

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

2022 Inventory of Current, Planned, and Potential Activities

Prior to both the 2019 and 2021 elections and in response to new threats, successful whole of government efforts were undertaken to [safeguard federal elections](#).

The nature of the threats continue to evolve. In response to both the changing environment and new mandate letter commitments, PCO-Democratic Institutions has been directed to develop a framework for an **emerging protecting democracy agenda**.

A first step is to take stock of what government is currently doing, what is being proposed, and what ideas warrant further consideration. This may lead to assessing what a new joined up effort looks like in order to put forward a new whole of government initiative.

This is an initial exercise. Please **consider the scope broadly** and **recall the four pillars of the Plan to Protect Canada's democracy**: enhancing citizen preparedness, improving organizational readiness, combatting foreign interference, and building a healthy information ecosystem.

There is overlap between an emerging protecting democracy agenda and a focus on mis- and disinformation. As such, another approach to this inventory is to identify those activities – current, planned, or potential – that:

- focus on **detecting, correcting, and/or countering mis- and disinformation**; and/or
- are **upstream** of mis- and disinformation, meaning those aimed at decreasing the likelihood of information pollution occurring eg. efforts to increase citizen resilience, to support institutions and democracy, to work with or potentially regulate social media platforms; and/or
- are **downstream** of mis- and disinformation, meaning those aiming to deal with its effects eg. efforts to counter distrust, or breakdown in civic discourse, or radicalization.

This inventory will primarily capture activities focusing on the medium- and long-term, but consideration should be given to including activities that may be rapidly initiated or expanded for immediate action given recent events.

The current objective is to canvass widely, and with minimal burden, across government to consider the policies, programs, and strategic communications initiatives already underway, or that could be proposed, to protect and strengthen our democratic institutions, immediately and over the longer term.

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

2022 Inventory of Current, Planned, and Potential Activities

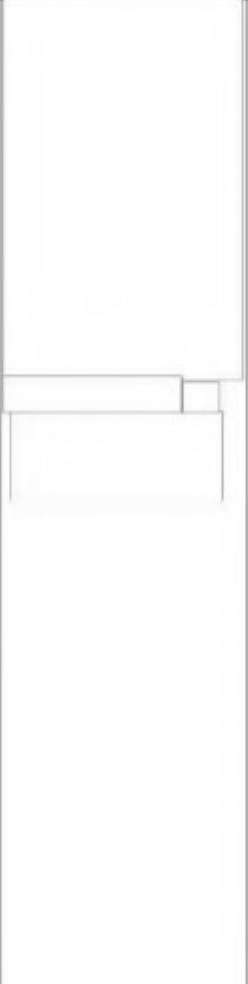
Department:	CSE, Cyber Centre
ADM level Contact name and title:	<i>(if multiple ADMs are responsible for the various activities described below, please either include all ADM names here, or separate your response into multiple templates so as to group them by ADM, whichever is easier)</i>

Activity: (Policy, Program, Monitoring, Communications) <i>Brief description of the activity, and how it contributes or could contribute to protecting and strengthening Canada's democracy and its democratic institutions</i> <i>Can the activity be rapidly initiated or expanded in response to the recently occurring events domestically, internationally?</i> <i>Provide links to publicly-available information, or to mandate letters or other direction-setting documents</i>	Status <i>Is the activity underway, proposed, or identified for further analysis and consideration?</i>	Funding <i>Is the activity funded, partially funded, or unfunded?</i>	Contacts	
			DG-level	Director or Analyst
Democratic Threat Analysis and Operational Coordination Democratic Threat Analysis and Operational Coordination supports critical infrastructure, including democratic institutions, in several ways including but not limited to:	<i>Discussion of CCCS resource and capacity limitations to provide electoral support.</i>			

