

Foreign Election Interference - December 13, 2022

Table of contents

- Opening remarks
- Questions and answers
- Background information
 - Protecting Democracy Plan
 - Critical Election Incident Public Protocol and the Panel
 - High-level summary of GC/parliamentary public reports on threats to Canada's democratic process
 - *Election Modernization Act* (re: foreign election interference)
 - CEO and CCE Recommendations Report (re: foreign election interference)
 - The Digital Citizen Initiative and the Digital Citizen Contribution Program
 - The Paris Call for Trust and Security in Cyberspace

Opening remarks

The Honourable Dominic LeBlanc, P.C., K.C., M.P.
Minister of Intergovernmental Affairs, Infrastructure and Communities
To the House of Commons' Standing Committee on Procedure and House Affairs
Foreign Election Interference
Ottawa, ON
December 13, 2022

Check against delivery.

Madam Chair,

I wish to thank the Committee for inviting me here today.

And I would like to further thank the Committee for undertaking this important study. Ensuring that we work diligently to uphold the integrity of our elections is a critical part of keeping Canada's democratic processes legitimate, credible and trustworthy.

Let me be very clear: Foreign interference in Canada's elections is not acceptable. The study this Committee is undertaking plays a key role in improving our collective response to this issue and I look forward to your recommendations.

Our Government is committed to protecting Canada's democratic institutions from complex foreign interference threats, including disinformation, and strengthening Canadians' trust and participation in our democracy.

As a world leader in various economic, technological and research sectors, Canada has always been subject to foreign interference activities.

That is why, at a time when many democracies have faced foreign interference, it has been, and continues to be, important that Canada prepare itself for an evolving foreign interference threat.

And we have done this, with a wide array of ground-breaking measures to address complex threats.

Canada led the way among its international partners with the plan to protect Canada's democracy, announced in early 2019. This strategy has four distinct areas of action.

The first part of our plan focuses on preparedness and prevention by enhancing digital media literacy. Since 2020, we have reached more than 12 million Canadians, under the Digital Citizen Initiative, through projects helping people recognize fraud, disinformation, and manipulation when they see it online.

Canada also co-led the Paris Call for Trust and Security in Cyberspace on Principle 3 with Microsoft and the Alliance for Securing Democracy. Together, we held workshops with global experts and practitioners, culminating in a "good practice guide" to prevent election interference from malicious cyber activities. I understand this Committee may have an opportunity to learn more about this work at a future meeting.

The second part of our plan focuses on improving our government's ability to identify threats, emerging tactics, and vulnerabilities in our systems. As part of these measures, we worked for the first time to provide security clearance to representatives from each of Canada's major political parties to make sure that they were able to protect their organizations, their candidates, and - ultimately - Canadians.

We also created the Critical Election Incident Public Protocol to make sure that a non-partisan Panel was in place during the election period to inform Canadians quickly and effectively of any incidents that threatened Canada's ability to have a free and fair election.

And we established the Security and Intelligence Threats to Elections Task Force – which I know this Committee is familiar with - to support the work of the Panel.

Third, as a global challenge, combatting foreign interference requires international cooperation. In this regard, Canada also stepped up on the international stage by leading the creation of the G7 Rapid Response Mechanism which established a coordinated effort with our allies to respond to foreign threats to democracy. More recently, we announced enhanced support to renew and expand the mechanism, including the creation of a team focused on countering Russian disinformation and propaganda.

The fourth part of our plan combines education and action by increasing transparency, authenticity, and integrity on social media platforms. In May 2019, we released the Canada Declaration on Electoral Integrity Online. The Declaration was updated in 2021 and received the support of multiple platforms, including Microsoft, Facebook, Twitter, Google, TikTok, YouTube and LinkedIn.

The Declaration established a mutual understanding of the responsibilities of social media and other online platforms, and the concrete actions they can take, such as removing malicious abuse including fake accounts and coordinated inauthentic behaviour, and helping users understand when and why they are seeing political ads.

Traditional and digital media, civil society, academia, and governments all have a role to play—with different tools available—to develop a healthy information ecosystem and build resilience against disinformation meant to undermine democratic processes, manipulate opinion, and incite division.

In Canada, we are fortunate to have academic and civil society organizations, such as the Disinformation Project at Simon Fraser University, CIVIX and DisinfoWatch, that are engaged and forward-looking on foreign interference and on disinformation. We are continuing to work with partners to further equip academia and civil society with resources to increase awareness on how disinformation can circulate in cyberspace. Working with civil society and academia, as well as with provinces, territories, and global partners, will be key to ensuring we continue to adapt to ever-changing challenges.

