

UNCLASSIFIED // FOR OFFICIAL USE ONLY



BRIEFING BINDER

Bill C-59

November 29, 2017

Briefing Binder Table of Contents**Background on C-59**

TAB A	CSE Act 101
TAB B	Foreign Signals Intelligence
TAB C	Cybersecurity and Information Assurance
TAB D	Assistance
TAB E	Foreign Cyber Operations
TAB F	Metadata
TAB G	Publicly Available Information
TAB H	SIGINT Operations
TAB I	Transparency and Accountability
TAB J	Graphics
TAB K	Bill C-59 Charter Statement

CSE ACT 101

TALKING POINTS

- It is crucial for CSE to keep pace with emerging technologies to better protect Canada's sensitive information.
- Bill C-59 proposes changes to CSE's governing legislation with the introduction of a *CSE Act*.
- This legislation would:
 - Clarify how we are authorized to operate in cyberspace, authorizing CSE to use advanced techniques to access foreign networks to collect intelligence.
 - Authorize CSE to be able to defend important networks outside of the Government of Canada at the request of the system owner.
 - Authorized CSE to take action online to disrupt foreign cyber threats targeting important networks.
- All of these activities would be subject to review by the National Security and Intelligence Review Agency (NSIRA).
- The Intelligence Commissioner would have a mandate to approve foreign intelligence and cybersecurity authorizations issued by the Minister of National Defence.

BACKGROUND

CSE is the Government of Canada's cyber centre of excellence, operating in a rapidly evolving technological world. However, CSE's authorities have not kept up with that change. The proposed legislation will enable CSE to work more effectively and proactively to protect Canada and Canadians.

The legislation enhances CSE's capabilities by:

- Maintaining CSE's ability to collect foreign signals intelligence, by authorizing CSE to use advanced techniques to access foreign networks to collect intelligence in support of government priorities;
- Authorizing CSE to defend important non-government of Canada networks by, upon request, deploying CSE's cybersecurity tools on non-government systems; and removing legal barriers to sharing cyber threat information and mitigation advice;
- Authorizing CSE to provide assistance to DND/CAF, including cyber operations for government-authorized military missions; and
- Authorizing CSE to undertake foreign cyber operations in support of broader government priorities.

Transparency and Accountability

Bill C-59 will also respond to calls from successive CSE Commissioners to clarify ambiguities in CSE's current legislation and increase transparency at CSE. The *CSE Act* will make it clear exactly what CSE is permitted to do.

Under the proposed legislation, CSE's activities would be reviewed by the proposed National Security and Intelligence Review Agency (NSIRA). NSIRA would review CSE's activities for lawfulness and to ensure that CSE's activities are reasonable, necessary, and compliant with ministerial direction. This includes the ability to review CSE's activities as they related to the active and defensive cyber operations aspect of CSE's mandate.

In addition, the proposed Intelligence Commissioner would have a mandate to approve foreign intelligence authorizations issued by the Minister of National Defence. Commissioner approval would be required for the authorizations to come into effect. The Commissioner would be fully independent of government and of CSE.

The National Security and Intelligence Committee of Parliamentarians (NSICOP) would also have a role in reviewing CSE activities; including CSE's activities as they relate to active and defensive cyber operations.

Resources

The legislation is focused on authorities and accountabilities and not on CSE resources. CSE is constantly looking at how best to define our own mission and mandate. To this end, this legislation is welcome as a means to more effectively help protect the safety and security of Canada and Canadians.

FOREIGN SIGNALS INTELLIGENCE

TALKING POINTS

- Under the proposed legislation CSE would be able to use a broader range of SIGINT capabilities to acquire foreign intelligence.
- Specifically, this new authority would allow CSE to interact with foreign targets operating on computer networks and systems.
- Under current and proposed legislation, we cannot and do not direct our activities at Canadians or anyone in Canada.
- The Act would also introduce a role for the Intelligence Commissioner – an independent, retired judge of a superior court – to approve Ministerial Authorizations before they come into effect.
- CSE's activities would be subject to review by the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency.

BACKGROUND

What does the CSE Act say?

Under the proposed legislation, CSE would be authorized to acquire, covertly or otherwise, information from or through the global information infrastructure, including by engaging or interacting with foreign entities located outside Canada or by using any other method of acquiring information, and to analyze, use, and disseminate the information for the purpose of providing foreign intelligence, in accordance with the government of Canada's intelligence priorities.

What does that mean?

In addition to CSE's existing SIGINT methods and techniques, CSE would be able to use a broader range of advanced capabilities to acquire foreign intelligence from foreign targets outside of Canada. This new authority would allow CSE to interact with foreign targets operating on computer networks and systems. CSE could gather information that provides an advantage to military commanders leading Canadian Armed Forces missions and other Canadian officials charged with mitigating threats related to terrorism, espionage, kidnappings and cyber intrusions.

Why are these changes needed?

The critical foreign intelligence provided by CSE is necessary to protect Canada and Canadians from foreign threats to our security and economic prosperity, and helps protect the rights and freedoms that Canadians enjoy. Technological advances have significantly impacted the way in which CSE operates. In order to continue to protect Canadians, the *CSE Act* would update CSE's authorities and clearly outline what CSE is permitted to do to ensure that CSE can deliver on its lawfully-mandated activities.

These proposals would strengthen Canada's resilience and ensure that CSE is able to continue to provide vital intelligence, such as:

- Supporting Canada's military operations;
- Uncovering foreign-based extremists' efforts to radicalize individuals to carry out attacks in Canada and abroad;
- Furthering Canada's national interests by informing foreign policy; and
- Supporting Canada's response to hostage takings overseas;

Transparency and Accountability

CSE's foreign signals intelligence operations are, and would continue to be, clearly and carefully targeted, by law, at the activities of foreign individuals, states, and organizations or terrorist groups that have implications for Canada's international affairs, defence or security. The proposed *CSE Act* does not change this. It will still be against the law for CSE to direct its foreign signals intelligence activities against Canadians anywhere, or against anyone in Canada.

The proposed *CSE Act* would improve transparency and accountability for CSE. It would give Canadians, including those institutions responsible for holding CSE accountable for its actions, such as the proposed Intelligence Commissioner, the proposed National Security and Intelligence Review Agency, the Privacy Commissioner and parliamentarians, a better and clearer sense of CSE's legal authorities. This Act would implement the following constraints on CSE's foreign intelligence mandate:

- Explicit statutory prohibition on targeting Canadians or any person in Canada;
- Explicit statutory requirement to protect privacy of Canadians and persons in Canada;
- Expanded Ministerial Authorization regime that would apply to all of CSE's acquisition of information from the global information infrastructure where the activity to acquire it would otherwise be unlawful or where the information has a privacy interest.