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<ul style="list-style-type: none"> • Production, publication and dissemination of alerts/ advisories and cyber flashes related to threats and vulnerabilities in technology used in Canadian elections or by democratic institutions. It should be noted that with various activities in the electoral process either using electronic devices or being conducted on the internet, the threat surface is broader at the provincial/ territorial and municipal levels. • Incident handling, response and coordination activities related to a DI-related event or an incident impacting democratic institutions or processes. • Establishing named operations to support democratic institutions during key or high-profile events. To date, this has been limited to federal elections and the census. • Operational outreach, aggregation and sharing of technical, operational, and incident information impacting democratic institutions, from FVEY and international partners. • Providing subject matter expertise related to incident management and response at engagement forums specific to democratic institutions. 	<p><i>Discussion of CCCS resource and capacity limitations to provide electoral support.</i></p>			
---	--	--	--	--

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>Democratic Threat Analysis and Operational Coordination plays a pivotal role in two of the Cyber Centre strategic objectives pertaining to democratic institutions:</p> <ol style="list-style-type: none"> 1. Evolve Canada’s capacity to mitigate, prevent, detect, respond to cyber security incidents. 2. Help to safeguard Canada’s critical infrastructure and democratic institutions. 				
<p>CCCS Cyber Defensive Planning</p> <p>To address and mitigate identified and anticipated cyber threats against the 2019 Federal Election, the Cyber Centre leveraged its new defensive cyber planning group to develop a Strategic Mitigation Plan (SMP) describing the Cyber Centre strategy to address, reduce or eliminate foreign cyber threats and foreign cyber interference in Canada’s democratic process. More specifically for the 2019 Federal Election, planning included activities to address cyber threats to the election process, political parties, candidates and their staff, and voters. The campaign plan consolidated all CSE/Cyber Centre efforts to provide advice, direction and operational support to the 2019 Federal Election.</p>		<p><i>Discussion of CCCS resource and capacity limitations to provide electoral support.</i></p>		

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>The Strategic Mitigation Plan for Defending Democratic Institutions is an enduring plan that is in place for an extended period, and it will undergo an annual review to ensure content is accurate, relevant, and consistent with national priorities and Cyber Centre objectives. The 2019 campaign plan was the first and only campaign plan conducted in support of protecting democratic institutions. It was conducted with available resources at the time and has now concluded. Since then, the Cyber Centre has established SMPs and related Campaign Plans for other domains of national importance including cybercrime and critical infrastructure. Owing to the success and effectiveness of the defensive cyber planning function, resources are committed to these other areas of importance, leaving a capacity gap to continue the campaign planning process for defending democratic institutions.</p> <p>While a campaign plan is focused on a specific threat area, it should be noted that SMPs may have multiple campaign plans and that defending democratic institutions is a broad area that also includes provincial and municipal levels, summits and other events. Beyond the</p>				
---	--	--	--	--

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>planning requirement, resources would develop the subject matter expertise in the realm of democratic institutions, to continuously look forward at potential and emerging threats in this space and to continue engagement with stakeholders both domestic and internationally. Malicious cyber threat activity against democratic processes is predominantly conducted by state-sponsored threat actors with links to Russia, China, and Iran. Democratic processes, however, are also targeted by cybercriminals, hacktivists, and politically motivated actors. These actors utilize a wide array of tactics, techniques and procedures (TTPs) and also leverage commercial markets to seek out ready-to use cyber tools and to hire talent. The proliferation of these open-source methods to disrupt democratic processes increases the difficulty to identify, attribute, and defend against cyber threat activity more broadly.</p> <p>The Cyber Defensive Planning efforts can be linked to the following Cyber Centre strategic efforts:</p> <ul style="list-style-type: none"> Fortify Canada's key national systems of importance and confront state sponsored threats 				
--	--	--	--	--