As previously noted, our government has also invested in efforts to help better equip Canadians to navigate the information they see online. With the right tools, Canadians can be the best line of defence in efforts to fight the growing threat of disinformation.

Canada's plan acknowledges that foreign interference and disinformation challenges are too complex and relentless for any one actor to tackle alone.

In Canada and around the world, democracy and its institutions face a growing threat from actors seeking to weaken them and undermine citizens' trust in their government. Our government has, and continues to, prioritize efforts to defend Canadians and Canada's institutions from malicious actors.

I would be remiss if I did not mention the critical role Canada's electoral administration regime plays in ensuring the security of our electoral processes. Observers routinely commend Canada for the high levels of integrity in our federal elections. In no small part, this is a result of Canada's electoral law, including the amendments this government passed through the *Elections Modernization Act* which took into account the recommendations made by this Committee in earlier Parliaments. The result is that our law, including our political financing regime, is regarded as one of the most thorough in the world.

We are fortunate to be able to count on Elections Canada to be our independent, non-partisan administrator of federal elections in Canada. Its independence ensures that

elections are administered without influence from political parties or the government of the day.

By working together, across borders and sectors of society, our democracies will be more effective at combatting foreign interference and disinformation. It is a common challenge, but as we share experiences today, we are brought together with a common purpose to address it.

Reflecting this common challenge and the need to ensure a cohesive and coordinated approach to tackling the challenges of threats to our democracy, including disinformation, our government has also committed, in B2022, a modest investment to bring sustained central leadership to new and enhanced efforts that support and contribute to existing work.

Madam Chair, as a result of having undertaken all of these initiatives, Canada is recognized as having stepped up as a global leader in responding to election interference. And we are continuing to build on the measures we put in place because threats to democracy will continue to evolve and Canada must be ready.

Thank you and I would be happy to take your questions.

Questions and answers

Protecting Democracy Plan

Q1: Why does Canada need a plan to protect democracy?

The Government of Canada is committed to protecting our democratic institutions. Malicious foreign actors have demonstrated their intent to undermine democratic societies, electoral processes, sovereignty and our security by targeting us or some of our partners and allies. Indeed, as noted by the Canadian Security Establishment in its landmark publications on cyberthreats to Canada's democratic process, "democratic processes remain a popular target" and "the vast majority of cyber threat activity affecting the democratic processes can be attributed to state-sponsored cyber threat actors".

A healthy democracy is built on fair and free elections. Protecting our democracy matters to everyone: Canadians, political parties, governments and the private sector. We recognize that, in any election, Canada may face threats of foreign interference and we must be prepared.

Q2: How was the Plan to Protect Canada's Democracy developed?

Attempts by foreign actors to interfere in elections around the world have become commonplace. As a result, leading up to the October 2019 general election, the government announced the Plan to Protect Canada's Democracy (the Plan) to safeguard Canadian democratic institutions and processes.

Since 2019, elements of the Plan have undergone internal and independent assessments, which have confirmed their utility. We have built upon and improved these measures, continuing to ensure a government-wide approach to protecting our democratic institutions and processes.

Q3: Does the Plan to Protect Canada's Democracy cover threats and interference activities coming from within Canada? Have you considered foreign interference that is leveraging or working in concert with Canadians?

One of the hallmarks of democratic societies is freedom of expression, and open debate and dialogue, particularly during election campaigns. Such dialogue and engagement are cornerstones of a healthy democracy.

The Plan to Protect Canada's Democracy encompasses efforts to protect this dialogue and engagement, but also to protect our democratic processes and institutions from threats, be they foreign, homegrown, or a combination of the two.

Critical Election Incident Public Protocol and the Panel

Q4: Who are the members that compose the Panel?

The Panel is a group of senior civil servants who are working with the national security agencies within the agencies' existing mandates.

This Panel is 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.

Q5: How can you ensure the integrity of the Protocol when the members were hand-selected by the government in power?

It is not the members themselves that were hand-selected by the government in power, but rather the positions they occupy. The members of the Panel are all senior officials within Canada's professional and non-partisan public service.

I have great confidence in the integrity of Canada's non-partisan public service. It has been recognized as one of the most effective civil services in the world.

The Clerk of the Privy Council – the head of Canada's public service – and the other four of deputy ministers have unique national security, foreign affairs, democratic governance and legal expertise, as well as considerable experience. They bring that

perspective and experience to this role, with the utmost of care, integrity and due diligence. They are also able to call on their respective organizations to support them in their roles as required.

There is an independent review of the Protocol undertaken after each election, and a report with recommendations is provided to the Prime Minister and to the National Security and Intelligence Committee of Parliamentarians. An unclassified public version of this document is made available to the public.

Q6: What is the threshold for making an announcement?

