Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Cyber Security Guidance for Elections Authorities

MANAGEMENT

FOREWORD

ITSM.10.020 Cyber Security Guidance for Elections Authorities is an UNCLASSIFIED publication issued under the authority of the Head of the Canadian Centre for Cyber Security (the 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 document is intended for elections authorities. It introduces common threats to Canada's electoral processes and provides guidance on protecting the systems and the people involved in these processes. 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.

Note that this document does not provide exhaustive guidance on the measures you should take to protect your organization against cyber threats. Your organization is responsible for defining its business and security requirements and ensuring that the appropriate measures are taken to protect the confidentiality, integrity, and availability of your networks, systems, and information.

The Cyber Centre was established under the Communications Security Establishment on October 1, 2018. The Cyber Centre is the national authority on cyber security, and its creation united operational security experts from across the Government of Canada (GC). In line with the *National Cyber Security Strategy* [1][1], the launch of the Cyber Centre represents Canada's unified approach to cyber security. The Cyber Centre provides advice and guidance to the GC and Canadian businesses to ensure the country's security, stability, and prosperity.

[1] Numbers in square brackets refer to works referenced in the Supporting Content section of this document.

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

The cyber threat activities taken against the democratic institutions in the United States (US) and Europe have raised concerns about similar threats that face Canada. Additionally, the recent cyber threat activity has emphasized issues related to ballot integrity, voter registration systems, and measures taken to ensure voter eligibility.

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 could be jeopardized.

1.1 RISK LANDSCAPE

Recently, there have been reports of cyber attacks that coincide with elections around the world. Although threat actors used a variety of techniques in these attacks, 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, 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 the public's 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.

It is difficult to know who is behind a cyber attack. However, it is likely that some of the attacks on other countries were state-sponsored attacks. Hackers (who may be working for hire), hacktivists, and cyber criminals may also be responsible.

1.2 EXAMPLES OF ELECTORAL INTERFERENCE

Based on the recent experiences of other countries, organizations that are involved in Canadian election processes should prepare for possible attacks and disruptions. In Table 1, we summarize recent case studies of disruptions that impacted other countries:

Table 1: Recent Examples of Electoral Interference

Year	Summary of Events
2015	Coinciding with the start of local elections and a referendum on e-voting, the websites of a European Union country's election commission, government, and civic registration service were the targets of denial-of-service (DoS) attacks.
2016	In the last US presidential election, both major political parties were subjected to cyberespionage attempts by Russia. Russian operatives used cyber capabilities to gain access to the emails of key political staff working on the Democratic Party campaign. The emails were subsequently leaked to embarrass the Democratic Party candidate.

	In 2018, authorities charged individuals based in Russia with interfering in the 2016 US presidential election, representing a shift from identifying and defending against malicious activity, to confronting and prosecuting cyber threats to the democratic process in the US.
2017	According to media reports, French intelligence believes that social botnets were used to influence the presidential election in France. Certain social media accounts, the same ones that were active during the previous year's US election, were promoting false and defamatory information against a leading candidate. In the final days of the election, one party was also victimized by the unauthorized release of thousands of campaign-related emails.
2019	Leading up to the March 2019 Ukrainian presidential elections, the Ukrainian Cyber Police claimed that attackers sent phishing emails to government officials and state employees (including those involved in the electoral process). The emails, which were sent as attempts to steal passwords and personal information, included malware-infected greetings cards. Claims were made that cyber actors bought personal details of election officials on the dark web.

1.3 THREATS TO ELECTORAL PROCESSES AND SYSTEMS

Canadian elections authorities, with the help of our international counterparts, need to continue to focus on protecting democratic processes by addressing emerging threats, such as the examples listed in Table 2. The table below also includes measures that can be taken to address the threats. For additional information, refer to our report, *2019 Update: Threats to Canada's Democratic Process* [2].

