



Government  
of Canada

Gouvernement  
du Canada

TOP SECRET////CEO

# Protecting Canada's Democracy

## *General Election Security*

For Public Release



Government of Canada

Gouvernement du Canada

TOP SECRET//[ ]/CEO

# Challenge On An International Scale

ACCUEIL | INFO | INTERNATIONAL | POLITIQUE AMÉRICAINE

**L'interférence russe et le silence de Donald Trump**

Publié le mardi 20 février 2018



**Successfully Countering Russian Electoral Interference**

*15 Lessons Learned from the Macron Leaks*

GLOBAL

**Russia's Interference in the U.S. Election Was Just the Beginning**

Democracies across the West are vulnerable to foreign influence—and some are under attack.

SECURITY

Europe prepares cyber defenses to protect elections from Russian interference

REUTERS | JANUARY 13, 2017 9:23 PM

**Denmark to ramp up cyber security efforts - defence minister**

By Teis Jensen  
Reuters 21 November 2017

LE MONDE diplomatique

LE SUSPECT IDEAL DES ELITES OCCIDENTALES

**Ingérence russe, de l'obsession à la paranoïa**

décembre 2017, pages 12 et 15

**Australia forms task force to guard elections from cyber attacks**

June 09 2018 09:36 AM



**Les Occidentaux se coordonnent pour accuser la Russie de cyberattaques**

Chose inédite, les Etats-Unis, le Royaume-Uni, les Pays Bas et le Canada ont accusé la Russie d'être responsable de cyberattaques majeures.

**Elections 2019: Why India cannot underestimate the 'foreign hand'**

India has become more vulnerable to attacks. Only, the 'weapons of mass destruction' now are data and social media, which any nation can use to influence our elections.

**Election Interference in the Digital Age: Building Resilience to Cyber-Enabled Threats**

#EUProtects | 15 October 2018 to 16 October 2018

TOP SECRET///CEO

## Protecting 2019 General Election

- **January 30, 2019** - Announcement details range of measures, new and existing, to protect the General Election, including:
  - Security and Intelligence Threats to Elections (SITE) Task Force;
  - Creating the Digital Citizen Initiative;
  - Offering additional cyber technical advice, guidance, and services to political parties;
  - Offering classified threat briefings to key leadership in political parties; and
  - Engaging with social media platforms, including through the Canada Declaration for Electoral Integrity Online
- **June 11, 2019** - Cabinet Directive on the Critical Election Incident Public Protocol (the Protocol) published
- **May 2019** - Panel began meeting to prepare for election