Before a foreign intelligence authorization takes effect, the Minister of National Defence must seek the Intelligence Commissioner's approval. In issuing a foreign intelligence or cybersecurity Authorization, the Minister must be satisfied that the conditions set out in law are met, including that the activities are reasonable, necessary and proportionate, and that appropriate privacy protections are in place. In order to approve an Authorization, the IC would have to be satisfied that the ministerial conclusions in this regard are reasonable.

CYBER SECURITY AND INFORMATION ASSURANCE

TALKING POINTS

- Canada is an attractive target for cyber threat actors. Our national security, well-being, and economic prosperity depend on the Internet and the smooth functioning of our cyber systems.
- Under current legislation, we are authorized to provide advice, guidance, and services to protect information and information infrastructures of importance to the Government of Canada. However, we can only deploy our unique cyber defence tools onto federal systems.
- Under proposed legislation, upon request and when designated by the Minister of National Defence as a system of importance to the Government of Canada, CSE would be authorized to provide more robust cyber defence services to a critical non-Government network.
- CSE cannot direct its cyber security and information assurance activities at Canadians or persons in Canada. The proposed CSE Act would not change this.
- Under the proposed legislation, CSE would be subject to additional transparency and accountability measures.
- Subject to review by the National Security and Intelligence Review Agency (NSIRA) and the Intelligence Commissioner. The Minister of National Defence would be required to seek the Intelligence Commissioner's approval before a cyber security authorization takes effect.

BACKGROUND

Under the proposed legislation, CSE would be authorized to:

- Provide advice, guidance and services to help ensure the protection of:
 - Federal institutions' electronic information and information infrastructures
 - Electronic information and information infrastructures designated by the Minister as being of importance to the Government of Canada
- Acquire information from the global information infrastructure or from other sources in order to provide such advice, guidance and services.

What does that mean?

In addition to CSE's current cybersecurity and information assurance mandate, CSE would be able to defend important networks outside of the Government of Canada. The proposed CSE

Act would also explicitly allow CSE to share cyber threat information with owners of systems outside of the federal Government so that they can better protect their networks and information.

For example, CSE could more extensively share information about specific cyber threats with the owners of critical infrastructure, like telecommunications companies or the banking sector.

CSE would also be permitted to deploy its unique cybersecurity tools on non-government systems at the request of the owners of those systems.

These additional activities will better protect Canadians' most sensitive information and important cyber networks from compromise as well as strengthen the country's cyber defences.

Why are these changes needed?

Canada is an attractive target for cyber threat actors. Our national security, well-being and economic prosperity depend on the Internet and the smooth functioning of our cyber systems.

Under the proposed *CSE Act*, CSE would have the authority to use its tools to help protect the vital information that Canadians have entrusted to both the Government of Canada and to private industry.

Transparency and Accountability

CSE's cybersecurity activities play a critical and unique role in protecting Canada and Canadians from cyber threats. However, CSE cannot direct its cybersecurity and information assurance activities at Canadians or persons in Canada. The proposed *CSE Act* would not change this.

With additional authorities under the proposed *CSE Act*, CSE would be subject to additional transparency and accountability measures.

The proposed *CSE Act* would give Canadians as well as the institutions responsible for holding CSE accountable for its actions, such as the proposed Intelligence Commissioner, the proposed National Security and Intelligence Review Agency, the Privacy Commissioner and Parliamentarians, a better and clearer sense of CSE's legal authorities.

This Act would implement the following constraints on CSE's cybersecurity and information assurance mandate:

- Explicit statutory prohibition on targeting Canadians or any person in Canada;
- Explicit statutory requirement to protect the privacy of Canadians and persons in Canada;
- Expanded Ministerial Authorization regime that would apply to all of CSE's acquisition of information from the global information infrastructure where the activity to acquire it would otherwise be unlawful or where the information has a privacy interest.

Before a cybersecurity authorization takes effect, the Minister of National Defence must seek the Intelligence Commissioner's approval.

UNCLASSIFIED

In issuing a foreign intelligence or cybersecurity Authorization, the Minister must be satisfied that the conditions set out in law are met, including that the activities are reasonable, necessary and proportionate, and that appropriate privacy protections are in place.

In order to approve an Authorization, the IC would have to be satisfied that the ministerial conclusions in this regard are reasonable.

ASSISTANCE TO FEDERAL SECURITY AND INTELLIGENCE PARTNERS

TALKING POINTS

- As Canada's national cryptologic and signals intelligence agency, CSE possesses unique capabilities and expertise.
- Under current legislation, we assist federal law enforcement and security agencies in the performance of their lawful duties.
- Under proposed legislation, we would be permitted to assist the Department of National Defence (DND) and the Canadian Armed Forces (CAF).
- CSE would continue to have the same authority to carry out an activity as the agency requesting the assistance.
- CSE would also be subject to any restrictions or conditions placed on the agency requesting that assistance.

BACKGROUND

Under the proposed legislation, CSE would be authorized to:

- Provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Armed Forces and the Department of National Defence in their performance of their lawful duties.

What does that mean?

CSE is currently authorized to assist federal law enforcement and security agencies in the performance of their lawful duties.

With new legislation and the increased accountability measures that come with it, CSE would also be permitted to assist the Department of National Defence (DND) and the Canadian Armed Forces (CAF), such as with cyber operations, to meet military objectives and protect our forces.

For instance, CSE could use advanced techniques to disrupt adversaries' ability to communicate with each other.

Why are these changes needed?

As Canada's national cryptologic and signals intelligence agency, CSE possesses unique capabilities and expertise. Where possible and most effective, CSE would be permitted to assist CAF missions and to help protect our forces with cyber operations.

Cooperation between CSE and the CAF for approved missions would ensure the best use of tools and capabilities, reduce duplication of efforts, and improve the chances of meeting mission objectives.

Authorities and Restrictions

As is currently the case when assisting partners, under the CSE Act, CSE would have the same authority to carry out an activity as the agency requesting the assistance. CSE would also be subject to any restrictions or conditions placed on the agency requesting that assistance, such as a warrant or applicable law.

In addition, for assistance to DND and the CAF, CSE would:

- receive a written request from DND or CAF authorized by an appropriate representative;
- comply with all instructions, parameters, and limits of the authorized CAF activity;
- comply with all relevant Ministerial Directives issued to CSE by the Minister of National Defence;
- adhere to agreements or arrangements with DND and CAF; and
- comply with all CSE policies and procedures related to the provision of assistance.

CSE has strict internal monitoring of assistance mandate activities for legal and policy compliance.

Accountability and Review

All of the activities that CSE would undertake in support of federal security and intelligence partners would be subject to review by the proposed National Security and Intelligence Review Agency, as well as other review bodies, such as the proposed National Security and Intelligence Committee of Parliamentarians, and the Privacy Commissioner.

