help you develop adequate protections for your information, you can use a selection of controls in each of the following control categories:

- **Administrative security controls**: Procedures implemented to define roles, responsibilities, policies, and administrative functions for managing an environment (e.g. hiring procedures, separation of duties).
- **Technical security controls**: Electronic hardware and software solutions implemented to control access to information and networks (e.g. intrusion detection systems, firewalls, anti-virus software).
- **Physical security controls**: Controls to protect people and your physical environment (e.g. locks, protective barriers).

You can find a catalogue of security controls in Annex 3A of ITSG-33 [2]. You should review this catalogue and determine which controls you need to implement based on your organization's needs and requirements. We recommend that you also review *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* [3], as it lists ten best practices that you can implement to secure your networks and systems.

2 VOTING SYSTEM SECURITY

Protecting voting mechanisms is fundamental to securing democratic processes. Table 1 below describes security measures that are recommended by the Cyber Centre as part of your voting system protection program.

The guidance in this document is based on information gathered from various sources and is only intended to provide a set of recommendations that you can implement in addition to your organizational policies and practices.

Table 1: Security Measures to Protect Voting Systems

Security Measure	Description
Network separation ("air gap")	An air gap is a network security measure in which you physically or conceptually isolate a secure computer network from unsecure networks (e.g. public Internet). Unless necessary, you should not connect a voting system to any other network, including local networks and the Internet. If you must connect voting systems to these networks, you should use isolation devices such as firewalls or cross-domain solutions.
Ballot creation	The ballot creation team should be in a room with limited, multi-factor badge access and surveillance systems. This room should not have network connections.
Ballot printing	You should print ballots in-house, mitigating the risks associated with relying on a vendor for ballot production. The printed ballot should contain a tint and a watermark. If in-house printing is not feasible, you should choose a vendor that is highly trusted.
Chain of custody	You should have strict chain of custody controls for ballots and voting components. A chain of custody documents the movement of ballots and voting components through their collection, safeguarding, and analysis lifecycle. The chain of custody documents each person who handles this information, the date and time of its collection or transfer, and the purpose for any transfers.[2]
Election results assurance	You should implement mechanisms to audit election counts for accuracy, such as two-person integrity.
Voter list maintenance	You should provide voters with clear instructions on how they can change their mailing addresses and contact information. Updating the voter list ensures that you reduce the occurrence of sending voter information to the wrong address.
Electronic poll book	You should use an electronic poll book to review and maintain voter registration information for an election. The poll book does not count votes. This technology can replace or complement paper-based systems. The elections official can look at the entirety of the election data or a single polling station, depending on the official's level of access. You should also encrypt communications between all devices. Devices must continue to operate even when connection is lost. Users should shut down and physically secure all devices when they are not in use. When using mobile devices, consider mobile device management to control security and

[2] Definition comes from the National Institute of Standards and Technology's (NIST) Computer Security Resource Centre Glossary [4].

	enforce policies (e.g. remote wipe, application blacklisting and whitelisting, data encryption enforcement, software updates).
Bulk data storage	You should *review ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information* [5] to determine cryptography best practices for storing information (e.g. data at rest) that you collect from voters.
Managed services and cloud services	You may want to use managed or cloud services, but you should take steps to ensure the provider's services have been assessed and are capable of securing data. You should also ensure that you clearly define the expected service levels regarding roles and responsibilities related to data security. Visit **cyber.gc.ca** to find our publications on managed services and cloud services. For more information on security related to managed services and cloud services, contact our Contact Centre.
Remote advanced polls	You must clearly define requirements for remote advanced polls. For example, for remote advanced polling systems, you must ensure that data always remains encrypted. You should use GC-endorsed cryptography for data in transit. See *ITSP.40.062 Guidance on Securely Configuring Network Protocols* [6] for more information.

3 NETWORK SECURITY

Network security includes the measures you take to protect the usability and integrity of your network and data. Basic network security measures can prevent most attacks from succeeding. When coupled with routine analysis and audits of the electoral processes, network security measures reduce the harm that a cyber attacker can cause.