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<ul style="list-style-type: none"> • Help to safeguard Canada's critical infrastructure and democratic institutions. 														
<p>Cyber Hotline - Federal Political Parties and Federal Ministers</p> <p>The CCCS provides a comprehensive 24/7 cyber services "Issue Response" to parliamentarians (Hotline) to help resolve problems or redirect Hotline requests to the appropriate responders. With political parties relying heavily on the Internet to organize and communicate with voters, and cyber threat actors targeting their websites, emails, social media accounts, networks and devices, the hotline enables timely response to suspected security breaches to limit associated damage. The hotline is offered to all registered federal political parties during an election period (and up to 30 days after the election date) and available to federal Ministers only outside of the election period.</p>	<p>This activity is currently underway.</p>	<table border="1"> <tr> <td data-bbox="1010 737 1255 797"></td> <td data-bbox="1255 737 1587 797"></td> </tr> <tr> <td data-bbox="1010 797 1255 829"></td> <td data-bbox="1255 797 1587 829"></td> </tr> <tr> <td data-bbox="1010 829 1255 1159"></td> <td data-bbox="1255 829 1587 1159"></td> </tr> </table>							<table border="1"> <tr> <td data-bbox="1255 472 1587 667"></td> <td data-bbox="1587 472 1791 667"></td> </tr> <tr> <td data-bbox="1255 667 1587 1256"></td> <td data-bbox="1587 667 1791 1256"></td> </tr> </table>					
<p>Update on Cyber Threats to Democratic Process Reports</p>	<p>This activity is currently underway.</p>													

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>Threats to Democratic Process reports are produced to highlight global trends in cyber threat activity against democratic processes and assess the threat to Canada.</p>									
<p>Cyber Security Advice and Guidance to Democratic Institutions</p> <p>CSE provides generic and tailored cyber security assistance, via technical guidance to democratic institutions, which addresses cyber threats, incident prevention and response, and intelligence gathering to increase the awareness of Canadians about disinformation and threats to democratic processes. By doing so, CSE will enhance Canada's capacity to identify foreign interference threats. Technical guidance is prepared in the form of communication packages. A communications package could include a specific advice and guidance, workshops or other communications that promote cyber security. CSE provides technical guidance products (i.e., publications, courseware, and consultations) on cyber security topics to federal and provincial/territorial/municipal democratic institutions to support them in taking protective measures against cyber threat actors who target electoral processes and infrastructure (including</p>		<table border="1"> <tr> <td data-bbox="1016 764 1121 792"></td> <td data-bbox="1121 764 1226 792"></td> </tr> <tr> <td data-bbox="1016 792 1226 889"></td> <td data-bbox="1016 792 1226 889"></td> </tr> </table>					<table border="1"> <tr> <td data-bbox="1253 696 1583 1333"></td> <td data-bbox="1583 696 1791 1333"></td> </tr> </table>		

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>by altering website and social media content, stealing information such as voter registration databases, and/or compromising the systems or communications underlying the election). Democratic Institutions includes both Elections Authorities, Political Parties and support for other guidance initiatives as needed.</p> <p>In addition, CSE has established a community of interest (COI) for the Elections Authorities across Canada and is proactively reaching out to federal political parties in anticipation of the next General Election. CSE also supports organizations such as the Leaderships Debates Committee and the House of Commons. During an election year CSE's federal support also extends to political parties.</p> <p>CSE is currently developing a technical guidance library for democratic institutions, with 7 publications and 3 courses under development and/or complete and is planning an additional 12+ publications, and 3+ courses.</p>			
<p>Technical Advice and Guidance on Cryptographic Security CSSD provides technical advice and guidance to clients on cryptographic security. In the past we have worked</p>	<p>CSSD has provided advice and guidance periodically as requested to clients.</p>		

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>with Elections Canada to provide advice and guidance related to voting systems.</p>				
<p>Secure Communications for National Leadership (SCNL) Program</p> <p>CSE, in partnership with SSC, and in support of PCO, support the PCO-led Secure Communications for National Leadership (SCNL) program. CSE builds and deliver secure mobile messaging and voice cell phone capabilities (SCNL mobile). SCNL mobile devices have been provided to senior elected officials and senior government leadership and, in conjunction with traditional secure communications in secure facilities have enabled more portable and flexible secure communications solutions for government. In 2020, CSE supported SSC and PCO in the addition of a secure videoconferencing solution (Video for Senior Officials – VFSO) that has further expanded senior elected officials and Cabinet committees to be held securely in a virtual setting.</p> <p>Both secure mobile and secure videoconferencing services continue to expand and grow in response to client</p>	<p>Underway</p>			