FOREIGN CYBER OPERATIONS

TALKING POINTS

- Defensive cyber operations would involve taking action to protect the information and networks of the federal government and designated systems of importance to the Government of Canada.
- Active cyber operations would involve carrying out activities to degrade, disrupt, influence, respond to, or interfere with the capabilities, intentions, or activities of a foreign threat actor.
- These operations would take place within a strict approval process.
- CSE would be prohibited from directing its active and defensive cyber operations at Canadians, any person in Canada, or the global information infrastructure in Canada.
- These activities must also be reasonable and proportionate.
- CSE also cannot cause death or bodily harm, or wilfully attempt to obstruct, pervert, or defeat the course of justice or democracy.
- CSE's activities would be subject to review by the National Security and Intelligence Committee of Parliamentarians (NSICOP) and the National Security and Intelligence Review Agency (NSIRA).

BACKGROUND

What is new?

Under the proposed *CSE Act*, CSE would be authorized to conduct both defensive cyber operations and active cyber operations.

The defensive cyber operations aspect of CSE's mandate would allow CSE to take action on or through the global information infrastructure to help protect:

- federal institutions' electronic information and information infrastructures; and
- electronic information and information infrastructures designated by the Minister as being of importance to the Government of Canada.

The active cyber operations aspect of CSE's mandate would be to carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to Canada's defence, security or international affairs.

What does that mean?

CSE could be authorized to proactively stop or impede foreign cyber threats before they damage Canadian systems or information holdings, and conduct online operations to advance national objectives. For example, under defensive cyber operations CSE could disable a foreign server that was attempting to steal information about Canadians from a Government of Canada network. Under active cyber operations CSE could use on-line capabilities to interfere with the ability of terrorist groups to recruit Canadians or plan attacks against Canada and its allies.

Why are new authorities needed?

With constantly evolving global technological and threat landscapes, governments are rethinking national approaches and strategies to protect their citizens from threats. CSE's foreign cyber operations mandate will provide Canada with the cyber means to respond to serious foreign threats, international crises, or events as part of a broader strategic approach.

Defensive Cyber Operations: CSE's defensive cyber operations mandate would protect Canada and Canadians from foreign cyber threats that may jeopardize Canadian security, economic prosperity, and rights and freedoms. CSE helps to protect important cyber networks, but does not currently have the authority to take action online outside of Government of Canada networks to deter imminent or ongoing malicious cyber threats against Canada. With new legislation and the increased accountability measures that come with it, CSE would be authorized to take action online to defend Canadian networks, owned by both the Government of Canada and the private sector, and proactively deter cyber threats before they reach our systems.

Active Cyber Operations: The proposed *CSE Act* would allow the government to utilize CSE's online capabilities in support of the government's broader strategic objectives. Within strict legal parameters and approvals at the highest level of government, CSE would be permitted to take action online to disrupt foreign threats, including activities to protect our democratic institutions, counter violent extremism and terrorist planning, or counter cyber aggression by foreign states.

Transparency and Accountability

CSE's active cyber operations would be carefully targeted, by law, to the activities of foreign individuals, states, organizations or terrorist groups that have implications for Canada's international affairs, defence or security. These operations would be developed as part of a broader Government of Canada strategic approach or in response to a serious crisis or threat, and would be built with Canada's foreign policy objectives in mind.

CSE would be prohibited from directing defensive and active cyber operations activities at Canadians, any person in Canada, or the global information infrastructure in Canada. The proposed *CSE Act* would require that these activities be reasonable and proportional, and prohibit CSE from causing death or bodily harm, or willfully attempting to obstruct, pervert or defeat the course of justice or democracy.

UNCLASSIFIED

These activities would only be undertaken under the authority of an active cyber authorization under a Ministerial two-key system. Ministerial Authorizations issued for active cyber operations would require the approval of the Minister of National Defence and the Minister of Foreign Affairs. Ministerial Authorizations issued for defensive cyber operations would require the approval of the Minister of National Defence and consultation with the Minister of Foreign Affairs. CSE would be required to report the outcomes of their activities to both ministers.

All activities conducted under the defensive cyber operations and active cyber operations mandate would be subject to review by the proposed National Security and Intelligence Review Agency, as well as the National Security and Intelligence Committee of Parliamentarians.

METADATA

TALKING POINTS

- The *CSE Act* requires that CSE obtain a Ministerial Authorization to acquire any information, when that acquisition would otherwise be unlawful or where the information acquired would have a privacy interest.
- Ministerial Authorizations would not come into effect until approved by the independent Intelligence Commissioner, a retired judge.
- The *CSE Act* also includes specific provisions on the use, retention and disclosure of information, including metadata.

If Pressed:

- The language *CSE Act* focuses on the word “information.” In context of the Act, information includes metadata.

BACKGROUND

The *CSE Act* responds to calls from successive CSE Commissioners for greater clarity and transparency in CSE’s legislation. In particular, the *CSE Act* addresses the current and previous CSE Commissioner’s recommendation that CSE’s legislation be amended to explicitly clarify CSE’s powers and privacy protections related to metadata (specifically CSE’s authority to collect, use, retain, share, and disclose metadata). It responds to this recommendation by expanding CSE’s oversight regime – the ministerial authorization regime – to cover some of these activities, and by explicitly articulating its authority to disclose certain types of information.

Metadata and CSE activities

Metadata refers to technical information associated with a communication that is used to identify, manage, or route communications on the global information infrastructure. Metadata is critical to the fulfillment of CSE’s mandate. In general, CSE utilizes metadata to map those parts of the global information infrastructure it needs to exploit for foreign intelligence purposes. CSE also uses the metadata it collects to develop collection profiles about foreign entities of intelligence interest to the Government of Canada and to locate the communications involving these foreign intelligence targets for collection purposes.

CSE does not target Canadian metadata for collection. However, due to the complexity of the global communications network, at certain collection points where CSE is active, Canadian communications are comingled with international communications. This could include metadata where one or both ends of a communications may be in Canada.

Metadata in the CSE Act

Acquisition, use, and retention

Today, under the *National Defence Act*, CSE requires a ministerial authorization when it conducts activities that risk intercepting private communications. While metadata is not a private communication, it may have a privacy interest. Under the *National Defence Act*, CSE collects metadata as part of its legislated mandate to acquire information from the global information infrastructure.

The *CSE Act*, instead of creating a separate oversight regime for metadata, would expand the scope of the ministerial authorization regime to require that CSE have a ministerial authorization when it directly acquires any type of information from the global information infrastructure where the acquisition of that information would otherwise be contrary to an Act of Parliament. In addition, to meet CSE's obligations under the *Charter of Rights and Freedoms*, CSE would get a ministerial authorization when it directly acquires information from the global information infrastructure that has a privacy interest.

In this context, information includes metadata. Therefore, the *CSE Act* requires that CSE have a ministerial authorization before it directly acquires metadata from the global information infrastructure where the acquisition would otherwise be unlawful, or where the metadata acquired would have a privacy interest.