To avoid introducing further operational risks, we recommend that you carefully plan and test any changes to infrastructure or your service provider offerings. We recommend implementing the security measures described in Table 2 as part of your network security program.

Table 2: Network Security Measures

Security Measure	Description
Firewalls	Install firewalls to monitor the flow of traffic in and out of a network.
Intrusion detection and prevention systems (IDPS)	Use an IDPS to detect and alert you when someone attempts to gain unauthorized access or carries out malicious behaviour.
User login security controls	Enforce a password policy, require the use of passphrases or complex passwords, use multi-factor authentication methods, and apply the principle of least privilege to control access. • For more information on passwords and passphrases, see *ITSAP.30.032 Best Practices for Passphrases and Passwords* [7]. • Multi-factor authentication requires the use of two or more authentication methods (i.e. a password and biometric, a password and token). • The principle of least privilege means that users only have the privileges they require to perform a task or function.
User account management	Disable unused accounts immediately.
Security updates and patch management	Apply security patches and updates by following your patch management process. You should test patches and updates before applying them.
Harden systems	Disable unnecessary services, ports, and protocols.
Enable security features that are available on your organization's systems	Enhanced security options available in your software/systems as provided by the vendor (Depend on system architecture and vendor used).
Legacy workstations	Avoid using outdated or unsupported operating systems and software. Replace legacy systems, if possible, with newer systems.
Continually monitor and assess security	Implement a security information and event management (SIEM) system to ensure the ongoing security of your networks and systems. A SIEM system performs functions like intrusion detection, vulnerability assessment, asset discovery and inventory, behavioural monitoring, and log management.

4 PERSONNEL SECURITY

All individuals involved in your organization and electoral processes (whether these individuals are local government employees, or they are in temporary roles at polling stations, managing postal votes or at the count) are responsible for protecting the security of your networks, systems, and information.

All personnel have a role in maintaining the public's confidence in the election process. We recommend the security measures, described in Table 3, as part of your personnel security program.

The guidance in this document is based on information gathered from various sources and is only intended to provide a set of recommendations that you can implement in addition to your organizational policies and practices.

Table 3: Personnel Security Measures

Security Measure	Description
Secure employee hiring	Perform background checks on potential hires. You may want to review the TBS *Standard on Security Screening* [8] for more information.
Define and manage roles and responsibilities	Implement policies that clearly define roles and responsibilities.
Assign access controls according to trust	Apply the principles of least privilege and separation of duties to ensure that personnel only have access to the systems and information that they require to perform job functions.
Physical security accountability	Hold personnel accountable for enforcing physical security practices. Document expected behaviours and consequences for non-compliance in your policies.
Mandatory security training	Provide mandatory training on cyber security and election security to all personnel, including volunteers. Your training activities should address phishing, social engineering, ransomware attacks, malware, password guidelines, physical security procedures, privacy awareness, mobile devices, and social media use.

5 INCIDENT RESPONSE

Even when you implement risk management activities, incidents can still occur, jeopardizing the security of electoral processes and sensitive data. These incidents may be malicious or accidental, but your ability to effectively respond to these incidents impacts the level of damage that they cause.

Your organization needs to establish an incident response strategy that follows the life cycle below:

- **Plan**: Establish an incident response process and a contingency strategy to address considerations, for example:
  - Mechanisms and tools to identify, contain, eradicate, recover, and follow up from an incident;
  - Roles and responsibilities of employees, managements, and the incident response team;
  - Reporting and communication plans; and
  - Disaster recovery and business continuity processes.
- **Identify**: Identify possible and most likely incidents and determine how your organization can detect these issues as they occur.
- **Contain**: Determine measures that you will take to minimize loss (e.g. theft of information and service disruption).
- **Eradicate**: Identify measures that you will take to remove the threat from your infrastructure.
- **Recover**: Identify the steps that you will take to restore computing services quickly and securely. Ensure that you are backing up systems and information so that you can revert affected systems to a known-good state. Test your recovery plan.
- **Follow-up**: Have a communication plan, assess responses to past incidents, and document the “lessons learned” or follow-up activities.