Government of Canada

Gouvernement du Canada

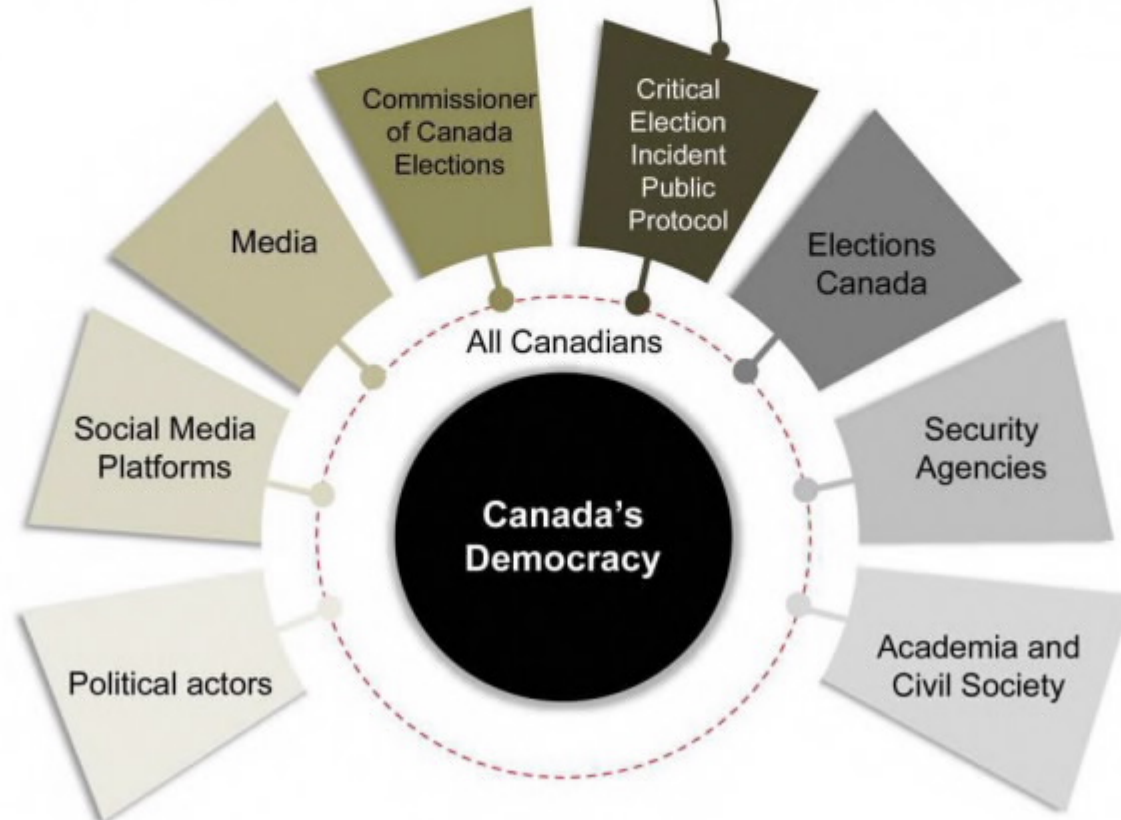
TOP SECRET/[redacted]/CEO

# Protecting Democracy Ecosystem

Protecting our democratic institutions from incidents that threaten our ability to have a free and fair election is a **shared responsibility** for all Canadians.

Panel of senior public servants:

