For Public Release

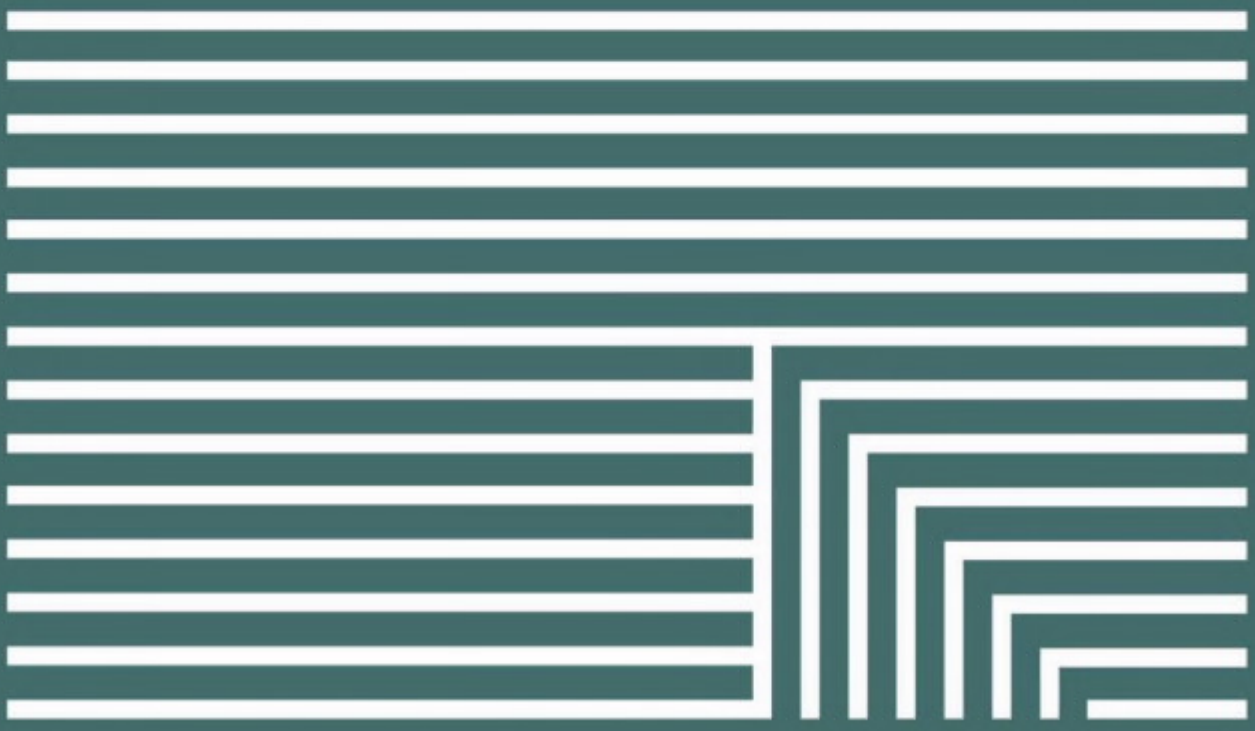
Protecting Democracy Unit | Unité pour la protection de la démocratie

Directors' Coordinating Group on Protecting Democracy

Tuesday, May 16, 2023

3:00pm – 4:00pm

80, Wellington Street, Ottawa, ON



Government of Canada
Privy Council Office

Gouvernement du Canada
Bureau du Conseil privé

Canada

Protecting Democracy Unit
Unité pour la protection de la démocratie

Table of Contents

Protecting Democracy Unit
—
Unité pour la protection de la démocratie

Agenda - Directors' Coordinating Group on Protecting Democracy

AGENDA ITEMS	DURATION
1. Introduction - Protecting Democracy Unit (PDU)	5 min.
2. Measures to protect Canada's democracy - Way forward on Plan to Protect Canada's Democracy (PDU) - Roundtable (All)	25 min.
3. Overview of Report on Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions - PDU and Foreign Interference Task Force	10 min.
4. Governance and next steps - All	10 min.

Protecting Democracy Unit

Protecting Democracy Unit (PDU)

- PDU was established through Budget 2022 to coordinate, develop, and implement government-wide measures designed to combat disinformation and protect our democracy.

Coordination
Build an integrated interdepartmental response

Research & Policy
Further government's understanding and use of evidence

Engagement
Learn from others, develop partnerships, and engage civil society

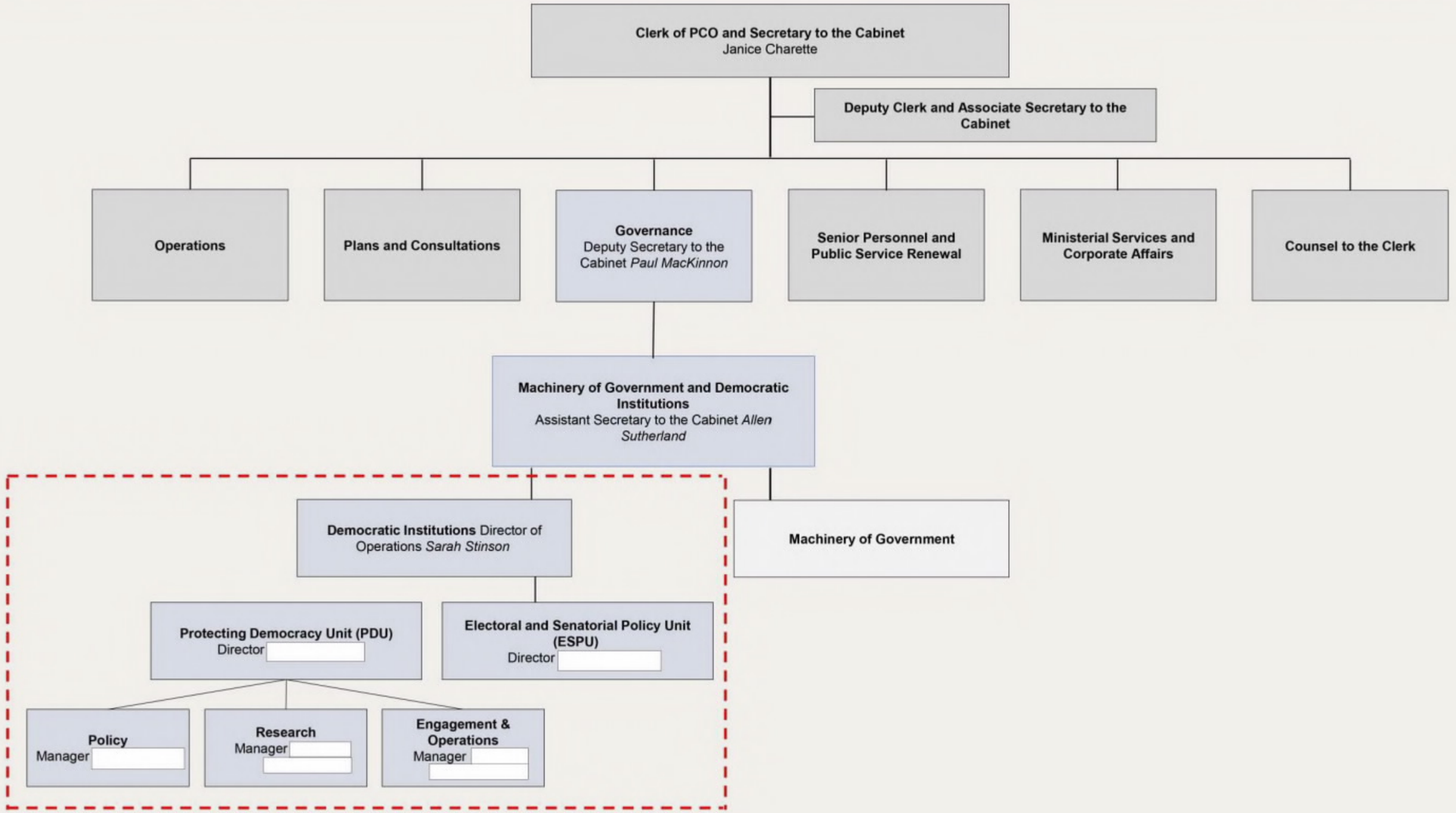
Communications: Monitoring & Response
Develop a framework for communications interventions

Areas of work include:

- Increasing understanding of mis/disinformation in Canada
- Creation of the Canadian Digital Media Research Network (funded through PCH's Digital Citizen Initiative)
- Enhancing the Plan to Protect Canada's Democracy
- Interdepartmental coordination and governance
- Support government efforts to prevent and counter foreign interference
- Engagement with the Organisation for Economic Co-operation and Development, provinces and territories, and other organizations within civil society and the public sector.
- Foster awareness and understanding of the threats to democracy and the drivers that erode trust in government, including the MIDI phenomenon
- Develop and/or disseminate tools to help identify and better combat threats to democracy

Protecting Democracy Unit

Where PDU Fits Within PCO



MEASURES TO COMBAT FOREIGN INTERFERENCE IN ELECTIONS

2016-2017

Establishment of Rapid Response Mechanism (RRM)

- G7 Summit, Charlevoix

Elections Modernization Act Royal Assent

- Political financing tightened
- Increased ad transparency
- New powers for the Commissioner of Canada Elections
- New offences, including the unauthorized use of computers

Amendments to the CEA

- *An Act to amend the Canada Elections Act (political financing)* - Enact an advertising and reporting regime for fundraising events attended by Ministers, party leaders or leadership contestant

2018

Communications Security Establishment (CSE) Initiatives

Commissioning of Threat Report

- Cyber Threats to Canada's Democratic Process

Services offered to Political Parties:

- Provided briefing to registered political parties on their public threat report

Provided Services to Elections Canada:

- Offered briefings on threat reports

2019

Protecting Democracy Plan

Four Pillars:

- **Enhancing Citizen Preparedness**
  - Critical Election Incident Public Protocol (CEIPP)
  - Digital Citizen Initiative
- **Improving Organizational Readiness**
  - Classified threat briefings and cybersecurity briefings to political parties.
- **Combatting Foreign Interference**
  - SITE Task Force, G7 RRM
- **Expecting Social Media Platforms to Act**
  - Canada Declaration on Electoral Integrity Online