Throughout the incident management life cycle, consider the following:

- **Communicate**: Notify all appropriate internal and external parties, maintain situational awareness, and circulate the emergency contact numbers as a part of your immediate response to the incident.
- **Analyze**: Examine available data to support your decisions for handling the incident.
- **Document**: Record and timestamp all the evidence you discover, as well as the information and actions that you take throughout the incident response plan (from identification to follow-up activities).

6 PARTNERSHIPS AND INTELLIGENCE SHARING

6.1 INFORMATION SHARING

We engage with elections authoritative bodies at federal, provincial, and territorial levels. We cannot share the information that results from our individual consultations without the express consent of our clients. However, these consultations shape our advice and guidance. We reflect the knowledge gained from these experiences in our guidance materials.

We recommend that you schedule lateral consultations with other elections authorities (e.g. provincial-territorial consultations). Many of the cyber security challenges that you face are common across elections authorities, and you can gain insight from the lessons learned by other elections authorities. You can use the lessons learned by your counterparts to strengthen your organization’s security posture.

6.2 RCMP AND LOCAL LAW ENFORCEMENT

If you suspect criminal activity or issues such as potential interference, you should contact the RCMP and your local law enforcement agency. These organizations can also provide physical security resources on election day.

6.3 CANADIAN ANTI-FRAUD CENTRE

If your organization is the target of fraud, such as a threat actor posing as your organization, contact your local police and file a report online through the Canadian Anti-Fraud Centre’s Fraud Reporting System.

7 CONTACT US

For more information on cyber security or to report a cyber security incident, email or phone our Contact Centre. You can also visit our website to find publications on various cyber security topics.

Contact Centre
www.cyber.gc.ca
contact@cyber.gc.ca
613-991-8700 or 1-833-CYBER-88

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CSE	Communications Security Establishment
GC	Government of Canada
IDPS	Intrusion detection and prevention system
IT	Information technology
RCMP	Royal Canadian Mounted Police
SIEM	Security information and event management
TBS	Treasury Board of Canada Secretariat
US	United States

8.2 GLOSSARY

Term	Definition
Air gap	An air gap is a network security measure in which you physically or conceptually isolate a secure computer network from unsecure networks (e.g. public Internet).
Authentication	The process of confirming the identify of a user or another entity (e.g. application) as valid and genuine.
Availability	The ability for the right people to access the right information or systems when needed. Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Chain of custody	A chain of custody is the process of documenting the movement of evidence through its collection, safeguarding, and analysis lifecycle.
Cloud services	Services, which are provided by a third company, that are made available to users on demand via the Internet, as opposed to services that are provided from a client's on-premises IT environment.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Cyber attack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
Integrity	The ability to protect information from being modified or deleted unintentionally or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
Managed services	Services provided by a third party to remotely manage IT infrastructure and user end systems on behalf of a client.

Term	Definition
Phishing	An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand, often for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.
Ransomware	A type of malware that denies a user's access to a system or data until a sum of money is paid.
Social engineering	An attack in which a threat actor tries to manipulate an individual into performing actions or divulging sensitive information.

8.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. *ITSM.10.020 Cyber Security Guidance for Elections Authorities.* May 2020.
2	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
3	Canadian Centre for Cyber Security. *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information*. October 2018.
4	National Institute for Standards and Technology. "Glossary". *Computer Security Resource Centre.*
5	Canadian Centre for Cyber Security. *ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information*. August 2016.
6	Canadian Centre for Cyber Security. *ITSP.40.062 Guidance on Securely Configuring Network Protocols*. August 2016.
7	Canadian Centre for Cyber Security. *ITSAP.30.032 Best Practices for Passphrases and Passwords*. September 2019.
8	Treasury Board of Canada Secretariat. *Standard on Security Screening*. October 2014.