The threshold is limited to addressing exceptional circumstances that could impair Canadians' ability to have a free and fair election, whether based on a single incident or a series of incidents. The context and details will matter in making the determination of whether the incident or incidents meet the threshold.

There are multiple considerations in making this judgment, including:

- the degree to which the incident or incidents undermine Canadians' ability to have a free and fair election,
- the potential of the incident or incidents to undermine the credibility of the election, and
- the degree of confidence officials have in the intelligence or information provided.

The threshold for making an announcement is high because the Panel is meant to be a last resort measure. That is why the decision rule is consensus and, without consensus, there is no announcement. The Panel should and will inform Canadians should there be a threat to Canadians' ability to have a free and fair election.

Q7: Based on the premise that a small number of ridings (and a small percentage of vote) could affect who forms government, do you think the threshold should be lower?

Each election is different, and one of the considerations for the Panel is the ability of the incident or incidents to affect the outcome of the election. Following the 2019 federal election, an independent evaluation of the Protocol was conducted by Jim Judd, a former Canadian public servant and director of CSIS who previously appeared before this Committee. He recommended in his evaluation that the threshold for an announcement remain unchanged. The high threshold helps to avoid the Panel becoming a frequent intervener in any general election.

The Protocol's mandate is very specific and circumscribed—a contingency mechanism to be used only in limited circumstances. As honourable members well know, democracy is rough and tumble – it is always going to be this way.

Q8: Some changes were made to the Protocol between the 2019 and the 2021 general elections. Could you explain why?

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; and
- 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.

Q9: One of the changes made to the Protocol between the 2019 and 2021 general elections is the removal of the reference to "foreign". Could you explain why?

The removal of the reference to "foreign" clarified the broad nature of interference. It was removed to clearly recognize that interference may not be limited to foreign actors. It may come from domestic actors, foreign actors and domestic actors working with foreign actors.

Additionally, as the Protocol recognizes, it may sometimes be difficult or impossible to ascertain who is behind the interference, particularly within the short time frame that the Protocol is in place.

Q10: Can the Prime Minister stop the Panel from making an announcement?

No, during the caretaker period when the Protocol is in place, no one, including the Prime Minister has the authority to veto any the Panel's decisions to inform Canadians.

Q11: Why were the Chief Electoral Officer or the Commissioner of Canada Elections not included in the Protocol?

The Protocol directive is clear that the Panel is to look at issues that are outside of Elections Canada's or the Commissioner of Canada Elections' (CCE) respective legislated mandates.

The Office of the Chief Electoral Officer (CEO) is Canada's independent, non-partisan election administrator that reports directly to Parliament and who is responsible for administering the *Canada Elections Act*. The CCE is responsible for ensuring compliance with and enforcement of the *Canada Elections Act*. This means that interference that impacts the administration of the election falls under their remit.

The changes to the Protocol that were made in 2021 recognize that there may be a need for the Panel to consult with the CEO if the circumstances warrant it, while respecting his independence. The Panel engaged with the CEO and the CCE during both the 2019 and 2021 election periods. The nature of this engagement was precautionary and focused on ensuring that there was a clear understanding of respective roles.

Q12: Do political parties have a role in the Protocol?

Political parties do not have a direct role in the operation of the Protocol. However, under the Plan to Protect Canada's Democracy, briefings are offered to all of the parties represented in the House of Commons to improve organizational readiness. Parties nominate key leaders involved with the national campaigns to receive security clearances. Classified briefings are offered on issues important to safeguarding our elections such as foreign interference, cyber security, violent extremism, and disinformation. They also serve as a valuable opportunity to facilitate information exchange amongst participants and learn about the mandates of the Security and Intelligence Threats to Elections (SITE) Task Force member agencies (CSE, CSIS, RCMP and GAC) and how they may act on different threats.

Q13: What is the Panel's responsibility if interference comes to light after the Caretaker period?

The Panel was created 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.

Response to, investigation of, and communications about potential election interference outside of this period would fall to various actors, including law enforcement agencies, depending on the specific nature of the incident.

Combatting disinformation

Q14: What is the Government of Canada doing to combat disinformation?

By becoming better informed about the information they see online, Canadians can be the best line of defence in efforts to fight disinformation.

Our Government established the Digital Citizen Initiative led by Heritage Canada in 2019 to contribute to these efforts. This initiative provides funding to civil society organizations undertaking research or citizen-focused activities, such as public awareness tools and online workshops, to help Canadians become more resilient and think critically about the information they consume online. Since 2020, under this initiative, more than 12 million Canadians have been reached through projects helping them recognize online fraud, disinformation, and manipulation.