Budget 2019

- **Canadian Heritage:**
  - $19.4 million over 4 years
- **Communications Security Establishment:**
  - $4.2 millioan over 3 years
- **Global Affairs Canada**
  - $2.1 million over 3 years
- **Canadian Security Intelligence Services**
  - $23 million over 5 years

Update to 2017 CSE Report

2019 update: Cyber Threats to Canada's Democratic Process:

- Details overview of threat landscape

2020

Support for Paris Call for Trust and Security in Cyberspace (Paris Call)

- Nine principles focused on enhancing cyber hygiene, and protecting Canada against foreign interference

Paris Call Workshops

Six Workshops:

- Focused on Improving multi-stakeholder information sharing, defining foreign interference, COVID-19 contingencies, mitigation and response, countering interference in election infrastructure, and empowering citizens

Critical Elections Incident Public Protocol (CEIPP)

- Release of CEIPP evaluation by former senior civil servant, James Judd
- Found overall that the CEIPP was implemented successfully

2021

Updating Protecting Democracy Plan

- **New Pillar: Building a Healthy Information Ecosystem Online**

Published Reports

- **CSIS Report**
  - Foreign Interference Threats to Canada's Democratic Process
- **CSIS Report**
  - Foreign Interference and You
- **CSE Report**
  - Cyber Threats to Canada's Democratic Process: July 2021 Update
- **Paris Call Community for Countering Election Interference Report**
  - Compendium on Countering Election Interference

Global Affairs Canada RRM

- G7 Foreign and Development Ministers Meeting in London, commitment to produce annual thematic reports
- 2021 G7 RRM Annual Report Release

Budget 2022

- Provided $2 million annually for the Privy Council Office to coordinate, develop, and implement government wide measures designed to combat disinformation and protect our democracy
- Provided $13.4 million over 5 years and $2.8 million ongoing to renew and expand the RRM

Fall Economic Statement

- Renewal of the Digital Citizen Initiative

2022

Critical Elections Incident Public Protocol (CEIPP)

- Release of CEIPP evaluation by former senior civil servant, Morris Rosenberg
- Found that the CEIPP worked well and should be maintained with some suggested improvements

Ongoing Projects

- Research to paint composite picture of mis- and disinformation in Canada
- Continued engagement with relevant industry stakeholders, provinces and territories, academia, and civil society

2023

Ongoing measures to protect democracy and combat MIDI

A four-pillar strategy - significant focus on election and writ period

Enhancing Citizen Resilience

- Critical Election Incident Public Protocol (Panel of 5)
- Public reports on threats to Canada's democratic process (CSE, CSIS)
- Digital Citizen Initiative (digital, news and civic literacy funding for civil society)

Improving Organizational Readiness

- Classified threat briefings to political parties
- Cybersecurity guidance to political parties
- Cybersecurity hotline for political parties during election campaign
- Engagement with Elections Canada

Combatting Foreign Interference

- Security and Intelligence Threats to Elections Task Force (CSE, CSIS, GAC, RCMP)
- Rapid Response Mechanism

Building a Healthy Information Ecosystem

- Canada Declaration on Electoral Integrity Online (with Facebook, Google, LinkedIn, Microsoft, TikTok, Twitter, YouTube)

Established in 2019 and renewed in 2021

$48 million over 5 years through Budget 2019

Backgrounder
Measures Taken to Protect Canada's Democracy

- The Plan to Protect Canada's Democracy is a whole-of-government and whole-of-society approach to safeguard Canada's elections and democratic institutions against interference.

- The Plan was initially implemented ahead of the 2019 general election and renewed and updated ahead of the 2021 election, following extensive assessments.

- The Plan includes activities under four pillars:
    - **Enhancing citizen preparedness**: by improving the critical thinking and digital literacy skills of Canadians and establishing the Critical Election Incident Public Protocol to ensure Canadians are informed of serious attempts to interfere with their ability to have a free and fair election
    - **Improving organizational readiness**: by providing classified threat briefings to political parties represented in the House of Commons; offering cybersecurity guidance to political parties; and engaging collaboratively with Elections Canada
    - **Combatting foreign interference**: by leveraging the G7 Rapid Response Mechanism and the Security and Intelligence Threats to Elections (SITE) Task Force
    - **Building a healthy information ecosystem**: by renewing and expanding voluntary commitments from digital and social media platforms to improve transparency, authenticity and integrity on their systems through the Canada Declaration on Electoral Integrity Online

- **Budget 2022** announced key investments in the Plan, including renewal of the Rapid Response Mechanism ($13.4 million over five years and $2.8 million ongoing) and $10 million over five years (with $2 million ongoing) in new resources for the Privy Council Office to coordinate, develop, and implement government-wide measures designed to combat disinformation and protect democracy.

The following specific activities have been initiated under each of the four pillars.

1. ***Enhancing Citizen Preparedness***

- Implementing the **Digital Citizen Initiative** to support digital news and civic literacy programming and tools to improve Canadians' resilience against disinformation. (Canadian Heritage).
- Releasing **public reports on threats to Canada's democratic process,** including 2019 and 2021 updates on *Cyber Threats to Canada's Democratic Process* (Communications Security Establishment) and a 2021 report on *Foreign Interference Threats to Canada's Democratic Process* (Canadian Security Intelligence Service).
- Implementing the **Critical Election Incident Public Protocol**, a mechanism for communicating with Canadians during the caretaker period in a clear, transparent, and impartial manner about incidents that threaten the integrity of the election. (Privy Council Office)
- Increasing the reach and focus of **Get Cyber Safe**, the national public awareness campaign created to educate Canadians about cyber security and the simple steps they can take to protect themselves online, to include greater linkages to cyber threats to Canada's democratic processes. (Communications Security Establishment)

2. ***Improving Organizational Readiness***

- Offering **classified threat briefings to key leadership** of political parties represented in the House of Commons to promote situational awareness and help them to strengthen internal security practices and behaviours. (PCO, Communications Security Establishment, Canadian Security Intelligence Service, Royal Canadian Mounted Police)
- Offering additional **cyber security technical advice and guidance** to political parties to enhance security. (Communications Security Establishment)
- Enhanced government-wide coordination, including deepened engagement with Elections Canada, which has leadership for the operational conduct of elections,

to ensure seamless integration with the Government of Canada's national security apparatus.

3. *Combatting Foreign Interference*

- Leveraging **Security and Intelligence Threats to Elections (SITE) Task Force** to improve awareness of foreign threats and support assessment and response, as well as ongoing work by security agencies to prevent covert, clandestine or criminal activities from interfering in the election. (Communications Security Establishment, Canadian Security Intelligence Service, Royal Canadian Mounted Police, and Global Affairs Canada)

- Leveraging the **G7 Rapid Response Mechanism** to strengthen coordination among G7 democracies in responding to threats to democracy, and monitoring malign actors in the social media space. (Global Affairs Canada)

4. *Building a Healthy Information Ecosystem*

- Establishing a common understanding with platforms about their responsibilities in the online democratic space through the Canada Declaration on Electoral Integrity Online, which was adopted in 2019 and updated in 2021, with new commitments and signatories (Facebook, Google, LinkedIn, Microsoft, TikTok, Twitter, YouTube).

Backgrounder
Critical Election Incident Public Protocol

Overview

- The Critical Election Incident Public Protocol (the Protocol) establishes a mechanism for senior public servants, referred to as the Panel, to communicate clearly, transparently, and impartially with Canadians during an election in the event of an incident or series of incidents that threaten the integrity of a federal election.

- First implemented in 2019, the Protocol underwent an independent assessment following the 43rd General Election and was renewed and updated for future elections.

- The threshold for an announcement by the Panel is very high and limited to exceptional circumstances that could impair Canadians' ability to have a free and fair election, whether due to a single incident or an accumulation of incidents. The incidents in question would pose a significant risk of undermining Canadians' democratic rights, or have the potential to undermine the credibility of the election.

- During the 2019 and 2021 general elections, the Panel received regular security briefings. The Panel did not observe any activities that met the threshold for public announcement.

Post-2019 Protocol Assessment by Jim Judd

- The evaluation of the Protocol following the 2019 federal election was conducted by James Judd, a former Canadian public servant and director of CSIS. The classified version of his report was provided to the Prime Minister and the National Security Intelligence Committee of Parliamentarians as per the Cabinet Directive. An unclassified version of the evaluation report was also made available to the public in November 2020.

- The evaluation of the Protocol found that overall, its implementation was successful and recommended that it be put in place for the next general election.

- It was additionally recommended that the institutional composition of the Panel remain the same. This includes the Clerk of the Privy Council; the National Security and Intelligence Advisor to the Prime Minister; the Deputy Minister of Justice and Deputy Attorney General; the Deputy Minister of Public Safety; and the Deputy Minister of Foreign Affairs.

- It was further recommended that the threshold for an announcement remain unchanged. The high threshold helps to avoid the Panel becoming a frequent intervener in any general election.

Changes to the Protocol in 2021

- Cabinet issued an amended Cabinet Directive in May 2021, removing reference to the Protocol's application during a specific general election. As a result, it will be in place for future general elections until revoked or amended by Cabinet.

- Additional key amendments include:
  - Alignment of the Protocol's application period with that of the Caretaker Convention.
  - Explicit provision for the Panel to consult with the Chief Electoral Officer, as appropriate.
  - Provision for the ability of political parties to alert security agencies of incidents that could threaten a free and fair election.
  - Recognition of the Panel's ability to examine domestically-driven interference, as well as to receive information from sources other than security agencies, at its discretion.

Post-2021 Protocol Assessment by Morris Rosenberg

- The 2021 assessment of the CEIPP, conducted by Morris Rosenberg, a former Deputy Minister from 1998 to 2013, was made public on February 28, 2023. It found that the CEIPP worked well and should be maintained with some suggested improvements. The Government of Canada will be reviewing the 16 recommendations carefully and responding in due course.