Table 2: Examples of Threats to Electoral Processes and Systems

Threat	Measures to Mitigate
Electronic manipulation of votes.	Elections Canada maintains manual processes to vote and count ballots.
Data interference through attacks on cloud services.	Choose a cloud service provider that implements security controls. Contact us to go through the cloud service provider IT security assessment process so that you can determine whether the service provider's security controls and processes align with your business and security needs.
DDoS attacks against electoral, government, or media websites to make them unavailable during key moments of an electoral campaign, such as voter registration deadlines or election day.	Build redundancies progressively into infrastructure. Continue to refer to the expanding knowledge base to configure your network hardware against attacks.
Phishing or social engineering attacks to obtain sensitive information.	Mandate training and exercises for all personnel so that they know how to identify these attacks and protect themselves and your organization.

2 PROTECTING SYSTEMS

Basic cyber security measures can prevent threat actors from succeeding in their attacks. When your organization couples these measures with routine analyses and audits of electoral processes, you can reduce the ability for a threat actor to cause widespread harm.

We recommend that you take preventative security measures by implementing various types of security controls that address your needs and requirements, such as:

- **Administrative security controls**: Procedures implemented to define roles, responsibilities, policies, and administrative functions needed to manage 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 the physical environment (e.g. locks, protective barriers).

For more information, see Annex 3a of *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [3], which includes a catalogue of security controls, and our *Baseline Cyber Security Controls for Small and Medium Organizations V1.1* [4].

To avoid introducing further operational risks, we recommend that you carefully plan and test any changes to infrastructure or your service provider offerings. Specifically, you should address the points listed in Table 3 below.

For more information on how you can protect your systems, refer to the *ITSM.10.021 Cybersecurity Playbook for Elections Authorities* [5]. We also recommend that you review *ITSM.10.189 Top 10 Security Actions to Protect Internet-Connected Networks and Information* [6].

Table 3: Basic Cyber Security Measures to Protect Systems

Security Measure	Examples
Privacy	Handle personally identifiable information, and the systems that hold bulk data sets containing PII (e.g. electoral management systems [EMS]), according to the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act.*
Regulatory	Store sensitive data according to legislative and regulatory requirements. For example, Treasury Board of Canada Secretariat's (TBS) *Direction for Electronic Data Residency: IT Policy Implementation Notice* [7] requires all GC organizations to store sensitive data, such as PII, in data centres located only within the geographical boundaries of Canada to ensure this information is subject to Canadian privacy laws.
Back-ups	Back up an EMS (particularly the electoral roll) regularly. You should store back-ups offline, in a separate secure location, and test your procedures for backing up and restoring systems and information. You should have the contact information for key suppliers (e.g. any EMS software and service providers) readily available. Remember that during an incident, the usual mechanisms for finding contact information may not be available.
Updates and security patches	Update and patch your infrastructure's software and hardware.
End user devices	Ensure personnel use corporately managed end user devices for functions such as those used to manage the electoral roll.
Administrative accounts	Monitor and restrict administrator account activity based on the principle of least privilege (i.e. only those who require administrative access to perform their tasks should have administrator access). Depending on the level of access your operational staff have to electoral systems, they may be able to perform significant privileged actions on EMS data. If so, you may need to consider these individuals as system administrators. Regularly review the level of access individuals have and ensure it is appropriate for their roles.

3 PROTECTING PEOPLE

Threat actors may try to exploit your staff and any individuals who are involved in the elections process, especially during periods of heightened pressure (e.g. on election day). Threat actors may try to use various attack methods, such as phishing and social engineering, to gain access to sensitive information. People who are in executive or official positions, or people who directly support these positions, are at a higher risk of being a target of these attacks because their information is publicly available. Individuals may also unintentionally give away information that threat actors can use to manipulate or compromise electoral processes. You should ensure all staff, especially election officials, know that they are required to be cautious when providing details on their election duties.

3.1 CYBER SECURITY TRAINING

As part of your risk management processes, you should provide mandatory training on cyber security to those who are involved in electoral processes. Training activities should include identifying phishing and social engineering attacks. You should also ensure that you have processes to prevent people from falling victim to these attacks.

> For example, an employee may receive an urgent email that appears to come from a software vendor. This email may be advising the recipient of an urgent software update. While the email may be legitimate, you should clearly indicate the process for validating the email. The recipient should check other sources to confirm that what is stated in the email is valid (e.g. check the vendor's support website to see if there is a notification about the update). You should ensure that your staff know how to get support if they receive suspicious or unusual communications (e.g. emails, texts, or phone calls).