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>demand and governmental response to domestic and international events.</p> <p>PCO is the business owner of these services [redacted]</p> <p>[redacted]</p> <p>with CSE hosting the SCNL mobile service, while SSC hosts the VFSO secure videoconferencing service.</p>				
<p>Cyber Sensor Operations</p> <p>Cyber Sensor Operations for key PD Canadian departments/agencies/ organizations. Cyber Sensor Operations are already initiated and are part of CSE's mandate. Specific operational details are not typically shared on a per client basis.</p>	<p>This activity is currently underway.</p>			
<p>Protected DNS for Political Parties</p> <p>Domain Name Service (DNS) provides a translation service from the human readable domain name that are typed into an internet browser (i.e. www.cyber.gc.ca) into an Internet Protocol (IP) address. This translation allows users to reach internet sites that they seek. Malware, however, also uses domain names to communicate. Protected DNS initiatives can identify,</p>				

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>filter and block malware communications and malicious domain names, building a protective DNS capability, and CSE can contribute threat intelligence to these services. CSE has used protected DNS under the project name Canadian Shield/Canadian Armour to help protect partners in the health care field. A similar approach could be used to support political parties and protect our democratic institutions from potential malware threats in the future.</p> <p>CSE has used protected DNS under the project name CANDIAN SHIELD / CANADIAN ARMOUR to support the Health Care Sector during COVID and could use a similar approach to helping political parties.</p>				
<p>Cyber Threat Landscape Reporting (OBSERVATION DECK) for key PD Canadian departments/ agencies/ organizations including plans for non-fed.</p> <p>Cyber Threat Landscape Reporting Operations are already initiated and are part of CSE's mandate. Specific operational details are not typically shared on a per client basis. Expansion (within technical capacity) is possible</p>	Underway			

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

based on an urgent request outside of our current expansion plans.			
<p>Cyber Log Ingestion for key PD Canadian departments/agencies/organizations inc non-fed.</p> <p>Some cyber Log Ingestion Operations are already initiated and are part of CSE's mandate. Specific operational details are not typically shared on a per client basis. Expansion (within technical capacity) is possible based on an urgent request outside of our current expansion plans.</p>			
<p>Security and Intelligence Threats to Elections (SITE) Task Force Supports the 'Combatting Foreign interference Pillar', detecting and countering mis- and dis-information, and exists largely in the 'upstream' space.</p> <p>This body, supported by analytic and investigative resources of each member department and agency, meets regularly to discuss trends and adversary behaviours, and ensures a coordinated flow of intelligence to senior government officials on a range of</p>	This activity is currently underway	<p><u>FUNDED</u></p> <p>SITE TF members contribute their own time and resources to ensure the body functions in an efficient manner. CSE analytic efforts underpinning intelligence production on threats are funded via existing programs.</p>	

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>potential threats to elections in order to facilitate assessment and threat response.</p> <p>In the lead up to an election, SITE closely monitors and evaluates the foreign threat environment, producing assessments and summaries to inform key partners. During the writ period, SITE performs the critical function of ensuring the panel of senior Deputy Ministers charged with administering the Critical Election Incident Public Protocol receive timely intelligence on relevant threats.</p> <p>SITE TF also provides regular briefings to various levels of the Elections Security Coordination Committee and other key GC partners. In coordination with PCO, SITE TF partakes in threat briefings and engagements with cleared members of registered political parties, to enable better visibility of the current threat environment and to encourage a two-way flow of information on potential threats.</p>				
---	--	--	--	--

For Public Release

PROTECTED B / PROTÉGÉ B

COUNTERING MIS- AND DISINFORMATION: DEVELOPING AN EMERGING PROTECTING DEMOCRACY AGENDA

<p>Foreign Intelligence efforts CSE produces foreign intelligence on the activities, intentions and capabilities of foreign threat actors. This intelligence effort responds to a wide range of Government of Canada requirements, including those specifically focused on hostile threats and threat actors.</p>	Underway			
--	----------	--	--	--