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



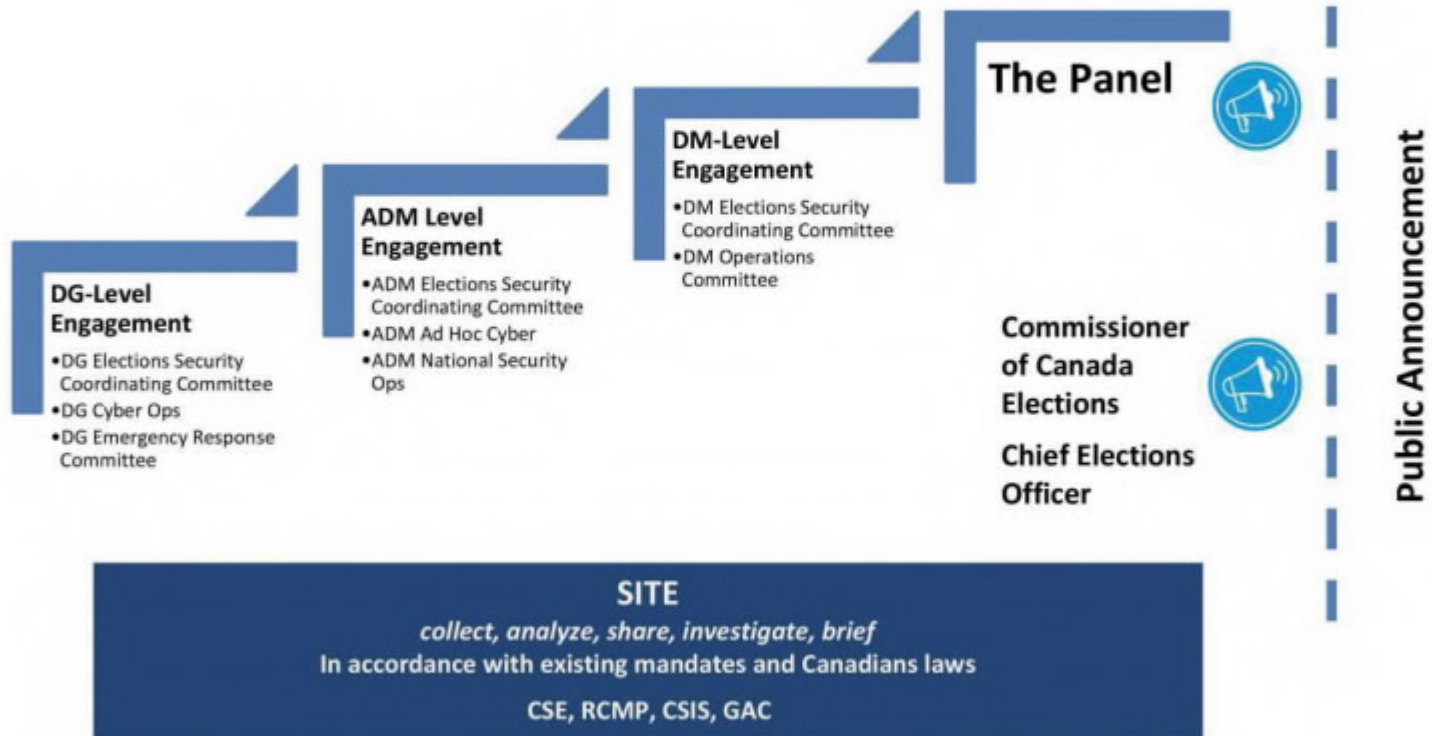


Government of Canada

Gouvernement du Canada

TOP SECRET///CEO

# Election Incident Response Architecture



For Public Release

# Critical Election Incident Public Protocol





---

**CRITICAL ELECTION INCIDENT PUBLIC PROTOCOL**

---

**AWARENESS**

---

THE GOVERNMENT OF CANADA BECOMES AWARE OF AN INTERFERENCE ATTEMPT IN THE ELECTION DURING THE WRIT PERIOD.



**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 Canada, Public Safety & Global Affairs Canada



**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 a press conference will be held



**PUBLIC ANNOUNCEMENT**

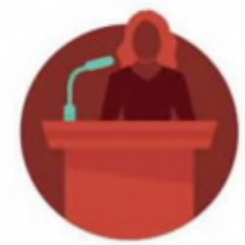
---

CANADIANS ARE INFORMED OF:

What is known about the incident

---

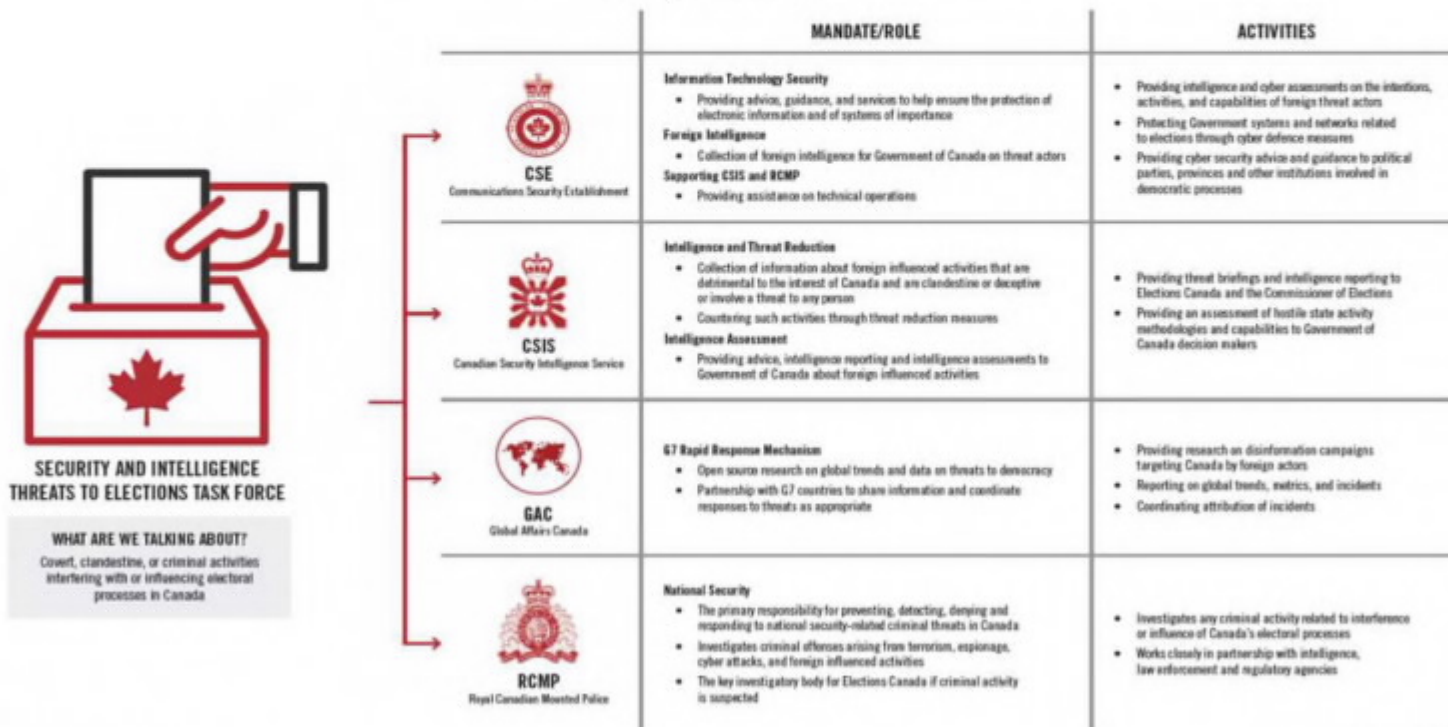
Any steps they should take to protect themselves