Your training activities should also cover topics such as ransomware attacks, malware, password guidelines, physical security procedures, privacy awareness, and secure use of mobile devices and social media. Note that this list of topics is not exhaustive. For more information on providing training, see *ITSM.10.093 Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training* [8].

For information related to campaign teams, see our *Cyber Security Guide for Campaign Teams* [9].

3.2 INSIDER THREATS

Individuals involved in Canadian electoral processes are required to show integrity and discretion. However, you should be aware of the risks posed by an insider threat. An insider threat is any individual who has knowledge of or access to your organization's infrastructure and information and who uses, knowingly or inadvertently, the infrastructure or information to cause harm.

An individual may intend to exploit their access for their own, unauthorized purposes. An insider threat may seek to manipulate or compromise electoral information or processes for financial gain, ideological reasons, or recognition. However, it is also possible for an employee to cause harm inadvertently, such as in the following examples:

- Misplacing mobile devices or removable media;
- Granting access to sensitive information to employees who are not authorized to access it; and
- Mishandling sensitive information (e.g. leaving it out in the open, forgetting to apply appropriate permissions).

You can prevent insider threats from occurring by performing background checks on potential hires and implementing access controls (e.g. principle of least privilege, separation of duties) to protect sensitive information. Refer to *ITSAP.10.003 How to Protect Your Organization from Insider Threats* [10] for more information.

3.3 CYBER SECURITY POLICIES

You should have policies that address the expected behaviour, the roles, and the responsibilities of all employees and personnel. All individuals (whether local government employees or those in temporary roles at polling stations, managing postal votes or at the count) involved in electoral and democratic processes have a vital part to play in ensuring the confidentiality, integrity, and availability of associated systems and information. By establishing policies, you ensure that everyone is held accountable for adhering to your organization's security practices.

You should determine how often you need to review your policies (e.g. annually) so that you can ensure updates are made when processes and procedures are changed or added.

4 CONTACT US

For more information on cyber security, 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

5 SUPPORTING CONTENT

5.1 LIST OF ABBREVIATIONS

Term	Definition
CSE	Communications Security Establishment
DoS	Denial of service
DDoS	Distributed denial of service
EMS	Electoral management system
GC	Government of Canada
IT	Information Technology
PII	Personally identifiable information

5.2 GLOSSARY

Term	Definition
Administrative security controls	Procedures implemented to define roles, responsibilities, policies, and administrative functions needed to manage an environment (e.g. hiring procedures, separation of duties).
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.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Denial of service attack	Any activity that makes a service unavailable for use by legitimate users or that delays system operations and functions.
Electoral roll	A list of persons who are eligible and registered to vote.
Insider threat	Any individual who has knowledge of or access to your organization's infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm.
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.
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, 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.

Term	Definition
Physical security controls	Controls to protect people and the physical environment (e.g. locks, protective barriers).
Social engineering	An attack in which a threat actor tries to manipulate an individual into performing actions or divulging sensitive information.
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).

5.3 REFERENCES

Number	Reference
1	Public Safety Canada. *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. 2018.
2	Canadian Centre for Cyber Security. *2019 Update: Threats to Canada's Democratic Process*.
3	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach.* November 2012.
4	Canadian Centre for Cyber Security. *Baseline Cyber Security Controls for Small and Medium Organizations V1.1*. June 2019.
5	Canadian Centre for Cyber Security. *ITSM.10.021 Cybersecurity Playbook for Elections Authorities*. May 2020.
6	Canadian Centre for Cyber Security. *ITSM.10.189 Top 10 Security Actions to Protect Internet-Connected Networks and Information.* October 2018.
7	Treasury Board of Canada Secretariat. *Direction for Electronic Data Residency: IT Policy Implementation Notice.* November 2017.
8	Canadian Centre for Cyber Security. *ITSM.10.093 Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training.* January 2020.
9	Canadian Centre for Cyber Security. *Cyber Security Guide for Campaign Teams.*
10	Canadian Centre for Cyber Security. *ITSAP.10.003 How to Protect Your Organization from Insider Threats.* February 2020.