In response to the growing disinformation threat, the Government is also providing funding for the Privy Council Office to coordinate, develop, and implement government-wide measures to combat disinformation and protect Canada's democracy.

Q15: How is the Government of Canada working with social media companies to combat disinformation?

Social media companies have a vital role to play in safeguarding our democratic institutions by reinforcing their terms and conditions, protecting against misrepresentation of political actors and removing fake accounts and inauthentic content.

The fourth pillar of Canada's Plan to Protect Democracy is Building a healthy information ecosystem. It combines education and action by increasing transparency, authenticity, and integrity on social media platforms. In May 2019, the Government of Canada released the Canada Declaration on Electoral Integrity Online with the support of numerous online platforms, including Microsoft, Facebook, Twitter and Google. The Declaration established a mutual understanding of the responsibilities of social media companies and the concrete actions they can take, such as removing fake accounts and inauthentic content and helping users understand when and why they are seeing political ads.

The Government of Canada is further working to ensure academia and civil society have resources to increase awareness on how social media platforms operate. These efforts will bring innovative solutions to better understand the information ecosystem, ensuring we continue to adapt to the ever-changing challenges caused by disinformation.

If needed: Twitter's new policy of not enforcing COVID-19 misinformation policy.

The Government of Canada is aware of Twitter's recent update to its content moderation policies, as a result of which users are no longer stopped from spreading false information about COVID-19 or vaccines. We are currently reviewing the impact of this policy and exploring ways to work with Twitter and other social media platforms to minimize the impacts on Canadians.

Q16: What is the Government of Canada asking of social media platforms?

Social media platforms have a role to play in our democratic life in helping Canadians understand where information is coming from, from whom, and for what purpose. The Government of Canada expects that social media companies will proactively apply the latest advancements and most effective tools from around the world to this task, as appropriate in the Canadian context.

Additionally, our Government is committed to putting in place a transparent and accountable regulatory framework for online safety in Canada that would apply to online communication service providers, including social media platforms. In working towards this commitment, from July to September 2021, the Government held a national consultation on a proposed approach to address harmful content online. In March 2022, an expert advisory group was established to provide the Honourable Pablo Rodriguez, Minister of Canadian Heritage, with advice on how to design the legislative and regulatory framework to address harmful content online for social media platforms and how to best incorporate the feedback from Canadians.

Q17: How is the Government of Canada strengthening communities that may be particularly at risk to disinformation, including remote and rural communities?

Canadians remain our best defense against disinformation. A critically thinking electorate is less likely to fall victim to disinformation in all its forms. Our role is to provide all Canadians, including those from remote and rural communities, with the tools they need to recognize disinformation when they encounter it.

The Digital Citizen Initiative, led by Canadian Heritage, provides funding for civic, news, and digital media literacy, ranging from awareness sessions and workshops to the development of learning materials. These projects reached more than 12 million Canadians from coast to coast to coast including youth, seniors, minority communities and official languages minority communities.

Yet, we can do more when it comes to engaging with communities at-risk of falling victims to disinformation. We look forward to receiving the committee's advice on this.

Trust

Q18: In light of the potential impacts of disinformation on our electoral integrity, how can we ensure Canadians' trust in our democratic institutions?

The Government of Canada's top priority is the protection of our democratic institutions. We are known for the robustness of our democratic system and institutions. That said, we must remain vigilant by monitoring the threat environment to identify new potential threats to our democratic system, and working to continually strengthen our institutions in the face of these threats.

Canadian elections rank as having a high degree of electoral integrity. This is in part a result of Canada's electoral laws, including our political financing regime which is regarded as one of the most rigorous and thorough in the world.

Additionally, we are fortunate to be able to count on Elections Canada to be our independent, non-partisan administrator of federal elections in Canada. Its independence ensures that elections are administered without influence from political parties or the government of the day. Where required, due to Elections Canada's mandate as the administrator of federal elections, the agency works with government organizations mandated to protect national security.

Q19: Do you think that increased transparency of the Panel's decision-making processes would increase Canadians' trust that the right measures are in place to protect our elections from foreign interference?

Under the Protocol, an independent evaluation of its implementation and effectiveness is required after every election. Through document review, interviews and research, a substantial review is completed and a classified report with findings and recommendations is presented to the Prime Minister and the National Security and Intelligence Committee of Parliamentarians (NSICOP).

Subsequent to that, an unclassified public version is made available which is the same report as is provided to the Prime Minister and the NSICOP except that some of the information with national security sensitivities has been removed. I believe that this provides a strong and appropriate level of transparency, and I encourage you to read the report done by Mr. James Judd following the 2019 General Election, if you have not already done so.

Specific incidents

Q20. Why did [specific alleged incident] not meet the threshold for the Panel to make an announcement?