In order to issue an authorization the Minister would have to have reasonable grounds to believe that conditions related to the acquisition, retention, and use of the information were met. These conditions are outlined in subsections 35(1), (2), and (3) of the *CSE Act*, and include:

- that any activity authorized was reasonable and proportionate;
- that any information (including metadata) acquired under a foreign intelligence authorization could not have been reasonably acquired by other means;
- that any unselected information (including unselected metadata) acquired under a foreign intelligence authorization could not have reasonably been obtained by other means (i.e. the information/metadata could only reasonably be obtained in an unselected manner);
- that any information (including metadata) acquired under a cybersecurity authorization is necessary to identify, isolate, prevent, or mitigate harm to a Federal Government information infrastructure, or an information infrastructure designated as being of importance;
- that the consent of all persons whose information (including metadata) may be acquired under a cybersecurity authorization for Federal Government information infrastructures could not reasonably be obtained;
- that privacy protection measures in place will ensure that any information (including metadata) acquired under a foreign intelligence or cybersecurity authorization will only

be used or retained if it is essential either to: a) international affairs, defence or security, in the case of a foreign intelligence authorization; or b) to identify, isolate, prevent, or mitigate harm to a Federal Government information infrastructure or an information infrastructure of importance, in the case of a cybersecurity authorization; and

- that any information (including metadata) acquired under a foreign intelligence or cybersecurity authorization will be retained for no longer than is reasonably necessary.

The *CSE Act* requires that the independent Intelligence Commissioner, a retired judge of a superior court, approve the reasonableness of the Minister's conclusions that the necessary conditions have been met. CSE cannot undertake any activities under a foreign intelligence or cybersecurity authorization until the Intelligence Commissioner has approved the authorization, except in urgent circumstances as described in section 47.

Importantly, the *CSE Act* would retain the prohibition on directing foreign intelligence or cybersecurity activities at Canadians or persons in Canada. There are certain narrow and explicit exceptions to this restriction, outlined clearly in section 24. The Act would also require that CSE have measures in place to protect the privacy of Canadians and in persons in Canada.

Disclosure

The *CSE Act* explicitly articulates CSE's authority to disclose certain types of information. It includes specific provisions governing the disclosure of certain types of information, including Canadian identifying information, and information for cybersecurity purposes under sections 44 and 45 of the *CSE Act*.

Review

All of CSE's activities would be reviewed by the proposed National Security and Intelligence Review Agency (NSIRA). NSIRA would review CSE's activities for lawfulness and to ensure that CSE's activities are reasonable, necessary, and compliant with ministerial direction. This includes the ability to review CSE's activities as they related to the collection, use, retention, sharing, and disclosure of metadata.

The National Security and Intelligence Committee of Parliamentarians (NSICOP) will also have a role in reviewing CSE activities; including CSE's activities as they relate to metadata.

PUBLICLY AVAILABLE INFORMATION

TALKING POINTS

- The intent of this provision is to allow CSE to conduct basic research in support of its mandate without fear of the restriction that it not direct its activities at Canadians or persons in Canada.
- This is not an authority to conduct investigations, or a means of collecting intelligence.
- For example, CSE may use publicly available information to provide useful context or background information to an intelligence or information assurance report.
- CSE must ensure that measures are in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and disclosure of publicly available information.

If pressed:

- CSE would not acquire information that was unlawfully obtained, such through a compromise or a leak, under this provision.

BACKGROUND

Publicly available information is information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or is available to the public on request, by subscription, or purchase.

Paragraph 24(1)(a) states that CSE may acquire, use, analyse, retain, or disclose publicly available information despite subsections 23(1) and (2), which state that certain CSE activities may not be directed at a Canadian, any person in Canada, or any portion of the global information infrastructure.

The acquisition and use of information already in the public realm would generally not intrude upon protected privacy rights. Where it would, the reasonable expectation of privacy would generally be low because the information is publicly available. Nevertheless, section 25 of the *CSE Act* explicitly requires that CSE have measures in place to protect the privacy of Canadians and persons in Canada in the use, retention, and disclosure of publicly available information. The *CSE Act* also maintains the focus of the foreign intelligence aspect of CSE's mandate on foreign individuals, states, organizations, or terrorist groups.

The intent of this provision and the definition is in place to allow CSE to conduct basic research in support of the mandates without fear of breaching the directed at restriction. This is not an investigative activity, or a means of collecting intelligence. CSE could only carry out these activities in support of its mandate. For example, CSE may use publicly available information to

provide useful context or background information to an intelligence or information assurance report.

Moreover, the proposed National Security and Intelligence Review Agency will review all of CSE's activities for lawfulness and to ensure that CSE's activities are reasonable, necessary, and compliant with ministerial direction. The review agency's findings will be detailed in an annual report provided to the Minister of National Defence.

The National Security and Intelligence Committee of Parliamentarians will also have a role in reviewing CSE activities and could review the measures it has in place to protect the privacy of Canadians.

Examples of information CSE would acquire under paragraph 24(1)(a)

Both Mandates

- CSE may use publicly available information in order to help protect the privacy of Canadians. Publicly available information may be used, as part of a larger analysis, in order to assess the nationality of a corporation or individual. This is done to minimize privacy risk by limiting the incidental collection of information relating to Canadians and persons in Canada under the foreign intelligence or cybersecurity aspects of CSE's mandate. Being able to assess the nationality of an entity allows CSE to establish terms and criteria that will identify information of *foreign* intelligence value, for the purposes of CSE's foreign intelligence mandate, and will help CSE to limit the incidental collection of information relating to Canadians and persons in Canada, as well as to apply measures to protect their privacy, under both mandates.
- CSE may use publicly available information to provide useful context or background information to an intelligence or information assurance report. This information would be used to introduce or explain an event being described in a report. For example, publicly available information could be used to provide important contextual information about a known compromise of a Canadian entity, or information technology product or service. This information would be used to complement CSE's report.

Cybersecurity and Information Assurance

- Vulnerability information is often available to everyone on publicly available sites. For example, publicly available security expert blogs are an important source of detailed technical information on vulnerabilities. The information available on information technology and security sites is valuable in helping CSE keep up to date with research and developments relating to new vulnerabilities.
- CSE may use publicly available information when CSE's analysts analyze malware in order to help protect infrastructure of importance to the Government of Canada. Often this information is available on publicly available websites. CSE uses these sources to assist with reverse engineering malware samples. For example, there are publicly available

databases that allow any user to submit malware samples and that return information on previously submitted examples, as well as anti-virus detection. The use of these websites help support CSE's ongoing malware research.