ANNEX

Cabinet Directive on the Critical Election Incident Public Protocol

1.0 Introduction

The protection and preservation of Canada's democratic institutions and practices is one of the core responsibilities of the federal government.

National security threat and risk assessments, along with the experience of key international allies, underscore that Canada's general elections may be vulnerable to interference in a number of areas. Recognizing this, significant work has been undertaken within the federal government to protect and defend electoral systems and processes. As part of this work, the Government of Canada has established the Critical Election Incident Public Protocol (CEIPP) in order to ensure coherence and consistency in Canada's approach to publicly informing Canadians during the caretaker period about incidents that threaten Canada's ability to have a free and fair election.

2.0 Purpose

The *Cabinet Directive on the Critical Election Incident Public Protocol* sets out the ministers' expectations with respect to the general directions and the principles to guide the process for informing the public of an incident that threatens Canada's ability to have a free and fair election during the period that the Caretaker Convention is in effect.

The Protocol is an application reflective of the Caretaker Convention. The Caretaker Convention puts into practice the principle that the government is expected to exercise restraint in its activities and "restrict itself" in matters of policy, spending and appointments during the election period, except where action is "urgent" and "in the national interest". The Caretaker Convention typically begins on the dissolution of Parliament. It ends when a new government is sworn-in or a result returning an incumbent government is clear.

During the caretaker period, announcements that must proceed are to be made in the name of the department to ensure a distinction between official government business and partisan activity.

3.0 Scope of application

The Critical Election Incident Public Protocol will have a limited mandate. It will only be initiated to respond to incidents that occur during the caretaker period, and that do not fall within Elections Canada's areas of responsibility (i.e., with regard to the administration of the election, as identified in the *Canada Elections Act*). Incidents that occur outside of the caretaker period will be addressed through regular Government of Canada operations.

4.0 Panel

The protocol will be administered by a group of senior civil servants who will, working with the national security agencies within the agencies' existing mandates, be responsible for determining whether the threshold for informing Canadians has been met, either through a single incident or an accumulation of separate incidents.

This Panel will be comprised of:

- the Clerk of the Privy Council;
- the National Security and Intelligence Advisor to the Prime Minister;
- the Deputy Minister of Justice and Deputy Attorney General;
- the Deputy Minister of Public Safety; and
- the Deputy Minister of Foreign Affairs.

5.0 Process

The protocol lays out a process through which Canadians would be notified of an incident that threatens Canada's ability to have a free and fair election, should notification be necessary.

During the caretaker period, the protocol for a public announcement would be:

1. The national security agencies will provide regular briefings to the Panel on emerging national security developments and potential threats to the integrity of the election. The Panel may also receive information and advice from sources other than the security and intelligence agencies.
2. Political parties will be instructed on how to report any interference that they may experience during the election.

3. If the head of a national security agency (i.e., the Communications Security Establishment, the Canadian Security Intelligence Service, the Royal Canadian Mounted Police or Global Affairs Canada, working within their respective mandates) becomes aware of interference in a general election, they will, in consultation with each other, consider all options to effectively address the interference. As part of this process, they will inform the Panel. Barring any overriding national security/public security reasons, the agencies will inform the affected party (e.g., a candidate; a political party; Elections Canada) of the incident directly.
4. The Panel will evaluate incidents to determine if the threshold (as set out in Section 6 below) for informing the public has been met. The Panel will operate on a consensus basis and will draw on expertise from across government, including national security agencies working within their existing mandates. The Panel may consult with the Chief Electoral Officer (CEO) to ensure mandates are being respected should issues of interference arise that are possibly relevant to both the Panel and the CEO.
5. If a public announcement is deemed necessary, the Panel will inform the Prime Minister, the other major party leaders (or designated senior party officials who have received their security clearances sponsored by the Privy Council Office) and Elections Canada that a public announcement will be made. These leaders would all receive the same briefing information.
6. Immediately after having informed the Prime Minister, the other political parties and Elections Canada, the Clerk of the Privy Council, on behalf of the Panel, may either issue a statement or ask the relevant agency head(s) to issue a statement to notify Canadians of the incident(s).

6.0 Threshold for informing the public

A public announcement during the caretaker period would only occur if the Panel determines that an incident or an accumulation of incidents has occurred that threatens Canada's ability to have a free and fair election.

Determining whether the threshold has been met will require considerable judgement. There are different considerations that could be included in making this judgement:

- the degree to which the incident(s) undermine(s) Canadians' ability to have a free and fair election;
- the potential of the incident(s) to undermine the credibility of the election; and
- the degree of confidence officials have in the intelligence or information.

The Panel brings together unique national security, foreign affairs, democratic governance and legal perspectives, including a clear view of the democratic rights enshrined in the *Canadian Charter of Rights and Freedoms*.

A disruptive event or incidents of interference may emanate from domestic and/or foreign actors. Attribution of interference attempts may be challenging or not possible within the timelines permitted by events, given that attempts to unduly influence the election may involve misdirection and disinformation. Further, it is possible that foreign actors could be working in collaboration with, or through, domestic actors. Ultimately, it is the impact of the incident on Canada's ability to have a free and fair election that is at issue in the determination of whether the threshold has been met, and if a public announcement is required. For clarity, Canadians – and democracy – are best served by election campaigns that offer a full range of debate and dissent. The Protocol is not intended to, and will not, be used to respond to that democratic discourse.

7.0 Announcement

The announcement would focus on:

a. notification of the incident;

b. what is known about the incident (as deemed appropriate); and

c. steps Canadians should take to protect themselves (e.g., ensure that they are well informed; cyber hygiene), if relevant.

8.0 Existing authorities

Nothing in this Directive in any way alters or expands the mandates of the national security agencies or any other department or agency. Specifically, nothing in this protocol supersedes the RCMP's independence.

9.0 Assessment

Following each general election, an independent report will be prepared, assessing the implementation of the Critical Election Incident Public Protocol and its effectiveness in addressing threats to the election. This report will be presented to the Prime Minister and to the National Security and Intelligence Committee of

Parliamentarians. A public version will also be developed. These reports are intended to help inform whether adjustments to the protocol should be made.

For Public Release

CRITICAL ELECTION INCIDENT PUBLIC PROTOCOL

1 AWARENESS

THE GOVERNMENT OF CANADA BECOMES AWARE OF AN INTERFERENCE ATTEMPT IN THE ELECTION DURING THE PERIOD THAT THE CARETAKER CONVENTION IS IN EFFECT.

2 SHARING INFORMATION

HEADS OF NATIONAL SECURITY AGENCIES BRIEF THE CRITICAL ELECTION INCIDENT RESPONSE PANEL:

Clerk of the Privy Council

National Security and Intelligence Advisor

Deputy Ministers of Justice, Public Safety, and Foreign Affairs.

3 ASSESSING THREAT

IF THE PANEL FINDS THAT THERE IS A SUBSTANTIAL THREAT TO A FREE AND FAIR ELECTION:

Inform the Prime Minister, political party officials and Elections Canada of the incident and that an announcement will be made

4 PUBLIC ANNOUNCEMENT

CANADIANS ARE INFORMED OF:

What is known about the incident

Any steps they should take to protect themselves

Government of Canada / Gouvernement du Canada

CANADA.CA/EN/DEMOCRATIC-INSTITUTIONS

Canada

For Public Release

Security and Intelligence Threats to Elections Task Force - Partner Roles

Leading to the next General Election

SECURITY AND INTELLIGENCE THREATS TO ELECTIONS TASK FORCE

WHAT ARE WE TALKING ABOUT?

Covert, clandestine, or criminal activities interfering with or influencing electoral processes in Canada

	MANDATE/ROLE	ACTIVITIES
CSE Communications Security Establishment	**Information Technology Security** • Providing advice, guidance, and services to help ensure the protection of electronic information and of systems of importance **Foreign Intelligence** • Collection of foreign intelligence for Government of Canada on threat actors **Supporting CSIS and RCMP** • Providing assistance on technical operations	• Providing intelligence and cyber assessments on the intentions, activities, and capabilities of foreign threat actors • Protecting Government systems and networks related to elections through cyber defence measures • Providing cyber security advice and guidance to political parties, provinces and other institutions involved in democratic processes
CSIS Canadian Security Intelligence Service	**Intelligence and Threat Reduction** • Collection of information about foreign influenced activities that are detrimental to the interest of Canada and are clandestine or deceptive or involve a threat to any person • Countering such activities through threat reduction measures **Intelligence Assessment** • Providing advice, intelligence reporting and intelligence assessments to Government of Canada about foreign influenced activities	• Providing threat briefings and intelligence reporting to Elections Canada and the Commissioner of Elections • Providing an assessment of hostile state activity methodologies and capabilities to Government of Canada decision makers
GAC Global Affairs Canada	**Mandate/Role** • Open source research on global trends and data on threats to democracy • Partnership with G7 countries to share information and coordinate responses to threats as appropriate	• Providing research on disinformation campaigns targeting Canada by foreign actors • Reporting on global trends, metrics, and incidents • Coordinating attribution of incidents
RCMP Royal Canadian Mounted Police	**Mandate/Role** • The primary responsibility for preventing, detecting, denying and responding to national security-related criminal threats in Canada • Investigates criminal offenses arising from terrorism, espionage, cyber attacks, and foreign influenced activities • The key investigatory body for Elections Canada if criminal activity is suspected	• Investigates any criminal activity related to interference or influence of Canada's electoral processes • Works closely in partnership with intelligence, law enforcement and regulatory agencies

Backgrounder
Digital Citizen Initiative and Digital Citizen Contribution Program

The Digital Citizen Initiative (DCI) is a multi-component strategy that aims to support democracy and social inclusion in Canada by building citizen resilience against online disinformation and building partnerships to support a healthy information ecosystem. It was launched as part of the Government of Canada's four pillar Plan to Protect Democracy in 2019.

DCI supports a community of Canadian researchers through its Digital Citizen Contribution Program (DCCP) which provides financial assistance for research and citizen-focused activities. Funded projects aim to support democracy and social inclusion in Canada by enhancing and/or supporting efforts to counter online disinformation and other online harms and threats.