# Security and Intelligence Threats To Elections (SITE) Task Force

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Security and Intelligence Threats to Elections Task Force - Partner Roles Leading to Election 2019



**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

Government  
of CanadaGouvernement  
du CanadaTOP SECRET////CEO

## 2019 General Election – Outcomes

- No threats met the threshold and therefore none were reported to Canadians.
- Procedurally, an evaluation of the CEIPP was conducted and written by Mr. Jim Judd.
  - while the Panel did not intervene during the 2019 election, it was prepared to do so and decision-making about potential interventions did take place behind the scenes as appropriate;
  - the Panel included a range of public service experience and was supplemented where needed; and,
  - the Panel was appropriately supported and worked well with its principal partners (e.g., Elections Canada, security agencies).
- That does not mean no activity was observed. SITE conducted a review and produced a classified, after action report.



Government  
of CanadaGouvernement  
du CanadaTOP SECRET///CEO

## Canada's Ongoing Threat Environment

What do we know?

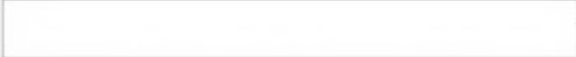
Who are the main threats?

What Happened During the US Election?

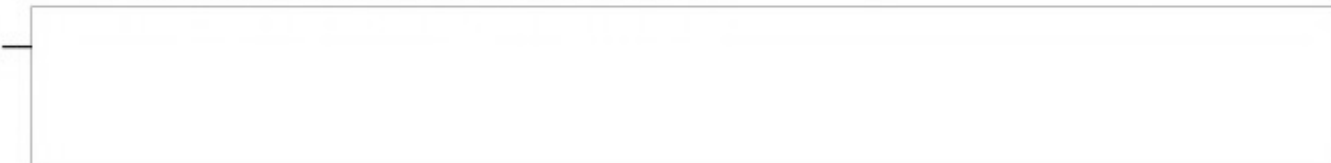
What can we expect and how is this complicated by the current pandemic?

Government  
of CanadaGouvernement  
du CanadaTOP SECRET////CEO

## What do we know

 foreign state actors over time have largely used human intelligence (HUMINT) in an effort to influence Canada's electoral processes.

- This is partly a result of the way that Canada conducts its elections (paper-based ballots, relatively robust federal financing laws, political party constitutional nomination processes)





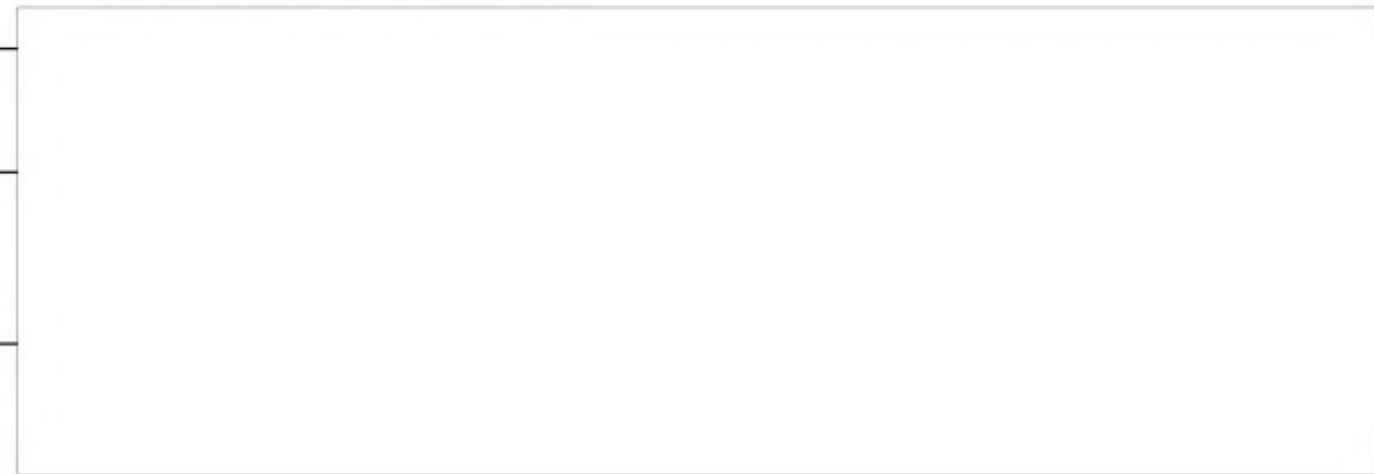
Government of Canada / Gouvernement du Canada