- Publicly available information may be used to determine new terms and criteria that will help identify a threat. This information is frequently available on publicly available resources, as a collaboration effort by security researchers. For example, in a cybersecurity context, security researchers may have shared amongst each other, on publicly-accessible fora, malicious code signatures that can be used by CSE for the purposes of identifying threats to Government of Canada computer systems or networks. Publicly available information of this kind is used by information technology professionals throughout the industry in order to improve situational awareness.
- CSE may use publicly available information to discover security threats to electronic information and information infrastructures of systems of importance to the Government of Canada. Cyber threat actors, such as hacktivists, will often use online public forums to discuss their plans to launch cyberattacks. The ability to access these online forums would assist CSE in its anticipation of and defence against threats, especially during a campaign launched by a threat actor against the Government of Canada. CSE will use the information for situational awareness and to prepare systems and networks under its protection against these threats. CSE would not, however, use the information to investigate the hacktivists or to prosecute them.
- Under CSE's cybersecurity and information assurance mandate, CSE is authorized to provide advice, guidance and services to ensure the protection of systems of importance to the Government of Canada. This information is useful to learn more about a particular sector or Canadian infrastructure to which CSE may be required to provide services. This could be something as simple as looking at a company's website to determine appropriate points of contact for the establishment, maintenance, termination or resumption of relationships in support of cybersecurity and information assurance activities.

Foreign Intelligence

- Publicly available information may be used to identify emerging geopolitical issues and trends to place foreign intelligence in context. For example, CSE analysts may look at the popularity of a hashtag in order to assess the morale of foreign fighters abroad. CSE would be interested in the aggregate of broadcasted information to scan topics or issues relevant to the GC's foreign intelligence priorities.
- Publicly available information could also be used to research technological trends. The effectiveness of CSE's foreign intelligence activities depends on CSE's ability to adapt to new technologies. For example, as our adversaries, including terrorists overseas, increasingly rely on new technologies to avoid detection, CSE's ability to provide foreign intelligence to the Government of Canada is reliant on its knowledge of computer science and mathematics. The ability to conduct research of publicly available information to learn

about the latest scientific developments (such as quantum computing) is critical to maintain CSE's capabilities against threat actors.

- CSE also requires publicly available information to understand the global information infrastructure and identify which portions of it are more likely to carry foreign signals. For example, this requires CSE to be aware of changes to or adoptions of international transmission protocols and standards. This knowledge can be built up and maintained by accessing a range of publicly available resources.
- CSE may purchase commercially available defence and security intelligence information platforms, to access a wide range of publicly available resources relevant to its mandate, including terrorism/threat analytics, daily country risk profiles and unclassified intelligence briefings.

Examples of information CSE would NOT acquire under paragraph 24(1)(a)

- CSE would not use paragraph 24(1)(a) for information that was unlawfully obtained and released to the public. Publicly available information is clearly defined in section 2 of the *CSE Act* as information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase. Information that was unlawfully obtained, such as private information obtained through a compromise or a leak, would not constitute "publicly available information" for the purposes of the *CSE Act*.
- CSE would not use paragraph 24(1)(a) to investigate Canadians or persons in Canada or build a dossier on them. CSE must only use publicly available information in furtherance of its mandate. CSE does not have the mandate to investigate or provide intelligence on Canadians or persons in Canada.

SIGINT OPERATIONS

TALKING POINTS

- CSE is a foreign signals intelligence agency authorized to collect information from the global information infrastructure, based on intelligence priorities set by Cabinet.
- Under current and proposed legislation, we cannot and do not direct our activities at Canadians or anyone in Canada.
- Activities are carried out in a highly complex operating environment in which global communications technologies, networks, and systems are rapidly evolving.
- Use a range of innovative collection methods and techniques.
- Have strong privacy protection measures.
- CSE is currently reviewed by the independent CSE Commissioner.
- CSE is also subject to review by the National Security and Intelligence Committee of Parliamentarians (NSICOP).
- Under the proposed legislation, subject to review by the National Security and Intelligence Review Agency (NSIRA) and the Intelligence Commissioner would have a mandate to approve foreign intelligence and cybersecurity authorizations issued by the Minister of National Defence.

BACKGROUND

In response to Government of Canada (GC) intelligence priorities, CSE collects the communications of foreign intelligence targets outside of Canada and produces intelligence reports for GC clients.

Threat actors are increasingly taking advantage of technological security measures to conceal their activities. These technological changes have made it much more difficult to collect and extract communications of interest using traditional collection methods.

To fulfill our SIGINT mission, CSE requires a range of innovative and agile collection measures. The complexity of these methods varies depending on the complexity of the targeted communications.

CSE's signal intelligence program has been and will remain a vital contributor to national security. Our success depends on targets being unaware of our interest in them and uncertain of our capabilities.

The CSE Act

The proposed *CSE Act* would clarify the activities that CSE is permitted to undertake, while also retaining the restrictions in the *National Defence Act*. Specifically, the legislation would explicitly state that the foreign intelligence aspect of CSE's mandate is to acquire "covertly or otherwise, information from or through the global information infrastructure including by engaging or interacting with foreign entities located outside of Canada or by using any other method of acquiring information, and to use, analyse, and disseminate the information for the purpose of providing foreign intelligence, in accordance with the Government of Canada's intelligence priorities."

Under the proposed legislation, CSE's activities would be subject to review by the National Security and Intelligence Review Agency (NSIRA). NSIRA would review CSE's activities not only for lawfulness, but also to ensure that CSE's activities are reasonable, necessary, and compliant with ministerial direction.

In addition, the proposed Intelligence Commissioner would have a mandate to approve foreign intelligence authorizations issued by the Minister of National Defence. Commissioner approval would be required for the authorizations to come into effect. The Commissioner would be fully independent of government and of CSE.

Finally, the National Security and Intelligence Committee of Parliamentarians will also have a role in reviewing CSE activities.

TRANSPARENCY AND ACCOUNTABILITY

TALKING POINTS

- CSE is currently reviewed by the Office of the Communications Security Establishment Commissioner.
- CSE's review and accountability framework will evolve to enhance the way in which CSE is reviewed, alongside the broader security and intelligence community.
- The legislation also strengthens CSE's Ministerial Authorization regime.
- The National Security and Intelligence Review Agency would assume responsibility for reviewing all national security activities across the Government of Canada, including all of CSE's activities.
- The Intelligence Commissioner would have a mandate to approve foreign intelligence and cybersecurity authorizations.
- Commissioner approval would be required for these authorizations to come into effect.

BACKGROUND

CSE is currently reviewed by the Office of the Communications Security Establishment Commissioner (OCSEC). Under proposed legislation, CSE's review and accountability framework will evolve to enhance the way in which CSE is reviewed, alongside the broader security and intelligence community. The legislation also strengthens CSE's Ministerial Authorization regime.

The Government is proposing to establish two new independent bodies through new legislation.

- the *National Security and Intelligence Review Agency (NSIRA)*
- the *Intelligence Commissioner (IC)*.