Since January 2020, the DCCP has provided $15 million in funding to third-party organizations undertaking research and learning activities, such as public awareness tools and online workshops, to help Canadians build resiliency and think critically about information they encounter online. These projects have reached over 12 million Canadians online and offline, in minority communities, in both official languages and in Indigenous communities.

Examples of past and current calls

In 2020, the DCCP dedicated around $4.3 million specifically towards organizations supporting citizens to think critically about the health information they find online and to help citizens identify mis- and disinformation and limit the impact of racist and/or misleading social media posts relating to the COVID-19 pandemic. Funded projects reached people nationally and locally, online and offline, in Indigenous and minority communities, in both official languages.

In March 2022, DCCP launched a special targeted call for proposals to fund initiatives that help people identify online mis-and disinformation related to the war in Ukraine and other national threats to social cohesion. As result, 11 projects received a total of more than $2.4 million in funding for activities ranging from educational workshops, documentary podcasts, new educational resources, and efforts to counter Russian disinformation.

The DCCP's latest open call closed in August 2022 and provided over $1.2M to fund 16 research projects that aim to evaluate online platforms' efficacy in countering disinformation and other online harms; understand what role non-news and alternative media sources play in the disinformation sphere; and/or identify the behavioral and psychological underpinnings of the spread of disinformation and harmful content.

For Public Release

Countering an Evolving Threat:

Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions

Canada

Table of Contents

Introduction

On March 6, 2023, the Government of Canada announced several measures to combat foreign interference in Canadian democratic processes. Included in these measures was a request to develop a plan to address outstanding recommendations from the National Security and Intelligence Committee of Parliamentarians (NSICOP) in 2018 and 2019[1], the Judd Report[2], and the Rosenberg Report[3]. The plan, set out below, outlines these recommendations, summarizes the actions that have been taken so far to address them, and proposes further action.

Between the years 2018 to 2023, 26 recommendations were made with 16 of those received in early 2023, as part of the Rosenberg Report. Since the recommendations from each of the reports touch on similar issues, they have been grouped under the following themes:

- Communicating with Canadians about Foreign Interference and Protecting Canada's Democracy
- Effective Governance and Strong Legal Frameworks
- Risks, Vulnerabilities, and Security Measures
- Engagement with Partners to Enhance Awareness and Improve Resilience to Foreign Interference

A table with the status of each recommendation can be found at **Annex A**.

This plan outlines the recommendations made in the reports to protect Canadian democratic institutions and processes; summarizes the actions that have been taken or are in progress to address the recommendations; and proposes further steps for consideration to bolster Canada's response to foreign interference threats. In order to implement these further steps, additional work will be required, including, the policy approach, undertaking consultations, possible legislation for Parliamentary review, and implementation.

Recommendations from the Four Reports Reviewed – Implementation Status, Potential Gaps and Next Steps

There has been significant work done to implement many of the recommendations from the reports, and the Government is continuing to work toward implementing others.

---

[1] The 2019 NSICOP Annual Report (NSICOP 2019), and the 2018 NSICOP Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018 (NSICOP 2018). Other published reports from NSICOP and the National Security and Intelligence Review Agency were not examined as they did not contain recommendations re lating to foreign interference.

[2] The Report on the assessment of the 2019 Critical Election Incident Public Protocol (Judd Report)

[3] The Report on the assessment of the 2021 Critical Election Incident Public Protocol (Rosenberg Report)

The five recommendations from the two NSICOP reports (2018 and 2019) have been partially addressed. Some action has been taken with respect to every recommendation, and additional options for consideration have been identified.

Four of five recommendations of the Judd Report have been implemented in whole or in part. One of the recommendations (#2) proposes that the Critical Election Incident Public Protocol be expanded to apply even when there is no election being held. This had not been implemented because Ministers already have the responsibility and the necessary powers to address any concerns about foreign interference that could arise between elections. Ministerial responsibility is a fundamental tenet of Canada's parliamentary democracy.

The Rosenberg Report, received in February 2023, outlined 16 recommendations which are in the process of being considered for early implementation.

Communicating with Canadians about Foreign Interference and Protecting Canada's Democracy	NSICOP 2019 (#1) Judd (#1, 5) Rosenberg (#1, 4-5, 10-11, 15, 16)

The four reports point out that equipping citizens with knowledge is the best defence against those who try to meddle in Canada's democratic processes. In its 2019 report, NSICOP outlined that, with regards to foreign interference, it is critical to "strengthen public awareness of threats to Canada." Mr. Rosenberg, in his recent report, emphasized the importance of establishing "a clear articulation of the problem and the approach to addressing it."

Current Status

The Government of Canada has taken steps to increase public awareness around foreign interference and to encourage a whole-of-society approach to addressing this threat. Since 2018, the Canadian Security Intelligence Service (CSIS) has highlighted the threat of foreign interference in every Annual Report. Before the 2021 federal election, CSIS released a public report focusing on foreign interference and threats to Canada's democratic process. The Communications Security Establishment (CSE) also began publishing reports on foreign cyber interference in the context of elections in 2017. The Government of Canada has also undertaken specific outreach activities to engage Canadians and communities, including CSIS stakeholder engagement (industry, universities, Canadian communities, civil society), CSE and Cyber Centre outreach (industry, small business, privately-owned critical infrastructure), and Royal Canadian Mounted Police (RCMP) community outreach efforts.

In advance of the 2019 election, Canada put in place the Plan to Protect Canada's Democracy. The Plan was the first of its kind internationally and recognized the importance of an informed citizenry in defending against foreign interference through the establishment of the Digital Citizen Initiative. This initiative supports democracy and social inclusion in Canada by building

citizen resilience against online disinformation and building partnerships to support a healthy information ecosystem. The Plan also recognized the importance of collaboration with allies and like-minded partners by expanding Canada's leadership role in the G7 Rapid Response Mechanism, which was launched at the G7 meeting hosted by Canada in 2018. This mechanism helps G7 and other allied countries to cooperate by sharing information about foreign interference on social media. Since 2018, the Government of Canada has invested close to $20 million in the G7 Rapid Response Mechanism, including $13.4 million over five years in May 2022, to deepen the coordination between countries in identifying, and responding to, foreign threats to democracy, including state-sponsored disinformation.

The Plan to Protect Canada's Democracy also signalled that government institutions need to continue to work together to prepare and respond to threats of foreign interference. The Cabinet Directive on the Critical Election Incident Public Protocol (the Protocol) is part of this effort. The Protocol establishes a non-partisan panel of deputy ministers (the Panel) tasked with communicating to Canadians about incidents during the writ period that threatened the integrity of a federal election.

The Panel's deliberations are informed by another innovation, the Security and Intelligence Threats to Elections (SITE) Task Force, which is made up of officials from the RCMP, CSE, CSIS and Global Affairs Canada, to report on covert, clandestine, or criminal activities by foreign actors.

The Plan recognized that foreign state interference and disinformation challenges are complex and inter-related – the latter being a tactic of the former. As such, the Plan outlined a whole-of-society approach to tackling them. The Government of Canada is working to further equip academia, civil society, and provinces and territories with the resources needed to increase awareness of these threats. Working with these partners is essential to ensuring Canada continues to adapt to ever-changing challenges.

The Government's approach continues to evolve. The Plan to Protect Canada's Democracy has been revised and improved since the 2019 federal election by bringing to bear four strategic areas of improvement:

- Strengthening a "full election cycle" view of threats;
- Broadening the Government's view on threat awareness;
- Developing central leadership on disinformation; and
- Continuously reinforcing the resilience of institutions and citizens.

The Plan to Protect Canada's Democracy has also been improved by addressing Mr. Judd's recommendations for the Critical Election Incident Public Protocol. These changes included:

- Alignment of the Protocol's application period with that of the Caretaker Convention;
- An explicit provision for the Panel to consult with the Chief Electoral Officer, as appropriate;

- A provision for the ability of political parties to alert security agencies of incidents that could threaten a free and fair election; and
- A recognition of the Panel's ability to examine domestically-driven interference, as well as to receive information from sources other than security agencies.

The Canada Declaration on Election Integrity Online was strengthened by expanding signatories beyond the original four – Facebook, Google, Microsoft and Twitter. In 2021, TikTok, LinkedIn and YouTube joined the Declaration. First established in 2019, the Declaration is a voluntary agreement with social media platforms to increase the transparency, authenticity and integrity of their systems to help safeguard Canada's federal elections. The Declaration recognizes that social media and other online platforms, as well as the Government of Canada, have respective responsibilities to help safeguard Canada's electoral processes. This directly responded to Mr. Judd's recommendation #5 and helped to reduce disinformation.

The renewed Plan to Protect Canada's Democracy also recognized the importance of departments and agencies working together to address quickly emerging challenges. It additionally strengthened interdepartmental cooperation in countering disinformation. Drawing upon insights developed by the United Kingdom's RESIST model, this work is founded on the need to recognize disinformation and to understand how it works. While still in its early stages, these efforts also seek to enhance the availability of reliable information on government programs and services, implement a counter disinformation toolkit, and offer training for Parliamentarians and public servants on foreign interference and disinformation.

Most recently, the Government of Canada established the Protecting Democracy Unit within the Privy Council Office and tasked it with coordinating, developing, and implementing government-wide measures designed to combat disinformation and to protect Canada's democratic institutions. Together, these efforts contribute to the overarching objective of one of NSICOP's 2019 recommendations to "build institutional and public resiliency" through "sustained central leadership and coordination."

Potential Gaps and Next Steps

Informed by earlier reviews and by evidence from the 2019 and 2021 federal elections in which the above measures were in place, Mr. Rosenberg finds that "the government's plan and public communications should acknowledge that the problem of interference occurs both before the election is called and during the caretaker period" – it is not just during the election period, but all the time.