TOP SECRET/[redacted]/CEO

### Who are the main threats?

The People's Republic of China (PRC), [redacted] India and the Russian Federation, pose the top-tier foreign interference (FI) threats to Canada's democracy.

— These states believe that they can operate under certain conditions in Canada with relative impunity.



Government  
of CanadaGouvernement  
du CanadaTOP SECRET///CEO

## What Happened During the US Election?

- ~~In General, US Authorities at the Cyber-Security and Infrastructure Security Agency (CISA) have said the most recent US election was relatively free of foreign interference~~
- ~~This is credited to actions of the US Government in naming threats as they emerged~~
- ~~For example, the FBI made a public statement exposing Russian and Iranian attempts at election interference~~
  - ~~Of note, the Iranians attempted to pass themselves off as members of the Proud Boys, a far-right militia, but were quickly detected and attributed by Facebook and the US Intelligence Services~~

Government  
of CanadaGouvernement  
du CanadaTOP SECRET///CEO

## What can we expect?

Consistent with the 2019 Canadian Federal election, there is no evidence of a significant specific cyber threat to Canadian elections or electoral processes.

PRC ~~HUMINT foreign interference~~ threat activities have not shifted or diminished following the 2019 election.

~~PRC continues efforts to cultivate relationships with current MPs and influence their views on issues of strategic importance.~~

Foreign state actors are increasingly able to ~~clandestinely~~ leverage domestic political rhetoric in their online disinformation campaigns, making this type of interference more difficult to attribute.

COVID related social and political restrictions  may create additional opportunities for online disinformation campaigns.

Government  
of CanadaGouvernement  
du Canada

TOP SECRET/[ ]/CEO

## Next Steps

- The Panel of Five has begun meeting again
- The Election Security Coordination Committees are meeting to monitor and adapt to emerging trends and threats
  - PHAC now has representatives at all levels to coordinate response should adversaries use the current pandemic to augment their efforts
- SITE continues to track, assess, react and share intelligence on foreign interference activity by foreign state and non-state actors.

## Slide Notes

### Slide 2:

Attempts by foreign states and non-state actors to interfere in democratic and electoral processes are not a new threat.

In past 10 years, almost 40 nations have experienced manipulation and interference in their democratic institutions and processes to varying levels – this is a global challenge for democracies.

Canada is not immune to this threat - we need to prepare our citizens and systems to respond to this threat

Governments and citizens have to contend with these challenges and risks while respecting democratic rights and freedoms.

A 2017 public threat report from the Communications Security Establishment identified political parties and politicians, electoral activities, and the media as vulnerable to threats, but also noted that our system has inherent strengths built-in. For example, paper-based ballots cannot be “hacked”.

The 2019 update to this report reinforced that it was very likely that Canadian voters would encounter some form of cyber interference during the 2019 elections. Canadian political parties, their candidates and staff were also identified as likely to be targeted.

### Slide 3:

Against this backdrop, Canada put in place a number of measures to safeguard the 2019 elections.

On January 30, Ministers Gould, Goodale and Sajjan announced the whole-of-government plan to counter interference in the election. This Plan was developed in recognition of the global trend of foreign interference and disinformation in the democratic space and builds on the experiences of some of our key allies who experienced interference in their own elections (e.g. the U.S., France etc.).

Canada developed a plan structured around four pillars: enhancing citizen preparedness, improving organizational readiness, expecting social media platforms to act, and combatting foreign interference. This whole-of-government initiative brought together 10 different federal departments and agencies, as well as collaboration from Elections Canada and the Commissioner of Canada Elections.

A number of new measures were put in place to protect the 2019 General Election, including:

Leveraging the newly-established Security and Intelligence Threats to Elections Task Force (SITE) to improve awareness of foreign threats and support assessment and response. The SITE task force brings together our national security and intelligence partners at CSIS, RCMP, CSE and Global Affairs Canada.