National Security and Intelligence Review Agency (NSIRA)

The NSIRA would assume responsibility for reviewing all national security activities across the Government of Canada, including all of CSE's activities. NSIRA would review CSE's activities for lawfulness and to ensure that CSE's activities are reasonable, necessary and compliant with ministerial direction. In addition, the NSIRA would serve as the new review body for any complaints against CSE.

The NSIRA would be led by a committee of up to seven members, appointed on the advice of the Prime Minister, in consultation with the leaders in the House of Commons and Senate. The NSIRA would have unfettered access to information necessary to review all national security activities across the federal government. The NSIRA would provide classified reports of its findings and recommendations to relevant ministers and would produce an annual unclassified public report to Parliament summarizing these findings and recommendations. The NSIRA would be fully independent of government and of CSE.

Intelligence Commissioner (IC)

The IC would have a mandate to approve foreign intelligence and cybersecurity Authorizations issued by the Minister of National Defence. IC approval would be required for the Authorizations to come into effect. The IC would be fully independent of government and of CSE. Given the nature of the office's mandate, the position of the IC would be filled by a retired judge of a superior court.

In issuing a foreign intelligence or cybersecurity Authorization, the Minister must be satisfied that the conditions set out in law are met, including that the activities are reasonable, necessary and proportionate, and that appropriate privacy protections are in place. In order to approve an Authorization, the IC would have to be satisfied that the ministerial conclusions in this regard are reasonable. The IC would be reviewing CSE's Ministerial Authorizations *before* CSE could conduct any operations under those Authorizations. The approval of the IC would be binding, meaning that CSE must have the IC's approval to proceed with those activities.

The Chief of CSE would be required to report to the Minister of National Defence on the outcomes of Ministerial Authorizations. The Minister would then be required to provide the NSIRA and the IC with a copy of that report.

Why are these changes needed?

Successive CSE Commissioners have called on the governments of the day to clarify ambiguities in CSE's legislation and increase transparency. Canadians have also been clear that they are looking for increased accountability and transparency of their security and intelligence agencies.

The establishment of NSIRA and the IC respond directly to those requests for clarity, accountability and transparency, and would create a more robust and coordinated review of CSE's activities along with new independent oversight of CSE's Ministerial Authorization regime. This proposed model recognizes the increasingly interconnected nature of the Government of Canada's security and intelligence activities and replaces the current siloed approach to review and accountability. Information sharing authorities between review bodies, and with the IC, would add to the depth of review as well as prevent the duplication of efforts.

These proposed changes would enhance transparency and provide as much information about national security activities to Canadians as possible, without compromising the national interest or the effectiveness of operations.

Additional Accountability

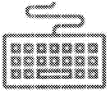
In addition to these proposed enhancements to how CSE's activities are reviewed, CSE would continue to be accountable to the Privacy Commissioner of Canada, the Auditor General, the Information Commissioner of Canada, the Canadian Human Rights Commission, and the Commissioner of Official Languages. CSE would also be subject to review by the proposed National Security and Intelligence Committee of Parliamentarians.

All of these proposed and existing forms of review and accountability will help ensure that CSE continues to respect and follow the law, and protect the privacy of Canadians, while at the same time conducting its critical intelligence and cybersecurity activities.

UNCLASSIFIED


PROPOSED AUTHORITIES & CAPABILITIES FOR CSE

FOREIGN SIGNALS INTELLIGENCE



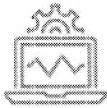
MAINTAIN CSE'S ABILITY TO COLLECT FOREIGN SIGNALS INTELLIGENCE
Use advanced techniques to access foreign networks to collect intelligence in support of government priorities

CYBERSECURITY & INFORMATION ASSURANCE



DEFEND IMPORTANT NON-GOVERNMENT OF CANADA NETWORKS
Upon request, deploy CSE's cybersecurity tools on non-government systems
Remove legal barriers to sharing cyber threat information and mitigation advice


ASSISTANCE TO FEDERAL SECURITY & INTELLIGENCE PARTNERS



ASSISTANCE TO DND/JCAF INCLUDING CYBER OPERATIONS FOR GOVERNMENT-AUTHORIZED MILITARY MISSIONS
Use advanced techniques to support military campaigns and protect military personnel