Mr. Rosenberg also finds that the Government should be clear that "the Protocol is only one element in a much larger set of measures aimed at addressing election interference". Mr. Rosenberg recommends "an early, fulsome communications approach" that explains the "full range of activities that occur during the caretaker period." These findings align closely with earlier findings from NSICOP that recommend that the Government "engage Canadian institutions more thoroughly on the significant threats they face" with regards to foreign

interference. It can, however, be challenging to speak openly about foreign interference, given the risk of revealing intelligence, the need to protect sources, and to ensure critical relationships are maintained with Canada's intelligence partners. NSICOP acknowledged this reality in its 2019 report when it emphasized the "challenges in communicating information" related to foreign interference "due to the sensitive nature of the information."

Nevertheless, it is clear that a central finding in the four reports studied relates to a requirement for increased transparency with Canadians about the extent and nature of foreign interference in democratic processes. There is more work to be done to ensure broader awareness of both the threats facing Canada and the measures put in place to address them. As per Mr. Rosenberg's recommendations to undertake more robust and frequent communications with Canadians on foreign interference and Canada's efforts to protect Canadian democracy, the Government, including responsible ministers as well as national security and intelligence officials, will find further opportunities to keep Canadians informed of the extent of foreign interference affecting all aspects of society, including in their democracy. An engaged, informed, and resilient citizenry is one of our best defenses against attempts to undermine our democracy and its institutions. Keeping Canadians informed of the activities being undertaken on their behalf, and adopting emerging communications best practices that draw from Canada and NATO's recent efforts to identify and counter Russian state sponsored disinformation in the invasion of Ukraine, will help ensure Canadians' democracy remains strong and secure.

Specifically, the Government will use the new National Counter Foreign Interference Coordinator and CSIS's upcoming Annual Report to bolster communications with Canadians.

Additionally, new briefings to be offered to Members of Parliament and Senators will increase awareness of the threat foreign interference poses. The new National Counter Foreign Interference Coordinator will work on expanding briefing mechanisms with provincial/territorial, municipal, and Indigenous officials.

Recently announced funding to strengthen the capacity of civil society partners to counter disinformation, including from foreign sources, will also help to increase resilience. The Government is also accelerating efforts to strengthen the capacity of the Government of Canada, and partners, to combat disinformation, including state-sponsored disinformation, through strategic communications, based on the RESIST model.

These measures are consistent with the commitments outlined in Minister LeBlanc's mandate letter – in which he is charged to "lead an integrated government response to protect Canada's democratic institutions, including the federal electoral process, against foreign interference and disinformation". This work will need to be done in close collaboration with others, including the Minister of Public Safety, who has the overall responsibility to lead the government-wide efforts to counter foreign interference. Efforts will also be informed by key partners such as the Chief Electoral Officer, whose post-election recommendations reports provide important insights on developments affecting Canada's electoral system.

8 Countering an Evolving Threat

Using the findings and recommendations from the Independent Special Rapporteur's review on foreign interference, as well as the ongoing reviews from NSICOP and the National Security and Intelligence Review Agency (NSIRA), the Government will take additional action.

Effective Governance and Strong Legal Frameworks	NSICOP 2019 (#1c-d) NSICOP 2018 (#2) Rosenberg (#8)

The reports studied highlighted the importance of having a modern and robust legal and governance framework to counter foreign interference, which balances national security considerations with privacy and other Charter protections.

Current Status

In 2017, Parliament created NSICOP, which provides a forum for Members of Parliament of all recognized political parties and Senators with top-secret clearance to review classified information. In line with the NSICOP 2019 recommendation #1d, which calls for a whole-of-government mechanism to identify and respond to foreign interference, the Government has recently taken several steps to respond to foreign interference through operational and policy mechanisms. Firstly, the Prime Minister announced the creation of the National Counter Foreign Interference Coordinator within Public Safety Canada, a new role with the express purpose of coordinating efforts to combat foreign interference. Budget 2023 announced an investment of $13.5 million over five years and $3.1 million ongoing to fund the Coordinator's office and its activities. Secondly, the Government launched public consultations regarding the implementation of a Foreign Influence Transparency Registry to expand Canada's toolkit to confront this evolving threat. These consultations are due to conclude in spring 2023.

In addition, the 2018 NSICOP special report highlighted the key role played by the National Security and Intelligence Advisor (NSIA) to the Prime Minister in providing advice as coordinator of the security and intelligence community and as advisor to the Prime Minister. Since then, steps were taken to further strengthen the national security governance framework to ensure that the NSIA maintains active awareness of ongoing threats and mitigation measures, including those related to foreign interference.

The NSICOP report from 2019 recommended (#1c) that the Government assess existing legislation that pertains to foreign interference, specifically the *Security of Information Act* and the *Canadian Security Intelligence Service Act* (CSIS Act), and make legislative changes as required. Departments and agencies have conducted extensive policy and legal analysis with respect to these laws, have identified gaps, and continue to develop options to address them with a view to strengthening Canada's legal framework.

The *Elections Modernization Act*, which Parliament passed in 2018, prohibits the use of funds from foreign entities and includes heightened transparency measures. The Government has also introduced other pieces of legislation, including Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, to bolster cyber security.

In 2019, the Government created NSIRA, which conducts independent expert review of national security and intelligence activities across all federal departments and agencies and informs Parliament and Canadians as to their lawfulness.

Additionally, Budget 2023 provides $53 million over two years to support departments and national security and intelligence agencies to support them in fulfilling their obligations to comply with legislated review requirements in a timely and efficient manner as well as implement recommendations.

Potential Gaps and Next Steps

In order to modernize Canada's legal toolkit to address foreign interference threats and fully implement the NSICOP recommendation on strengthening the legal framework, the Minister of Public Safety, informed by the ongoing work of the Independent Special Rapporteur and the reviews of NSICOP and NSIRA, will:

- Work on changes to modernize the *CSIS Act* which was written before the internet was widely available. Changes could be advanced to allow CSIS to better operate in a digital world by effectively collecting and using digital data; enable CSIS to share intelligence with non-government partners to help them counter threats; and collect intelligence and conduct activities to counter foreign threats that were not envisioned when the *CSIS Act* received Royal Assent in 1984. This work should also be informed by the recommendations in the Public Order Emergency Commission's final report that pertain to the *CSIS Act*. Given the need for Canadians, particularly members of diaspora communities, to have confidence that their national security agencies are working to protect their interests and respect their Charter rights, robust dialogue and consultation on any proposals will be required; and
- Working with enforcement partners and national security agencies, explore if further amendments to existing provisions are needed and whether to create new offences under the *Security of Information Act* and the *Criminal Code* to facilitate prosecution of foreign interference activities.

In referring to the 2018 *Election Modernization Act*, Mr. Rosenberg notes that "Canada's election laws have been modified to more effectively counter foreign interference." The Minister of Intergovernmental Affairs, Infrastructure and Communities is currently working on amendments to the *Canada Elections Act*. As part of this process, the Minister is examining potential amendments to also counter foreign interference.

Risks, Vulnerabilities, and Security Measures

NSICOP 2019 (#1a-b)
Rosenberg (#2-3)

The reports reviewed provided several recommendations related to the requirement for the Government to have the ability to evaluate risks and vulnerabilities resulting from the growing threat posed by foreign interference in order to be able to adapt the Government's toolkit to the evolving threat.

Current Status

The NSICOP 2019 report highlighted the need to identify risks and harms to institutions posed by the foreign interference threats (#1a), as well as requirements to undertake a full examination of resulting vulnerabilities (#1b). In response, departments and agencies have developed assessments of threats and risks posed by foreign interference, and measures to counter these threats. Departmental Chief Security Officers (CSO) and Chief Information Officers (CIO) have, under the leadership of the Privy Council Office, undertaken training to better inform the CSO and CIO community of threats and possible mitigation strategies (e.g., technical safeguards and cyber hygiene tips). In addition, as part of the assessments of threats and risks, departments and agencies have been engaging with stakeholders from sectors of strategic interest – such as critical infrastructure operators – to help identify risks and address vulnerabilities relevant to their specific areas of operation.

In order to address foreign state efforts to interfere in Canada's democracy by intimidating diaspora communities in Canada, Budget 2023 provides $48.9 million over three years to the RCMP to protect Canadians from harassment and intimidation, increase its investigative capacity, and more proactively engage with communities at greater risk of being targeted.

Potential Gaps and Next Steps

Foreign interference can be subtle and the potential effects difficult to identify, quantify and articulate. As such, departments and agencies continue to engage with stakeholders in academia and through other outreach programs to assess short- and long-term impacts of foreign interference in Canada, while continuing to make updates to assessments as the threat evolves. Mr. Rosenberg made the recommendation (#2) that "preparations for the next election should include an assessment of whether ministerial security, [RCMP] protective policing, and local policing capabilities are adequate for the level and persistence of threats and whether there is effective coordination among these bodies. There should also be a review of the coordination between political parties and the government with respect to campaign and security operations." The Minister of Public Safety and the Minister of Intergovernmental Affairs, Infrastructure and Communities have undertaken a comprehensive analysis of security threats and protective

measures available to Ministers, other Parliamentarians and senior officials, including foreign interference threats. The Ministers are evaluating tools to align with the threat environment and alleviate risks and vulnerabilities.

Mr. Rosenberg also recommended (#3) that "[t]here should be an assessment as to whether any adjustments should be made to the role of the SITE membership in light of the growing problem of domestic interference". This will be considered through further enhancements to the Plan to Protect Canada's Democracy, building on the guidance laid out in Minister LeBlanc's mandate letter, and will include an examination of making SITE a permanent entity, with a mandate to conduct regular reporting on foreign interference activities.

Engagement to Raise Awareness and Improve Resilience to Foreign Interference	NSICOP 2019 (# 1e, 1f, 1g, 2) NSICOP 2018 (#1 (A and B)) Judd (#3-4) Rosenberg (#6-7, 12-14)

Foreign interference is both a local and a global threat. It affects individuals, organizations, companies, as well as democratic processes at every level. It cannot be effectively addressed by any entity or order of government acting in isolation. It evolves quickly, making the sharing of information one of the most effective tools to stay abreast of the risks. The Government of Canada must work with partners both domestically and internationally to ensure the strongest defences possible are in place. Each of the four reports provided recommendations that point to the need for a whole-of-society approach in countering foreign interference. These include recommendations to enhance engagement domestically and internationally, as well as to ensure partners and stakeholders are informed and able to contribute to collective efforts.