As the honourable members know, it is important to note that threats and interference are not new. The Critical Election Incident Public Protocol and Panel was developed with some of the incidents that we saw around the world in mind.

The 2021 Canadian Security Intelligence Service (CSIS) report on threats to Canada's democratic process stated that the agency continues to observe steady, and in some cases increasing, clandestine and covert foreign interference activity by state actors, and that interference threats affect all orders of government and all facets of society (media, voters, political parties, etc.).

I am not a party to the Panel's deliberations including specific incidents. However, I can say that the Panel is mandated to consider the degree to which any particular incident or series of incidents could undermine Canadians' ability to have a free and fair election. This includes the source, whether the activity can be attributed, and whether the situation or threat is self correcting (for instance, traditional media or civil society are debunking the story).

I would reiterate that the threshold for an announcement is high and is meant to be a last resort.

Q21. Why was [specific person] not informed of an incident?

An announcement by the Panel has always been a last resort measure. Section 5.4 of the Cabinet Directive notes that Security and Intelligence Threats to Election (SITE) Task Force will, working within its members' respective mandates consider all options to effectively address the interference. Barring any national security or public security reasons, the agencies will inform the affected party.

Q22. Can you elaborate on the baseline threat or ongoing threats?

As has been set out in reports from and appearances at this Committee by CSE and CSIS, the agencies continue to observe steady, and in some cases increasing, clandestine and covert foreign interference activity by state actors, and those interference threats affect all orders of government and all facets of society. But there are ways to protect against these threats without intervening on all of them and bringing disruption into our election.

While there may not be a noticeable uptick of interference activities during an election, foreign interference can serve to undermine Canada's democratic institutions and the intimidation or coercion of communities in Canada by hostile state actors constitutes a threat to Canada's social cohesion, sovereignty, and national security.

Q23: Why did you choose not to tell Canadians in January 2022 when you found out about allegations of Chinese interference in the 2019 election?

The Government of Canada takes all allegations of foreign interference extremely seriously, and we are confident that our security agencies have the resources and capacity to investigate these allegations. They thoroughly investigate all allegations of foreign interference in our elections.

Furthermore, the Government of Canada is committed to enabling democratic accountability without sharing information that could compromise Canada's security or the safety of Canadians.

Foreign states and other actors routinely threaten a broad range of Canadian interests and Canada takes appropriate actions to mitigate risks and respond as required. Threats to these institutions are not new and we can expect to see them continue. It is rarely easy for us to get into great details when we talk about the threats we all work to address.

Q24: Could there have been individual ridings where foreign interference affected outcomes, even if the global assessment was that 2019 and 2021 elections were free and fair?

Each election is different, and one of the primary considerations for the Panel is the ability of the incidents to affect Canadians' ability to have a free and fair election. As stated by the Panel members themselves before this Committee, they did not observe any activities of foreign interference that met the threshold of affecting Canadians' ability to have a free and fair election.

Foreign states and other actors routinely threaten a broad range of Canadian interests and Canada takes appropriate actions to mitigate risks and respond as required. Threats to these institutions are not new and we can expect to see them continue. When she was before this Committee, CSIS representative Michelle Tessier noted that CSIS does observe activity of foreign interference or attempts of foreign interference, but not enough to have met the threshold of impacting the overall electoral integrity.

Based on the assessments provided by Canada's experts on the matter, I am confident that the elections were free and fair.

Other questions

Q25: What has been done to modernize our election laws in the face of new threats of foreign interference?

Canada's election laws have been strengthened and include amendments to specifically protect our elections from foreign interference. The *Elections Modernization Act*, (Bill C-76), came into force in June 2019 and prohibits a foreign person or entity from unduly influencing an elector to vote or refrain from voting, or to vote or refrain from voting for a particular candidate or registered party. It also prohibits third parties from using foreign funds for partisan advertising and activities, and prohibits foreign entities from spending on partisan advertising and activities during both the pre-election and election periods.

Q26: Will the Government implement the CEO's recommendations?

We have been carefully studying the recommendations of the Chief Electoral Officer and the Commissioner of Canada Elections. We will of course seriously consider any enhancements to the Act that would contribute to strengthening our resilience to foreign interference. We are also looking forward to your recommendations to that effect.

Background information

Protecting Democracy Plan

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.

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).

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.

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).

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).

Critical Election Incident Public Protocol and the Panel

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

As required in the Cabinet Directive, an evaluation of the Protocol, its implementation and its effectiveness in addressing threats to the 44th general election is currently underway by Mr. Morris Rosenberg. A former Canadian public servant, Mr. Rosenberg served as Deputy Minister of Foreign Affairs, Deputy Minister of Health Canada, and

Deputy Minister of Justice and Deputy Attorney General of Canada. This report will be presented to the Prime Minister and to the National Security and Intelligence Committee of Parliamentarians. A public version of the report will also be developed.