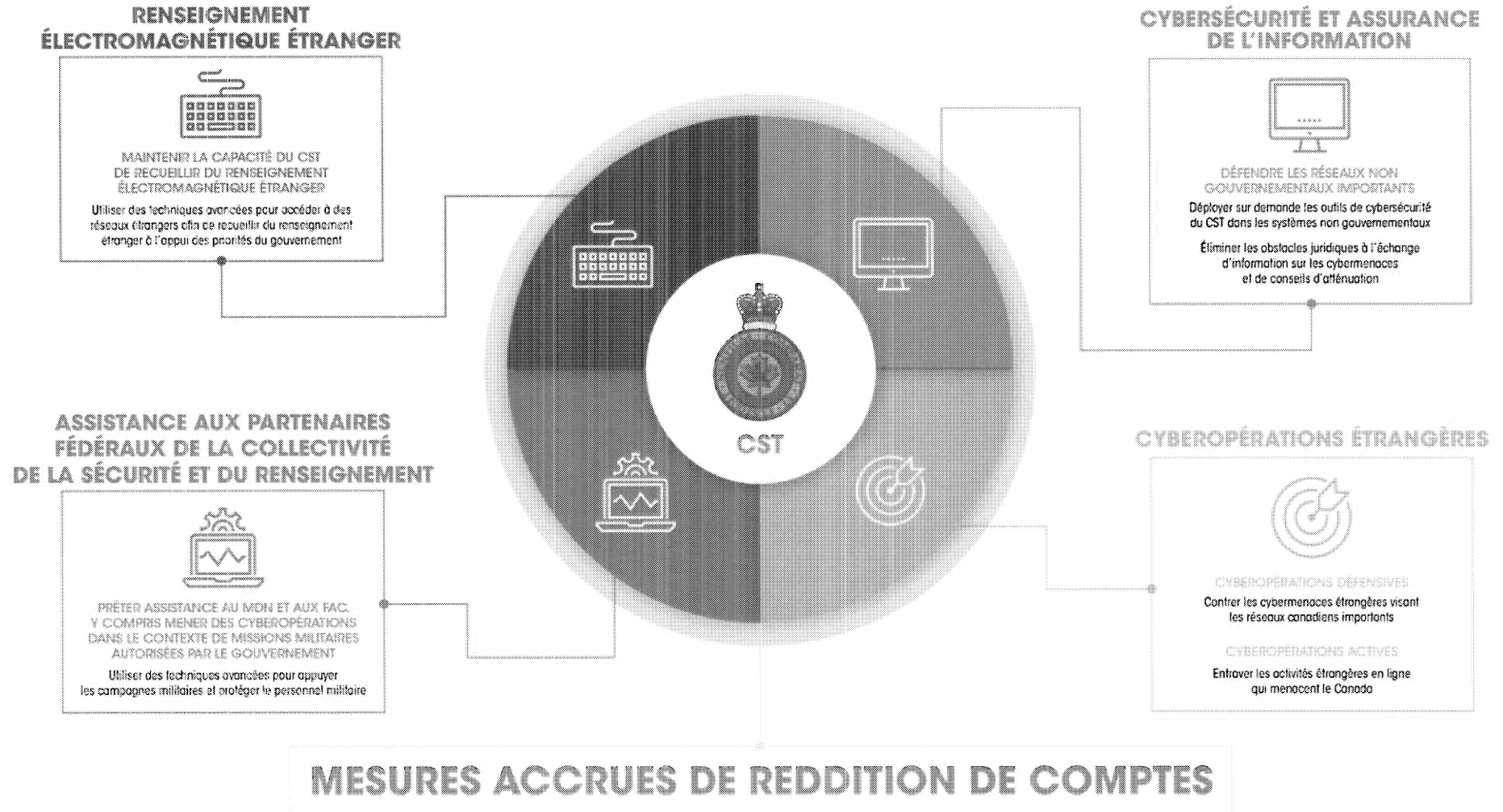
FOREIGN CYBER OPERATIONS



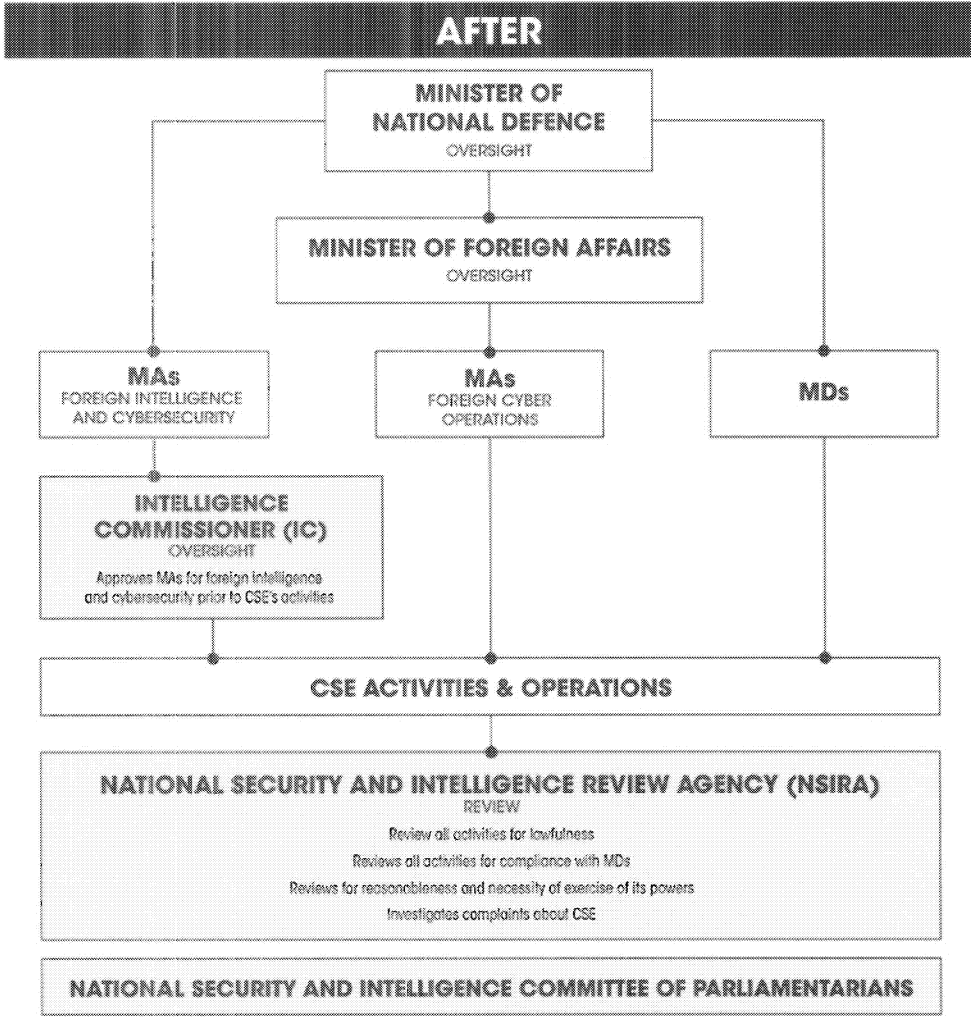
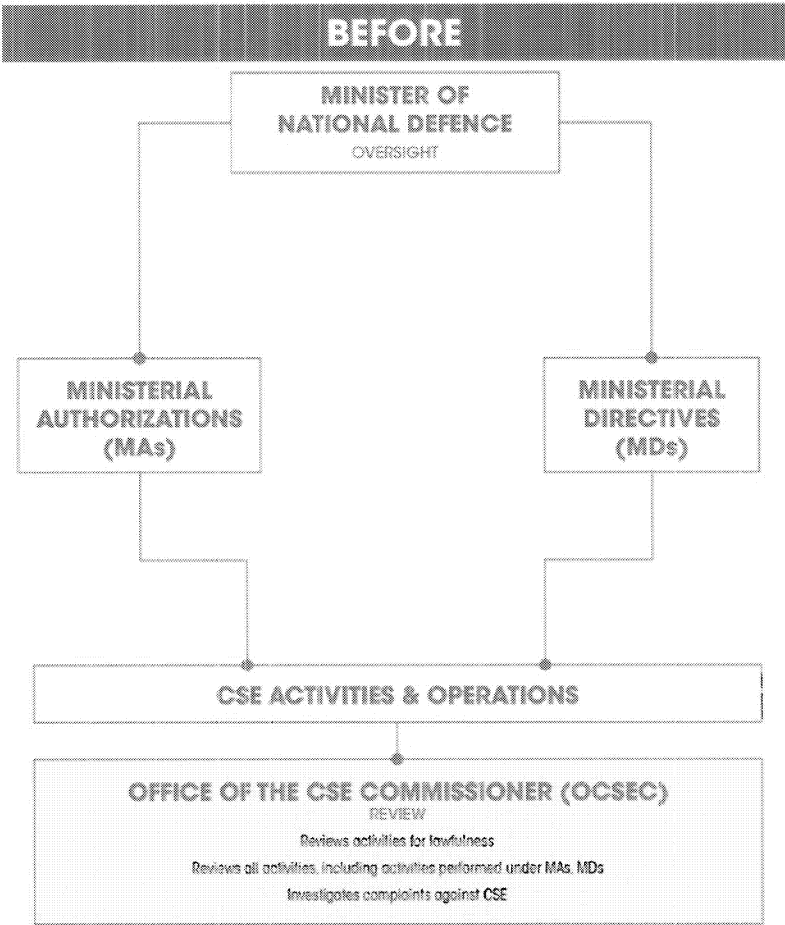
DEFENSIVE CYBER OPERATIONS
Disrupting foreign cyber threats targeting important Canadian networks
ACTIVE CYBER OPERATIONS
Interfere with foreign online efforts that threaten Canada