Current Status

In response to recommendations made by NSICOP in 2018 and 2019, the Government has advanced several efforts. The Prime Minister announced the creation of the National Counter Foreign Interference Coordinator within Public Safety Canada, which directly responds to the NSICOP 2019 recommendation #2. The Government has also made progress in response to two other NSICOP 2019 recommendations. For example, security and intelligence agencies, including the RCMP, CSIS, Public Safety Canada, and the Canadian Centre for Cyber Security, have expanded engagement with provincial, territorial and municipal representatives, as well as with Indigenous leaders and communities, and critical infrastructure owners and operators to increase awareness of threats and build resilience (#1e). The RCMP also works with police of jurisdiction (POJ) to counter foreign interference, including for the countering of state backed harassment and intimidation, as POJs are often the first to be made aware of foreign interference-related activities. Further, the security and intelligences agencies and others continue to engage regularly with international partners on collaborative efforts to address foreign interference, including through

intelligence sharing. Cooperation with Canada's allies is also undertaken by the Minister of Public Safety as Canada's representative at the annual Five Country Ministerial, where Five Eyes security ministers meet to collaborate on various national security issues, including foreign interference; discuss respective approaches to shared issues; and coordinate a cohesive Five Eyes response (#1g).

In its 2018 special report, the NSICOP recommended (#1) that, "in the interest of national security, members of the House of Commons and the Senate should be briefed upon being sworn-in and regularly thereafter on the risks of foreign interference and extremism in Canada." It further recommended that Ministers "should be reminded of the expectations described in the Government's *Open and Accountable Government*... [and that] ... consistent with the *Conflict of Interest Act*, public office holders must always place the public interest before private interests." Measures exist that address this recommendation. First, expectations and obligations for Ministers and their actions have been made public as part of their individual mandate letters. Second, the Parliamentary Protective Service provides security briefings to incoming Parliamentarians which address various threats, including foreign interference. SITE has also offered briefings to political party representatives during the writ period, while the Privy Council Office briefs all incoming Ministers and Parliamentary Secretaries upon appointment on the range of security threats, including foreign interference.

Mr. Judd recommended that Canada "should monitor any international developments, with particular attention paid to any evolution in tactics by malign actors and any developments in defensive counter-measures taken by target countries (legal, regulatory and operational)." The Government has pursued international collaboration in many fora, including through the Rapid Response Mechanism, bringing together G7 countries to identify and respond to foreign threats. The Paris Call for Trust and Security in Cyberspace (Paris Call) was launched in November 2018 and calls on states, the private sector, and civil society organizations to work together to enhance security in cyberspace, fight disinformation and address new threats that emerge. Through the Paris Call, Canada and other groups exchange information and good practices on several aspects related to foreign electoral interference. Workshops were organized resulting in the publication of Multi-Stakeholder insights: A compendium on countering election interference in 2021.
In response to Mr. Judd's recommendation #4, the Government offered briefings for political parties in the lead up to the 2021 federal election, including providing information about issues the parties may face during the campaign.

Mr. Rosenberg highlighted "the need to work with external partners in Canada and globally, from academia, industry, and civil society, to support information integrity during elections. These external partners play several important roles. They have perspectives on the evolving threat environment that may differ from those of the national security agencies. They have a public education role. They can also alert the public to attempts at interference both before and during the campaign." To this end, the Government of Canada has worked to empower Canadians,

particularly youth, with the right skills to navigate online information. Since January 2020, the Digital Citizen Initiative has invested over $15 million in 96 projects by civil society and academic organizations to build citizen resilience against disinformation. The Government's commitment to the Digital Citizen Initiative was further expanded in the 2022 Fall Economic Statement with an investment of $31 million over four years, more than doubling the program's yearly funding. On March 6, 2023, the Government of Canada announced an investment $5.5 million to strengthen the capacity of civil society partners to provide important insight into the dynamics of Canada's information ecosystem, strengthening the resilience and digital literacy of government, industry, civil society and citizens.

Potential Gaps and Next Steps

NSICOP's 2019 report recommended (#1f) that Canada's strategy to counter foreign interference and build institutional and public resilience should "include an approach for ministers and senior officials to engage with fundamental institutions and the public." As the Government reviews the Protocol following the release of Mr. Rosenberg's report, the Government will look at establishing a process by which Ministers and senior officials, including members of the Panel as part of the Critical Election Incident Public Protocol, engage with stakeholders and communities. This engagement would seek views on best practices to mitigate the impact of foreign interference and disinformation on Canada's institutions.

The Government will also continue working with Canadian partners to further the work accomplished through the Paris Call to ensure that everyone has access to the most current expertise to protect Canada's electoral processes.

The report by Mr. Rosenberg also included recommendations to brief political party representatives in a secure location in Ottawa (#12) and to fix briefing schedules during the election period in advance while being flexible to urgent situations (#13). These recommendations will be implemented. The report further suggested providing a program for unclassified briefings for Parliamentarians and their staff on foreign interference and ways they can protect themselves (#14). Briefings will be offered to Parliamentarians and their staff following their swearing-in and on a regular basis in the future.

Conclusion and Next Steps

The Government of Canada has implemented a number of measures in recent years to counter foreign interference in all aspects of society, including those related to democratic processes. These measures respond to several recommendations made by NSICOP, Mr. Judd and Mr. Rosenberg, either in whole or in part. This plan outlines further actions to respond to the outstanding recommendations and close any remaining gaps.

This work includes further increasing transparency and communications with Canadians about the threat of foreign interference and the specific Government actions being undertaken to mitigate it. This includes reviewing existing legislation, such as the *CSIS Act*, the Criminal Code, the *Security of Information Act*, and the *Canada Elections Act*. It also includes enhancing the security of senior public officials and exploring possible improvements to SITE and the Cabinet Directive.

Any steps taken will be undertaken with close consideration for ongoing work done by NSICOP, the National Security and Intelligence Review Agency, and the Independent Special Rapporteur, the Right Honourable David Johnston, to ensure Canadians continue to have confidence in their democratic institutions and electoral processes.

Annex A – Table of Recommendations and Associated Actions

	Recommendation	Key Actions and Next Steps
National Security and Intelligence Committee of Parliamentarians (NSICOP) Annual Report 2019		
1	The Government of Canada develop a comprehensive strategy to counter foreign interference and build institutional and public resiliency. Such a strategy should:	Departments and agencies work together as part of an effective governance framework to identify and respond to foreign interference activities. The new National Counter Foreign Interference Coordinator will play a leading role to ensure Government-wide efforts to combat foreign interference are working effectively and towards the same goal. Using the findings and recommendations from the Independent Special Rapporteur's review on foreign interference, as well as the ongoing reviews from NSICOP and the National Security and Intelligence Review Agency, the Government will take additional action.
	a) Identify the short- and long-term risks and harms to Canadian institutions and rights and freedoms posed by the threat of foreign interference.	Departments and agencies have developed comprehensive assessments of foreign interference threats and risks. This analysis is ongoing, and takes into account how the threat—and the measures to counter it—evolve. Departments and agencies have been engaging with stakeholders in various sectors to share information on threats and help identify risks. Challenges remain in concretely measuring and articulating foreign interference harms in certain sectors of strategic interest. The Government will leverage the new National Counter Foreign Interference Coordinator, academic and other outreach programs to engage stakeholders to further assess the short- and long-term impacts of foreign interference in Canada.
	b) Examine and address the full range of institutional vulnerabilities targeted by hostile foreign states, including areas expressly omitted in the NSICOP's review.	Departments and agencies have developed comprehensive assessments of foreign interference threats and risks. The tools used by foreign state actors to conduct interference activities continue to evolve, require ongoing assessments of risks. Departments and agencies will continue to

	Recommendation	Key Actions and Next Steps
		collaborate with stakeholders to assess vulnerabilities in strategic sectors. Budget 2023 provides $48.9 million over three years to the Royal Canadian Mounted Police (RCMP) to protect Canadians from harassment and intimidation, increase its investigative capacity, and more proactively engage with communities at greater risk of being targeted.
	c) Assess the adequacy of existing legislation that deals with foreign interference, such as *Security of Information Act* or the *Canada Security Intelligence Service Act* (CSIS Act), and make proposals for changes if required	Over the past few years, departments and agencies have conducted policy and legal analysis to identify gaps and develop options to address them. The Minister of Public Safety, informed by the ongoing work of the Independent Special Rapporteur and the reviews of NSICOP and NSIRA, will work and consult on changes to the *CSIS Act*, the *Security of Information Act*, and the *Criminal Code*.
	d) Develop practical, whole-of-government operational and policy mechanisms to identify and respond to the activities of hostile states.	The establishment of the Counter-Foreign Interference Coordinator enhances the existing national security governance and the government's capacity to effectively address foreign interference activities. Budget 2023 provides $13.5 million over five years, and $3.1 million ongoing to Public Safety Canada to establish a National Counter-Foreign Interference Office. The 2023 Budget further proposes $48.9 million over three years to the RCMP to protect Canadians from harassment and intimidation, increase its investigative capacity, and more proactively engage with communities at greater risk of being targeted. Departments and agencies work together as part of an effective governance framework to identify and respond to foreign interference activities. Over the past years, steps were taken to strengthen the national security governance framework to ensure that the NSIA maintains active awareness of ongoing threats and mitigation measures, including those related to foreign interference. Budget 2022 provided $2 million annually for the Protecting Democracy Unit at the Privy

