For Official Use Only
Limited Distribution

[redacted]

Election Incident Response Playbook

1.0 INTRODUCTION

There is no greater responsibility for the federal government than the protection and preservation of Canada's democratic institutions and practices. Threat and risk assessments, as well as the experience of key international allies, indicate that Canada's 2019 General Election (GE 2019) is vulnerable to interference in a number of areas.

Building on the information sharing models established by relevant federal response plans, the Election Incident Response Playbook (the Playbook) ensures an integrated, effective, and well-coordinated response, across government, to an incident or threat that could potentially threaten the security and/or the integrity of GE 2019.

1.1 Purpose

The purpose of the Playbook is to strengthen coordination and to facilitate information sharing between the security and intelligence (S&I) community and those federal government departments and agencies with mandates and responsibilities for administering GE 2019 and ensuring compliance with the *Canada Elections Act*.

1.2 Scope

The Canadian S&I community's response to any national security incident requires collaboration across numerous areas of expertise and responsibility to provide a comprehensive response. Each federal department and agency is guided by their respective response plans in accordance with their mandates and authorities. Relevant federal response plans, senior coordinating committees, and relevant senior officials provide the overarching direction.

The Playbook is not intended to replace the existing operational models established by other federal response plans, including the *Government of Canada Cyber Security Event Management Plan*, the *Federal Terrorism Response Plan* (FTRP) and the *Federal Emergency Response Plan* (FERP). Nor does the Playbook supersede departmental and agency-specific response plans and resources that may be used during a national security incident. The Playbook establishes an expanded information sharing and incident management framework that integrates departments and agencies beyond the S&I community that have mandates related to the administration and protection of GE 2019.

2.0 STRUCTURES

2.1 Primary Departments/Agencies

- **Canadian Security Intelligence Service** (CSIS) is responsible for investigating activities suspected of constituting threats to the security of Canada and reporting on these threats to the Government of Canada. If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures Canada, to reduce the threat.

- **Commissioner of Canada Elections** (CCE) is the independent officer responsible for ensuring compliance with and enforcement of the *Canada Elections Act*. During the writ period, the Commissioner and his staff work to ensure that political entities, third-party organizations, stakeholder groups and other individuals engaged in the electoral process do so in compliance with the rules.

- **Communications Security Establishment** (CSE) is responsible for acquiring and using information from the global information infrastructure for the purpose of providing foreign intelligence in accordance with Government of Canada intelligence priorities. CSE also provides technical and operational assistance to federal law enforcement and security agencies in the performance of their duties.
    - Within CSE, the **Canadian Centre for Cyber Security** (CCCS) provides advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada.

- **Elections Canada** (EC) is responsible for administering general elections, by-elections, referenda, and other aspects of the electoral process.

- **Global Affairs Canada** (GAC) manages Canada's diplomatic relations, provides consular services to Canadians overseas, promotes the country's international trade and leads Canada's international and humanitarian assistance.
    - Within GAC, the **G7 Rapid Response Mechanism** (RRM) is an initiative to strengthen coordination across the G7 in identifying, preventing and responding to threats to G7 democracies. This includes a capacity for social media analytics to monitor foreign threats in the digital landscape.

- **Privy Council Office – Democratic Institutions** (PCO-DI) is responsible for developing policy and coordinating efforts across government in support of the mandate of the Minister of Democratic Institutions and supporting the Minister's efforts in leading the Government of Canada's efforts to defend the Canadian electoral process from cyber threats.

- **Privy Council Office – Security & Intelligence** (PCO-S&I) is responsible for advising the National Security and Intelligence Advisor to the Prime Minister (NSIA) on national

security and intelligence operations and policy, ensures the effective coordination of the S&I community through the coordination of Deputy Minister level committees on national security and supports the Cabinet in managing national security and intelligence activities.

- **Public Safety Canada** (PS) supports coordination and information sharing activities as required in relation to significant events and situations necessitating a national response. This includes providing the coordination function as outlined in the FTRP and the Secretariat function to Assistant Deputy Ministers' Committee on National Security Operations.
    - Within PS, the **Government Operations Centre** (GOC) provides an all-hazards integrated federal emergency response to events (potential or actual, natural or human-induced, accidental or intentional) of national interest. They ensure strategic situational awareness and high-level coordination for consequence management and associated planning.

- **Royal Canadian Mounted Police** (RCMP) has primary responsibility for the investigation, prevention, and prosecution of criminal activities related to national security. The RCMP may be the police of local jurisdiction, or may be asked to provide support by local law enforcement.

2.2 Interdepartmental Coordination

- **Security and Intelligence Threats to the Election (SITE) Task Force** is a coordination body comprised of CSE, CSIS, GAC and the RCMP, tasked with providing intelligence on threats to GE 2019. Each agency leverages its mandate to bring to the table unique information on threats to Canadian security in order to effectively share intelligence, contextualize the threats based on information received through a range of partnerships, and review together any potential actions to mitigate threats directed at Canadian democratic institutions.