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:

- notification of the incident;
- what is known about the incident (as deemed appropriate); and
- 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.

High-level summary of GC/parliamentary public reports on threats to Canada's democratic process

In 2017, the Communications Security Establishment (CSE) produced a public [assessment of the cyber threats to Canada's democratic process](#). Updates to this report were published in the months leading up to the 2019 and 2021 general elections.

The [2019 update](#) found that foreign cyber interference targeting voters had become the most common type of cyber threat activity against democratic processes worldwide. The update also noted growing recognition that digital platforms are tools that can be used in both the promotion of a democratic marketplace of ideas and the propagation of disinformation.

The [2021 update](#) concluded that although Canada's democratic process was a lower-priority target for state-sponsored cyber actors relative to other countries, Canadian voters were "very likely" to encounter some form of foreign cyber interference (i.e., cyber threat activity by foreign actors or online foreign influence) ahead of, and during, that year's general election.

Meanwhile, the 2021 Canadian Security Intelligence Service (CSIS) [report on threats to Canada's democratic process](#) stated that the agency continues to observe steady, and

in some cases increasing, clandestine and covert foreign interference activity by state actors, and that interference threats affect all orders of government and all facets of society (media, voters, political parties, etc.). Nevertheless, Canada's democratic institutions and processes remain strong.

The Canadian Centre for Cyber Security's [National Cyber Threat Assessment 2023-2024](#) identified five themes to anticipate in the next two years: (1) ransomware is a persistent threat to Canadian organizations, and the most disruptive form of cybercrime facing Canadians; (2) critical infrastructure is increasingly at risk from cyber threat activity; (3) state-sponsored cyber threat activity, especially programs of China, Russia, Iran and North Korea, is impacting Canadians; (4) cyber threat actors are attempting to influence Canadians by degrading trust in online spaces and exploiting social divisions through the use of misinformation, disinformation and malinformation; and, (5) disruptive technologies bring new opportunities and threats.

A [Government Response to the December 18, 2020 motion on Foreign Interference](#) was tabled in the House of Commons. The response provided a review of the breadth and scope of foreign interference in Canada. It acknowledged that the COVID-19 pandemic has accelerated foreign interference related trends by providing foreign threat actors with unique opportunities to pursue their hostile activities. It also identified measures taken by the Government of Canada to respond to and counter the threat of foreign interference, including investigations and monitoring, measures to protect against economic-based threats to national security, measures to protect our democratic institutions, strategies to reach out to Canadians, and ways the Government of Canada collaborates with like-minded states on this issue.

The National Security and Intelligence Committee of Parliamentarians (NSICOP) produced the [2019 annual report](#) that recommended that the Government of Canada develop a comprehensive strategy to counter foreign interference and build institutional and public resilience, and that the Government of Canada support this comprehensive strategy through sustained central leadership and coordination.

The subsequent NSICOP [2020 annual report](#) concluded that the threat from espionage and foreign interference is significant and continues to grow, and that China and Russia remain the primary culprits. The effects of espionage and foreign interference are the most significant long-term threats to Canada's sovereignty and prosperity.

Following the 2019 general election, former director of CSIS, James Judd released his [independent assessment](#) of the Critical Election Incident Public Protocol. Mr. Judd made a number of recommendations, including that the Protocol and the Panel continue to be in place for future elections, which were taken into consideration prior to the 2021 general election.

Global Affairs Canada's G7 Rapid Response Mechanism's [annual report for 2021](#) summarizes steps taken in Canada to safeguard the 2021 general election. The report also notes evolving trends in state-sponsored information manipulation activities, including foreign state actors' efforts to leverage divisive issues, social cleavages, key influencers, and proxy news sites, and their targeting of non-state bodies and forums at

sub-national levels. It also summarizes allies' efforts to protect their respective institutions and electoral processes from foreign interference.

The Media Ecosystem Observatory's [report on the Canadian 2021 general election](#) found that although there was widespread misinformation during the election, its impact on the election overall was minimal. The report makes four recommendations to address existing vulnerabilities and build resilience against mis- and disinformation in Canada: to develop a community of practice for tackling misinformation; to engage in strategic countering of misinformation; to increase public resilience to misinformation, and to extend initiatives to limit and counter misinformation to non-election periods.