Creating the Digital Citizen Initiative to expand citizen focussed programming on resilience against disinformation and supporting a healthy information ecosystem.

Offering additional cyber technical advice, guidance, and services to political parties to build their cyber hygiene and security.

Offering classified threat briefings to key leadership in political parties to promote situational awareness and encourage them to strengthen internal security practices and behaviours.

Engaging with digital platforms to encourage them to implement specific voluntary measures to increase transparency and combat the spread of disinformation, including signing the Canada Declaration for Electoral Integrity Online.

One of the signature initiatives is the establishment of the Critical Election Incident Public Protocol, which is a mechanism for communicating with Canadians during the writ period in a clear, transparent, and impartial manner about incidents that threaten the integrity of the election.

Work is ongoing to provide Government with options to protect democracy for GE44 and beyond

**Slide 4:**

The Protocol is one of many safeguards towards protecting the 2019 General Election, and part of a broader ecosystem of players that each have a role in protecting our democratic institutions. This is ultimately a shared responsibility.

The Protocol was put in place because there may be instances in which the government can detect concerted disinformation or interference campaigns that could have a significant impact on Canada's election, and needs to inform Canadians about these occurrences.



The Protocol was administered by a Panel of DMs who have vast experience in security, international affairs, law, public policy, and public safety, and who bring various considerations to the decision-making table.

The Panel met regularly, and was apprised of the threat environment on an ongoing basis during the writ period.

The Protocol was also established in a way that reflects the Caretaker Convention. The Caretaker Convention puts into practice the principle that the government is expected to “restrict itself” in matters of policy, spending and appointments during the election period, except where action is “urgent” and “in the national interest”.

The Protocol included provisions for: informing candidates, organizations or election officials if they have been the known target of an attack; briefing the group of senior public servants at the heart of the Protocol; informing the Prime Minister and other party leaders (or their designates) that a public announcement is planned; and notifying the public.

**Slide 5:**

Internal to GoC Ecosystem

Conscious of the various players in the ecosystem and of a requirement to coherently support the Panel, an Elections Security Architecture was established and has met regularly since 2019.

This system includes non-traditional partners and a requirement for the security community to engage these partners in new ways.

It feeds into the work of the Panel and is supported and underpinned by the work of the security community.

Internal to PCO this has necessitated close collaboration of S&I, DI and Comms.

**Slide 6:**

This slide outlines the step-by-step process of how the CEIPP works in practice, and how a public announcement would be made.

Step 1: Awareness

Government of Canada becomes aware of an election interference attempt in the election during the writ period.

Step 2. Sharing information

Heads of national security agencies brief the Critical Election Incident Response Panel.

**Step 3. Assessing threat**

If the Panel finds that there is a substantial threat to a free and fair election, they inform the Prime Minister, political party officials and Elections Canada of the incident and that an announcement will be made. None of these stakeholders can veto the decision to make an announcement.

**Step 4. Public announcement**

Canadians are informed of what is known about the incident; and any steps they should take to protect themselves.

**Slide 7:**

In August 2018, a focal point task force comprised of the CSE, CSIS, RCMP and Global Affairs Canada was activated.

To improve situational awareness of foreign threats to Canada's electoral processes and help Government assess and respond to threats

Ongoing engagement with foreign partners for lessons learned and trends

Partners operate within their existing mandates, and the task force provides an added layer of coordination.

**Slide 8:**

During the election, the threshold triggering the use of the CEIPP was limited to exceptional circumstances that could impair Canada's ability to have a free and fair election, whether based on a single incident or an accumulation of incidents.

Procedurally, evaluation of the CEIPP was conducted and written by Mr. Jim Judd, a former Canadian public servant, diplomat, and director of CSIS.

In terms of recommendations, the evaluation suggests that given the current minority Parliament, the lowest-risk option would be to re-implement the CEIPP and the Panel, as well as consider changing the CEIPP's timeframe to begin during the pre-writ period and strengthen ongoing monitoring of election interference issues. It also suggests continuing to provide cyber security guidance and access to classified intelligence for representatives from federal political parties beyond the electoral period, and evaluating outcomes from the Canada Declaration on Electoral Integrity Online.

During the 2019 election, no threats met the threshold and therefore none were reported to Canadians. That does not mean no activity was observed. SITE conducted a review and produced a classified, after action report, which feeds into the threat briefing.