2.3 Committee Structure

Political Level

- The **Incident Response Group** (IRG) is a dedicated, emergency response committee at the political-level that will convene in the event of a domestic or international incident which may have major implications for Canada. Led by the Prime Minister, the IRG brings together relevant ministers and senior government leadership to coordinate a prompt federal response and make fast, effective decisions to keep Canadians safe and secure, at home and abroad. The core membership of the IRG includes: the Prime Minister (Chair), the Minister of Public Safety and Emergency Preparedness, the Minister of Foreign Affairs, the Minister of National Defence, the Minister of Intergovernmental Affairs and Northern Affairs and Internal Trade. Other ministers are invited as required (e.g. Health, Indigenous Services, Transport, Natural Resources).

For Official Use Only
Limited Distribution

GE 2019 Security Structure

- **Critical Election Incident Public Protocol Panel** (the Panel) establishes a clear, transparent, and non-partisan process to inform Canadians if there is a threat to the integrity of GE 2019. The Panel consists of five principals: the Clerk of the Privy Council; the NSIA; the Deputy Minister of Justice and Deputy Attorney General (DMJDAG); the Deputy Minister of PS (DMPS); and the Deputy Minister of Foreign Affairs Canada (DMGAC). This committee has a mandate only during the writ period.
- **Deputy Ministers' Elections Security Coordinating Committee** (DM ESCC) provides direction for ensuring interagency collaboration and coordination and system preparedness as it relates to electoral security. Composition of DM ESSC is: PCO-S&I, PCO-DI, PS, EC, CSIS, CSE, and CCE.
- **Assistant Deputy Ministers' Electoral Security Coordinating Committee** (ADM ESCC) provides direction for ensuring interagency collaboration and coordination and system preparedness as it relates to electoral security. Composition of Committee is: PCO-S&I, PCO-DI, PCO Communications, PS, EC, CSIS, CSE, and the Office of the CCE.
- **Director General Electoral Security Coordinating Committee** (DG ESCC) provides direction for ensuring collaboration, coordination, and system preparedness as it relates to electoral security. Composition: PCO-S&I, PCO-DI, PS, EC, CSIS, CSE, the RCMP, GAC and the Office of the CCE.

National Security Operations

- **Deputy Ministers' Committee on Operational Coordination** (DMOC) provides direction and ensures collective action to a national security incident. Composition of the Committee is: PCO (NSIA (Chair), FDPA), Department of National Defence (DND) and the Canadian Armed Forces (CAF), CSIS, RCMP, GAC, CSE, Canada Border Services Agency (CBSA), PS and Immigration, Refugees and Citizenship Canada (IRCC).
- **Assistant Deputy Ministers' Committee on National Security Operations** (ADM NS OPS) facilitates decision-making during national security incidents. The committee will coordinate security and intelligence federal activity and provide situational awareness and can integrate other key partners as needed to facilitate a response. Composition of Committee is: PCO, PS, RCMP, CSIS, CBSA, GAC, IRCC, DND and CAF, CSE, Financial Transactions and Reports Analysis Centre of Canada, Integrated Terrorism Assessment Centre and Transport Canada.
- **Director General Cyber Operations Committee** (DG Cyber Ops) ensure that the federal response to cyber threats and incidents of national interest is coordinated and that national operational policy issues are advanced. DG Cyber Ops is the operational sub-group of the DG Cyber Committee. DG Cyber Operations is differentiated from that group by its operational focus and reduced membership. Participation in DG Cyber Ops is limited to those organizations with mandated operational cyber security functions. Composition is: the CCCS, PCO-S&I, CSIS, GAC, Treasury Board Secretariat, the RCMP, DND and CAF, PS/GOC.

3.0 INCIDENT MANAGEMENT AND INFORMATION SHARING

3.1 Threat Detection and Identification

Information on a national security threat or incident that could potentially threaten the security and/or the integrity of GE 2019 could come from a variety of sources. These include the public, social media, foreign allies, and/or information provided by partners within the S&I community.

3.1.1 Incident Type

Threats against GE 2019 are organized by incident type or threat vector into three broad categories. It should be noted, however, that an incident may fall across more than one of the categories listed below.

1. Cyber – e.g. interference activity enabled by cyber tools.

2. Terrorism – e.g. physical attack on voters, politicians, or elections infrastructure.

3. Foreign Interference - e.g. clandestine, deceptive or threatening manipulation by foreign powers. The foreign may be working through or with domestic actors to interfere in the election process.

3.1.2 Targets

Threats may also be organized by target or victim into 3 categories. Threats may target more than one of the categories listed below.

1. Elections – e.g. tampering with election results; stealing voter databases.

2. Voters – e.g. preventing citizens from registering; preventing voters from voting; voter manipulation and disinformation.

3. Political parties and politicians – e.g. violence, espionage, or cyber-espionage against a political target; blackmailing a political target; embarrassing or discrediting a political target; stealing or manipulating party databases.

It should be noted that incidents related to foreign interference can span the cyber and human categories and can be aimed at more than one target. Further, hostile state activities are often complex and part of ongoing campaigns where effects can be cumulative.