	Recommendation	Key Actions and Next Steps
		Council Office to coordinate, develop, and implement government-wide measures designed to combat disinformation and protect Canada's democratic institutions and processes. This includes developing a whole-of-society approach to protecting Canada's democracy, the implementation of a counter disinformation toolkit, and training for Parliamentarians and public servants on misinformation and disinformation, building upon the United Kingdom's RESIST model. It also includes further developing options to strengthen interdepartmental governance, in consideration of existing committees. The Government of Canada announced a $5.5 million investment to strengthen the capacity of civil society and research partners to provide important insights into the dynamics of Canada's information ecosystem, including with respect to disinformation and activities of state actors.
	e) Establish regular mechanisms to work with sub-national levels of government and law enforcement organizations, including to provide necessary security clearances.	Over the past few years, the RCMP, CSIS, the Canadian Centre for Cyber Security, and Public Safety Canada have engaged with provincial, territorial and municipal colleagues, as well as with critical infrastructure owners and operators to increase awareness of foreign interference threats and build resilience. Sustained, regular, and coordinated engagement with partners is essential to detect threats, build resilience and effectively counter foreign interference activities. The new National Counter Foreign Interference Coordinator will work on expanding briefing mechanisms with provincial/territorial, municipal, and Indigenous officials. The Protecting Democracy Unit within the Privy Council Office will expand its work with provinces and territories.
	f) Include an approach for ministers and senior officials to engage with fundamental institutions and the public	Departments and agencies have been developing their capabilities to conduct outreach activities, including CSIS stakeholder engagement (industry, universities, research and development, Canadian communities, civil

	Recommendation	Key Actions and Next Steps
		society), Communications Security Establishment and Cyber Centre outreach (industry, small business, privately-owned critical infrastructure), and RCMP community outreach efforts. Communications and outreach are key elements of the government strategy to counter foreign interference. Efforts will continue to engage with partners effectively and cohesively across all jurisdictions. The Government will use the new National Counter Foreign Interference Coordinator and CSIS's upcoming Annual Report to bolster communications with Canadians. Recently announced funding to strengthen the capacity of civil society partners to counter disinformation, including from foreign sources, will also help to increase resilience. New briefings will be offered to Members of Parliament and Senators and the Coordinator will work on expanding briefings to partners outside the Federal Government. The Government will look at establishing a process by which members of the Panel as part of the Critical Election Incident Public Protocol, engage with stakeholders and communities. This engagement would seek views on best practices to mitigate the impact of foreign interference and disinformation on Canada's institutions.
	g) Guide cooperation with allies on foreign interference.	Departments and agencies each engage with their international counterparts in collaborative efforts and partnerships to address foreign interference. The Counter Foreign Interference Coordinator will increase the coherence of these interdepartmental efforts, and will ensure alignment with Canada's foreign policy objectives. Cooperation with Canada's allies is also undertaken by the Minister of Public Safety as Canada's representative at the annual Five

	Recommendation	Key Actions and Next Steps
		Country Ministerial, where Five Eyes security ministers meet to collaborate on various national security issues, including foreign interference; to discuss respective approaches to shared issues; and to coordinate a cohesive Five Eyes response.
2	The Government of Canada support this comprehensive strategy through sustained central leadership and coordination. As an example of a central coordinating entity to address foreign interference, the Committee refers to the appointment and mandate of the Australian National Counter Foreign Interference Coordinator.	The Prime Minister announced the establishment of the Counter Foreign Interference Coordinator. Budget 2023 proposes to provide $13.5 million over five years, and $3.1 million ongoing to Public Safety Canada to establish a National Counter-Foreign Interference Office. Budget 2022 provided $2 million annually to the Privy Council Office to coordinate, develop, and implement government-wide measures designed to combat disinformation and protect Canada's democracy.
National Security and Intelligence Committee of Parliamentarians (NSICOP) Special Report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018		
1	1.A. Members of the House of Commons and Senate should be briefed upon being sworn-in and regularly thereafter on the risks of foreign interference and extremism in Canada.	The Parliamentary Protective Service provides security briefings to incoming Members of Parliament. The Security and Intelligence Threats to Election Task Force (SITE) offers briefings to political party representatives during writ period. The Privy Council Office Security Operations Division briefs all incoming Ministers and Parliamentary Secretaries on the spectrum of threats, including foreign interference. CSIS also provides briefings to Parliamentarians upon request. Briefings for Members of Parliament and the Senate will be provided upon their swearing-in and on a regular basis.
	1.B. Cabinet Ministers should be reminded of the expectations described in the directive on *Open and Accountable Government*, including that Ministers exercise discretion with whom they meet or associate, and clearly distinguish between official and private media messaging,	Expectations and obligations for Ministers and their actions have been made public as part of *Open and Accountable Government*.

	Recommendation	Key Actions and Next Steps
	and be reminded that, consistent with the *Conflict of Interest Act*, public office holders must always place the public interest above private interests.	
2	The Minister of Public Safety and Emergency Preparedness should consider revising the *** to include a formal role for the NSIA. The Committee believes that the NSIA has a legitimate role to provide advice as coordinator of the security and intelligence community and advisor to the Prime Minister.	Steps were taken to further strengthen the national security governance framework to ensure that the National and Security and Intelligence Advisor to the Prime Minister (NSIA) maintains awareness of ongoing threats and mitigation measures, including those related to foreign interference.
Report on the assessment of the 2019 Critical Election Incident Public Protocol (Judd Report)		
1	Implement the Protocol for the next election using the same model and Panel membership. Prepare Panel members early, starting with new members. The high threshold and decision by consensus should be maintained, as well as the support and participation from the same departments and agencies. The rationale is that this model has already been accepted by political parties and there is the ability to maintain some consistency in membership. An accompanying media strategy should also be developed.	The Cabinet Directive on the Critical Election Incident Public Protocol was updated ahead of the 2021 federal election. It maintained the same general framework and included some changes informed by Mr. Judd's evaluation. While the Government's media strategy was not as comprehensive for the 2021 election compared to 2019 in a minority Parliament context, a more proactive communications strategy will be developed by the Privy Council Office for future elections and would build on the recommendations made by Mr. Rosenberg.
2	The Protocol should also cover the pre-writ period, recognizing this may not be possible in the event of an election triggered by a non-confidence vote.	This recommendation was not implemented since ministers already have the responsibility and the necessary powers to address any concerns about foreign interference that could arise between elections. Ministerial responsibility is a fundamental tenet of Canada's parliamentary democracy. Building on Mr. Rosenberg's recommendations, the Government will find further opportunities to communicate with Canadians about threats to democratic institutions and electoral processes at all times, irrespective of the electoral calendar.
3	Privy Council Office support teams (Democratic Institutions and Security and Intelligence) should monitor any international developments, with particular attention paid to	The Government will continue to build on existing work from allies and learn from best practices. For instance, the Government could re-engage with Canadian partners to further

	Recommendation	Key Actions and Next Steps
	any evolution in tactics by malign actors and any developments in defensive counter-measures taken by target countries (legal, regulatory and operational). This can also include academic and think-tank research.	the work accomplished through the Paris Call to ensure that Canada's allies have access to the most current expertise to protect electoral processes. In addition, Budget 2022 provided funding to coordinate, develop, and implement government-wide measures designed to combat disinformation and protect Canada's democracy. The Protecting Democracy Unit is undertaking research on threats to democracy. The Government also provided $13.4 million over five years in May 2022 to deepen the coordination between countries in identifying, and responding to, foreign threats to democracy, including state-sponsored disinformation.
4	Immediately establish the same relationships with the political parties, particularly with respect to guidance and support around cyber issues as the parties are likely targets beyond simply the election period.	Briefings were offered in the lead up to the 2021 elections. SITE plans to hold similar briefings in future elections, building on recommendations by Mr. Rosenberg.
5	Conduct an evaluation on the extent to which the social media platforms lived up to the Canada Declaration on Electoral Integrity Online. Once complete, hold discussions with the platforms on the Government's expectations for the next election. Participation in the Paris Call could possibly inform any new agreements.	A lessons learned exercise in relation to the Declaration was conducted following the 2019 election. Discussions with the platforms were held in the lead up to the 2021 election resulting in a revised Declaration and three additional signatories (TikTok, LinkedIn and YouTube).
	Report on the assessment of the 2021 Critical Election Incident Public Protocol (Rosenberg Report)	
1	Public communication about the Protocol should provide a clear explanation for the inclusion of domestic actors and of the types of activities that are of concern.	The Privy Council Office will develop a strategy to better communicate with Canadians about the Protocol and how it fits within the suite of measures to counter foreign interference and protect democratic institutions.
2	Preparations for the next election should include an assessment of whether ministerial security, Royal Canadian Mounted Police protective policing, and local policing capabilities are adequate for the level and persistence of threats and whether there is effective coordination among these bodies.	The Government will evaluate tools to enhance the security and information for Parliamentarians in order to address the changing threat environment, security gaps and concerns for safety. This is in keeping with the mandate letter commitment for the Minister of Public Safety to work with the

	Recommendation	Key Actions and Next Steps
	There should also be a review of the coordination between political parties and the government with respect to campaign and security operations.	Minister of Intergovernmental Affairs, Infrastructure and Communities to bolster the security of Ministers and Parliamentarians.
3	There should be an assessment as to whether any adjustments should be made to the role of the SITE membership in light of the growing problem of domestic interference.	With a view to continuously improved measures under the Plan to Protect Canada's Democracy, the Government will review the mandate and membership of SITE.
4	There should be an announcement, within a year of the previous election, about the government's plan to safeguard the integrity of Canada's elections, including an explanation of the reason for the Protocol.	The Privy Council Office will develop a strategy to better communicate with Canadians about the Protocol and how it fits within the suite of measures to counter foreign interference and protect democratic institutions.
5	The government's plan and public communications should acknowledge that the problem of interference occurs both before the election is called and during the caretaker period. It should be clearer on how and by whom pre-election interference will be addressed, beyond saying that it will be handled through normal ministerial channels.	The Minister of Intergovernmental Affairs, Infrastructure and Communities, with the support of the Privy Council Office and the Minister of Public Safety, will look for opportunities to increase communications with Canadians about threats to democratic institutions and electoral processes at all times, irrespective of the electoral calendar.
6	The government should consider options to ensure that the Panel is well-prepared in advance, and as much as possible, continuity of members is maintained between elections.	The Privy Council Office will ensure Panel members are in a permanent state of readiness to assume their Panel-related responsibilities by briefing new Panel members within three months of being appointed to their new position to explain Panel roles and responsibilities.
7	Briefings of the Panel should begin much earlier in the mandate and include non-government actors with expertise on interference and disinformation.	The Privy Council Office will ensure Panel members are in a permanent state of readiness to assume their Panel-related responsibilities by briefing new Panel members within three months of being appointed to their new position to explain Panel roles and responsibilities. Beginning in spring 2023, Panel meetings will be held regularly.
8	There should be an opportunity for a review body to assess the decisions of ministers with respect to the use of threat reduction measures during the caretaker period.	NSICOP and NSIRA may undertake reviews in accordance with their mandates.
9	The government should consider amending section 6.0 to provide that, barring any national security or public interest reasons, an	Following Mr. Rosenberg's report, the Government is reviewing the Cabinet Directive and examining possible changes.