Election Modernization Act (re: foreign election interference)

The *Elections Modernization Act*, which came into force in June 2019, made changes to the *Canada Elections Act* intended to address the potential for foreign interference in Canada's electoral process. These updates included:

- A. New third party spending limits for partisan advertising, partisan activities, and election surveys and a new obligation that such spending come from a dedicated Canadian bank account¹
- B. Blanket prohibition on the use of foreign funds by third parties for advertising at all times and for partisan activities during the pre-election and election periods²
- C. Prohibition on knowingly selling advertisement space to a foreign person or entity to enable undue influence in the election process³
- D. Clarification on what is considered undue influence by foreign persons and entities, including foreign governments, agents, and mandataries of foreign governments⁴
- E. Clarification on the prohibition related to making false statements about the election process⁵
 - a. In February 2021, the Ontario Superior Court found s. 91(1) to be an unjustifiable limit on s. 2(b) of the *Charter* and struck the section down with immediate effect⁶
 - b. The Government of Canada did not appeal the decision, choosing instead to address the Court's concerns by adding a knowledge element to s. 91(1) in the *Budget Implementation Act*⁷ in June 2021
- F. Prohibition on the distribution of materials, in any form, with the intent to mislead the public as to the source of the material⁸

- G. Prohibition on the malicious use of a computer including to manipulate public opinion⁹
- H. New requirement that online platforms maintain a publicly available registry of partisan and election advertising for a period of two years following an election¹⁰

CEO and CCE Recommendations Report (re: foreign election interference)

Following a general election, the Chief Electoral Officer is required to provide a report that sets out recommendations for legislative amendments that, in his opinion, are desirable for the better administration of the Act. The report also includes recommendations from the Commissioner of Canada Elections related to the enforcement of the Act.

On June 7, 2022, the CEO tabled “[Meeting New Challenges: Recommendations from the Chief Electoral Officer of Canada following the 43rd and 44th General Elections](#)”, which proposes 32 recommendations to the *Canada Elections Act* (CEA). Of the 32 recommendations, six expressly focus on protecting Canada’s electoral process from foreign interference:

- A. Require third parties that wish to use their own funds to provide audited financial statements to EC that show that no more than 10% of their revenue comes from contributions; and require that all other third parties¹¹ incur expenses only from a separate account established for regulated expense purposes, and identify the contributors, who must be individual Canadian citizens or permanent residents (Recommendation 2.3.1)
- B. Prohibit (foreign and domestic) person or entities from knowingly making false statements about the voting process, including about voting and counting procedures, in order to disrupt the conduct of the election or to undermine the legitimacy of the election or its results (Recommendation 4.1.1)
- C. Extend the prohibitions against foreign interference¹² to the pre-election period, and extend the prohibition against misleading publications that falsely claim to be by an election worker, political party, leadership contestant, nomination contestant or candidate to all times¹³ (Recommendation 4.2.1)
- D. Broaden the scope of the unauthorized use of a computer offence¹⁴ to include acting fraudulently with the intention of disrupting the conduct of the election or undermining the legitimacy of the election or its results (Recommendation 4.2.2)
- E. Require that online platforms (redefined by Recommendation 5.1.2) publish their policies on the administration of paid electoral communications and on user accounts during the pre- and election periods, and on addressing (paid or unpaid) content that misleads electors about voting methods, timing and

locations or that inaccurately depicts election-related procedures during election periods (Recommendation 5.1.1)

- F. Amend the definition of “online platform” to extend beyond only those that sell advertising space and eliminate the threshold requirement for digital ad registries¹⁵ (Recommendation 5.1.2)

Of the 22 recommendations put forth by the Commissioner of Canada Elections (CCE), three relate, to varying degrees, to protecting Canada’s electoral process from foreign interference:

- G. Add a new provision that provides that the powers and duties of the CCE may also be exercised or performed in respect of a conspiracy, attempt, accessory after the fact, and counselling in relation to a violation or offence that is not committed (Recommendation 1.3)
- H. Require that the contact information of the person who authorized the publication of the message also be included in the online ad registry, and require political entities and third parties to take reasonable steps to ensure that the online platform they use to publish advertising is compliant with *Canada Elections Act* provisions (Recommendations 1.5.1 and 1.5.2)
- I. Clarify and align definitions related to undue influence and foreign corporations or foreign entities (Recommendation 2.2)

The Digital Citizen Initiative and the 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 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 open calls

In 2020, DCCP funded public awareness tools and online workshops to help Canadians increase their resilience and be critical of misinformation about COVID-19. More than \$3.5 million was allocated to ten organizations supporting citizens to think critically about the health information they find online, to identify mis- and disinformation, and limit the impact of racist and/or misleading online content relating to COVID-19.

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 research 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 funds research that aims 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 behavioral and psychological underpinnings of the spread of disinformation and harmful content.