3.2 Enhanced Coordination and Information Sharing

For the purposes of protecting the security and/or the integrity of GE 2019, the developed structures and committees are designed to enhance coordination for incident management and information sharing by integrating departments and agencies, beyond the S&I community, that have mandates related to the administration and protection of GE 2019. This is intended to ensure information sharing flows both within the S&I community to facilitate a response and also into the GE 2019 Security Structure (DG, ADM & DM ESCC and the Panel) to ensure coordination and appropriate escalation.

To the greatest extent possible, departments and agencies will share timely, accurate and reliable information related to specific incidents. While some information may be compartmentalized as part of an operational investigation or due to the sensitivity of the source or situation, departments and agencies with relevant information should ensure that the applicable departments and agencies have situational awareness so that actions are coordinated.

The sharing of information must be done in a manner that respects Canadian privacy legislation, departmental mandates, the *Charter of Rights and Freedoms*, caveats, originator controls, and the integrity of ongoing investigations. Information sharing authorities are set out in relevant Acts (including *the Security of Canada Information Sharing Act*), memoranda of understanding and the spectrum of applicable Ministerial Direction.

When sharing information as part of a response to a national security incident, the following items should be addressed:

- Level of classification and appropriate caveats;
- Target audience/distribution list;
- Guidance for action, if applicable;
- Need to know; and
- Protection of sensitive or operationally critical information.

In order to ensure information sharing during the writ period, the following cadence of meetings and information products will be established:

- DG ESCC will meet (virtually or in person) Monday, Wednesday and Friday;
- ADM ESCC will meet jointly with DG ESSC on Fridays;
- A daily overview of the election and any incidents/events affecting its conduct will be distributed via the GOC;
- The Panel will meet regularly (e.g. weekly) and as required in the event of an incident.

3.3 Departmental and Agency Responses

The tactical/operational response of relevant departments and agencies will be managed in accordance with its standard operational procedures and includes standard interdepartmental coordination, information sharing, and deconfliction (i.e. the Playbook does not constitute a new operational procedure and is not intended to replace existing structures). Responses of departments and agencies to the aforementioned incident types (cyber, terrorism or foreign

interference) may occur in accordance with the underlying nature of the event. Whether it be individually or a combination of:

1. Criminal activity.
2. National security.
3. Administration of the elections / protection of democratic institutions.

3.4 Standard Coordination

Should an incident (cyber, terrorism or foreign interference) require a more coordinated federal response, information will be escalated to the relevant senior-level (ADM or DM) committees. If an incident or event is deemed to be serious enough, a decision may be made to implement the relevant federal response plan and structures. For example, a response to a serious cyber-related incident would be coordinated via the *Government of Canada Cyber Security Event Management Plan*, with relevant organizations providing direction and guidance on how to proceed with event response. A cyber event at this level would also trigger the Treasury Board Cyber Security Communications Framework. Similarly, in the event of a terrorism-related incident, the response would be coordinated through the FTRP, including its related communications plan.

In the event of severe or catastrophic events that affect multiple government institutions, confidence in government or other aspects of the national interest, response plans will shift to the FERP governance structure, coordinated by the GOC, in order to ensure the harmonization of federal response efforts.

4.0 ROLE OF THE PANEL

4.1 Pre-Writ Period

Incidents that occur prior to the writ period will be addressed by regular Government of Canada operations and relevant response plans.

4.2 Writ Period - Critical Election Incident Public Protocol Panel of Five

If an incident occurs during the writ period that does not fall within Elections Canada's area of responsibility (i.e., the administration of the election) the Critical Election Incident Public Protocol (CEIPP) may be invoked.

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

4.2.1 Threshold

The threshold for the Panel's intervention during the election will be very high. It will be limited to addressing exceptional circumstances that could impair Canada's ability to have a free and fair election.

As such, potential considerations could include:

- the potential impact of the incident on the national interest;
- the degree to which the incident undermines Canadians' democratic rights;
- the potential of the incident to undermine the credibility of the election; and
- the degree of confidence officials have in the intelligence.

The Prime Minister cannot veto the decision by the Panel to notify Canadians.

4.2.2 Public Engagement and Public Announcements

The Protocol includes a process whereby if the heads of a national security agency (i.e., CSE, CSIS, RCMP or GAC) become aware of interference in the 2019 election, they will inform the affected party (e.g. a specific political party or politician) of the incident directly unless there is some overriding national security or public safety reason not to do so.

Should the Panel decide that an incident meets the threshold for a public announcement, the Clerk of the Privy Council will direct the relevant national security agency head(s) to hold a press conference to notify Canadians of the incident(s). The announcement would focus solely on notification of the attack, what is known about the attack (as deemed appropriate), and/or steps Canadians should take to protect themselves (e.g., ensure that they are well informed; cyber hygiene), if required. The announcement will not address attribution (i.e. the

source of the attack) and will not include classified information. Further, while the announcement might affirm that steps are being taken to address the situation, it would not necessarily provide details of those actions.