	Recommendation	Key Actions and Next Steps
	announcement would be made if the threshold is met.	
10	The government should consider removing the fourth sentence in the final paragraph of section 6.0 and clarifying that actual or potential impact is one of several considerations that the Panel takes into account in exercising its judgment as to whether the threshold has been met.	Following Mr. Rosenberg's report, the Government is reviewing the Cabinet Directive and examining possible changes.
11	There should be further study of the issue of whether the Protocol should be amended to provide for the possibility of announcements below the threshold set out in section 6.0.	Following Mr. Rosenberg's report, the Government is reviewing the Cabinet Directive and examining possible changes.
12	There should be an effort made to provide briefings to political party representatives at downtown Ottawa secure locations.	During electoral periods, the Privy Council Office will ensure briefings to political party representatives take place at downtown Ottawa secure locations.
13	The times for briefings of political party representatives should be fixed in advance, with flexibility to address urgent situations.	During electoral periods, the Privy Council Office will ensure a schedule of briefings is provided to political party representatives as soon as possible following the issue of the writ.
14	The national security agencies should develop a program of unclassified briefings to increase the awareness of Members of Parliament and Senators on foreign interference and on election interference and on measures they can take to safeguard themselves and their online information.	New briefings will be made available to Parliamentarians and staff.
15	The Protocol should be maintained with the modifications noted in this report.	The Cabinet Directive remains in effect and, therefore, the Protocol will be in place for the next federal elections. Changes will be considered as indicated herein.
16	Public communications on the Protocol should emphasize the full range of activities that occur during the caretaker period, rather than being focused on the announcement by the Panel.	The Privy Council Office will develop a strategy to better communicate with Canadians about the Protocol and how it fits within the suite of measures to counter foreign interference and protect democratic institutions.

Table of Initiatives – Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions

Initiative	Lead
Communicating with Canadians About Foreign Interference and Protecting Canada's Democracy	
Undertake more robust and frequent communications with Canadians on foreign interference and efforts taken to protect Canadian democracy	PSC, RCMP, PCO
Adopting emerging communications best practices to strengthen the capacity of the Government of Canada to help combat disinformation based on the RESIST model	PSC, PCO
Use CSIS' upcoming Annual Report as an opportunity to bolster ongoing communications related to foreign interference with Canadians	CSIS, PCO, PSC
Explore expanding briefing mechanisms on foreign interference to provinces, territories, municipalities and Indigenous officials	PCO, PSC
Strengthen capacity of civil society partners to counter disinformation	PCO, PCH
Ensure Panel members (as part of the Critical Election Incident Public Protocol) are in a constant state of readiness to assume their Panel-related responsibilities	PCO
Effective Governance and Strong Legal Frameworks	
Creation of the National Counter-Foreign Interference Coordinator within Public Safety	PSC
Public consultations on the implementation of a Foreign Influence Transparency registry	PSC
Explore modernizing the *CSIS Act* to allow CSIS to better operate in the digital world by: • Effectively collecting and using digital data • Enabling intelligence sharing with non-government partners to help counter threats • Enabling intelligence collection and conducting activities to counter foreign threats not envisioned when *CSIS Act* came into force • Examining how the Public Order Emergency Commissions final report recommendations can information legislative changes to the *CSIS Act* • Developing a consultation and communications plan to address how Canadian interests and Charter rights will be respected while still enabling necessary legislative reform	PSC, CSIS, DOJ, PCO
Undertake analysis to determine if further amendments or new offences to facilitate the prosecution of foreign interference activities are required under the *Security of Information Act* and the *Criminal Code*	PSC, RCMP, PCO, DOJ, PPSC

Initiative	Lead
Examine whether potential amendments to the *Canada Elections Act* are required to counter foreign interference	PCO
Risks, Vulnerabilities, and Security	
Protect Canadians from harassment and intimidation, increase investigative capacity, and engage more proactive with at-risk communities through Budget 2023 investments	RCMP, PSC
Continue to engage with stakeholders in academia and other outreach programs to assess short and long-term impacts of foreign interference in Canada	PSC
Continue to update assessments as threat of foreign interference evolves	PSC, PCO, CSIS, CSE, RCMP
Undertake a comprehensive analysis of security and tools to align with the threat environment, including foreign interference, threats and protective measures available to Ministers, other Parliamentarians and senior officials	PSC, PCO
Develop further enhancements to the Plan to Protect Canada's Democracy, including: • An examination of making the Security and Intelligence Threats to Elections (SITE) Task Force a permanent entity with a mandate to conduct regular reporting on foreign interference activities • Reviewing the Cabinet Directive on the Critical Election Incident Public Protocol based on the recommendations suggested by Mr. Morris Rosenberg in his evaluation of the Protocol following the 2021 general elections	PCO, others
Engagement to Raise Awareness and Improve Resilience to Foreign Interference	
Strengthen the capacity of civil society partners to provide insight into Canada's information ecosystem, strengthen resilience and digital literacy of the government, industry, civil society and citizens	PCO, PCH, others
Establish a process for Ministers and senior officials, including Panel members, to engage with stakeholders and communities to seek views on best practices to mitigate the impact of foreign interference and disinformation on Canada's institutions	PSC, PCO
Continue working with Canadian partners to further the work accomplished through the Paris Call to ensure broad access to the most current expertise to protect Canada's electoral processes	PCO
Develop briefings for political party representatives in secure locations in Ottawa, with flexibility in scheduling that can adapt/react to urgent situations that may arise during election periods	PCO
Provide briefings to Members of Parliament and the Senate to increase awareness on the threat of foreign interference. This includes the development of a program for unclassified briefings for Parliamentarians and their staff on foreign interference including ways to protect themselves following their swearing-in and ongoing basis going forward	PCO

Proposed Membership of the Directors' Coordinating Group on Protecting Democracy

Participants	Team
Privy Council Office	
	Protecting Democracy Unit, Democratic Institutions
	Intergovernmental Affairs – Strategic Policy and Social Portfolio
	Policy, Protecting Democracy Unit, Democratic Institutions
	Research, Protecting Democracy Unit, Democratic Institutions
	Engagement and Operations, Protecting Democracy Unit, Democratic Institutions
PCO – Security and Intelligence	
PCO – Foreign Interference Task Force	
Canadian Heritage	
	Digital Citizen Initiative
	Strategic Policy and Horizontal Integration
Public Safety	
	Countering Radicalization to Violence
	Canada Centre for Community Engagement Prevention of Violence
PS – National Security Policy	

Participants	Team
Global Affairs Canada	
	Centre for International Digital Policy
	Task Force for Establishing a Centre for Democracy
	Office for Human Rights, Freedoms and Inclusions – Democracy, Inclusion and Religious Freedom
Innovation, Science and Economic Development Canada	
	S&T Policy Advice Directorate
	Privacy and Data Protection Policy Directorate
Treasury Board of Canada Secretariat	
	Policy Suite Integration Directorate
	Open Government and Portals
Department of Justice Canada	
	Policy Implementation Directorate
Crown-Indigenous Relations and Northern Affairs Canada	
	Strategic Policy Directorate
Indigenous Services Canada	
	Strategic Policy Directorate
Immigration, Refugees and Citizenship Canada	
	Integrated Policy and Programs
	Anti-Racism Task Force

Participants	Team
Environment and Climate Change Canada	
	Environmental Justice and GBA+
Health Canada	
	Policy Coordination and Planning Directorate
Public Health Agency of Canada	
	Public Health Security and Intelligence Division
Women and Gender Equality Canada	
	Strategic and Program Policy
Royal Canadian Mounted Police	
Canadian Security Intelligence Service	
Communications Security Establishment	

High Level Work Plan 2023-2024 – Protecting Canada's Decmocracy

Spring 2023

- **Setting up of the Directors' Coordinating Group on Protecting Democracy (May 2023)**
- Interim report from the Independent Special Rapporteur (May 23, 2023)
- Meeting of the Protecting Democratic Institutions Research Group (June 2023)
- Stock taking of whole-of-government measures to protect Canada's democracy

Summer 2023

- Meetings of the Protecting Democratic Institutions Research Group (July and September 2023)
- **Meeting of the Directors' Coordinating Group on Protecting Democracy (August 2023)**
- Stock taking of whole-of-government measures to protect Canada's democracy (cont.)
- Initiating drafting on "integrated govenrnment response" to protect Canada's democracy

Fall 2023

- Meeting of the Protecting Democratic Institutions Research Group (October 2023)
- Final report from the Independent Special Rapporteur (late October 2023)
- **Meeting of the Directors' Coordinating Group on Protecting Democracy (November 2023)**
- Potential Ministerial Roundtable on Foreign Interference (November 2023)
- Drafting government response to PROC and ETHI studies' reports (TBC)
- Propoposing "integrated govenrment response" to protect Canada's democracy
- Launch of a "Countering Disinformation Guidebook" for communications practitioners

Winter 2024

- Meeting of the Protecting Democratic Institutions Research Group (January 2024)
- **Meeting of the Directors' Coordinating Group on Protecting Democracy (February 2024)**
- Drafting budget asks, as appropriate