The Paris Call for Trust and Security in Cyberspace

In November 2018, French President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace (Paris Call) with a goal of combatting new cyberspace threats that endanger citizens, and critical network infrastructure. The Paris Call calls on states, the private sector, and organizations in civil society to work together to enhance security in cyberspace, fight disinformation, and address new threats that emerge. Ultimately, the Paris Call provides a platform for these groups to exchange information and good practices on several aspects related to foreign electoral interference. This call marks the largest voluntary multi-stakeholder cybersecurity agreement having been endorsed by over 1,100 international entities, nearly 75 Governments, 350 international, civil society and public sector organizations, and more than 600 private sector actors.

The Paris Call outlines nine principles: (1) increase prevention against and resilience to malicious online activity; (2) protect the accessibility and integrity on the Internet; (3) cooperate in order to prevent interference in electoral processes; (4) work together to combat intellectual property violations via the Internet; (5) prevent the proliferation of malicious online programs and techniques; (6) improve the security of digital products and services; (7) enhance collective cyber hygiene; (8) clamp down on online mercenary activities and offensive action by non-state actors; (9) work together to strengthen the relevant international standards.

Prime Minister Trudeau publicly pledged Canada's support for the Paris Call in November 2018. In September 2019, Microsoft approached Canada to consider co-leading initiatives outlined by Principle 3, namely the commitment to *cooperate to prevent interference in electoral processes*, along with the German Marshall Fund's

Alliance for Securing Democracy (ASD) who signed on in November 2019. ASD is a non-partisan advocacy group that works to defend and deter foreign state interference. The resulting partnership between Canada, Microsoft, and ASD was announced by Minister LeBlanc alongside Brad Smith, President of Microsoft, and Laura Rosenberger, Director of ASD, in May 2020.

Paris Call workshops

In March 2020, the Government of Canada, Microsoft and ASD hosted six workshops on preventing foreign interference involving Canadian and international partners.

The workshops focussed on (1) effective information sharing, (2) defining foreign interference, (3) countering election interference during a pandemic, (4) countering and responding to disinformation, (5) protecting election infrastructure (6) building resilience. The goals of these workshops were to: (1) learn about best practices around the world, (2) highlight key observations from experts, (3) identify concrete next steps, (4) learn how the Government of Canada can better combat election interference.

PCO-DI convened nearly 34 leaders from various civil society organizations, academic spaces, and government departments to participate in these workshops.

Key takeaways from workshops

- Workshop 1: Improving multi-stakeholder information sharing, focussed on assessing vulnerable parts of the electoral cycle, and emphasized the need to foster intra-governmental coordination.
- Workshop 2: Foreign Interference versus Acceptable Nation-State influence, analyzed key terms that should be included in defining foreign interference. This included and considered the scope and framing of definitions that apply to a full range of threat actors and vectors.
- Workshop 3: Countering election interference in a pandemic environment, emphasized the need to balance competing priorities to ensure that cybersecurity is not sidelined because of pandemic-related issues.
- Workshop 4: Mitigation and Response: focussed on combatting disinformation.
- Workshop 5: Countering the Threat of Interference in Election Infrastructure, spoke to the benefits of keeping voting technology up to date.
- Workshop 6: Understanding and Building Community Resilience to Counter the Threat of Election Interference; sought to invest resources in supporting and empowering trusted speakers, and ensuring proactivity in the information environment.

Multi-Stakeholder Insights: A Compendium on Countering Election Interference

- Following the completion of the workshops, the three partners released the insights gleaned through these workshops the form of a compendium entitled *Multi-Stakeholder Insights: A Compendium on Countering Election Interference*. The compendium is a collection of key observations from leading Canadian and international partners in government, industry and civil society aimed at countering election interference.

Endnotes

Endnote 1

Summary, *Elections Modernization Act*.

Endnote 2

Section 349.02, *Canada Elections Act*.

Endnote 3

Section 282.4(5), *Canada Elections Act*.

Endnote 4

Section 282.4(1), 282.4(2) *Canada Elections Act*.

Endnote 5

Sections 91-92, *Canada Elections Act*.

Endnote 6

Canadian Constitution Foundation v. Canada (AG), 2021 ONSC 1224.

Endnote 7

Section 361, *Budget Implementation Act 2021*.

Endnote 8

Section 481(1), *Canada Elections Act*.

Endnote 9

Section 482(1), *Canada Elections Act*.

Endnote 10

Section 352.1(2), *Canada Elections Act*.

Endnote 11

That are not individuals.

Endnote 12

Section 282.4 of the CEA.

Endnote 13

Section 481 of the CEA.

Endnote 14

Section 482 of the CEA.

Endnote 15

Section 325.1 of the CEA.