INCREASED ACCOUNTABILITY MEASURES

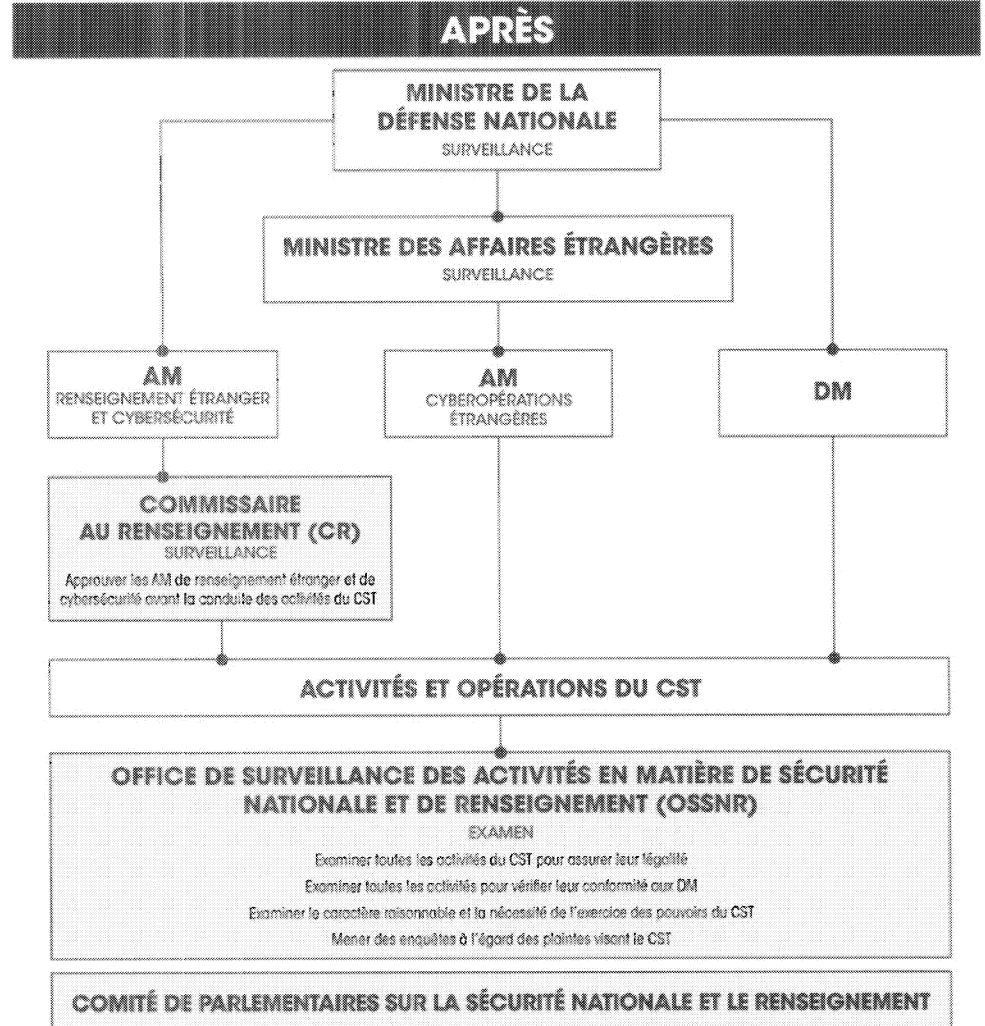
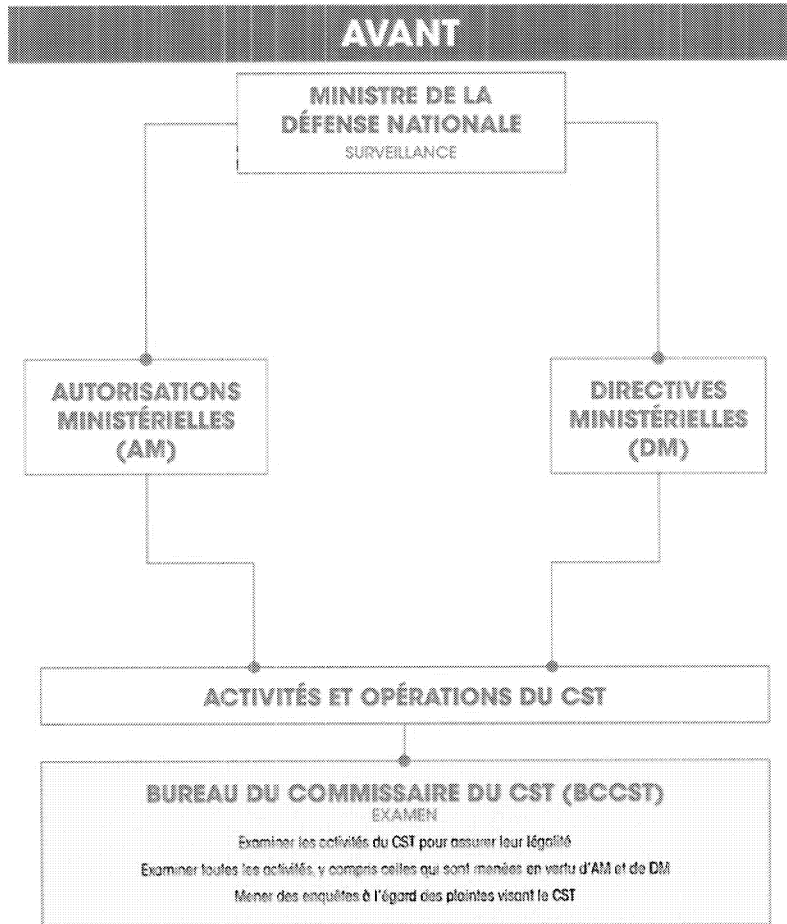
POUVOIRS PROPOSÉS ET CAPACITÉS DU CST



CSE ACCOUNTABILITY BEFORE & AFTER THE CSE ACT



REDDITION DE COMPTES DU CST AVANT ET APRÈS LA LOI SUR LE CST



Charter Statement - Bill C-59: *An Act respecting national security matters*

Tabled in the House of Commons, June 20, 2017

Explanatory Note

The Minister of Justice prepares a “Charter Statement” to help inform public and Parliamentary debate on a government bill. One of the Minister of Justice’s most important responsibilities is to examine legislation for consistency with the *Canadian Charter of Rights and Freedoms* [“the Charter”]. By tabling a Charter Statement, the Minister is sharing some of the key considerations that informed the review of a bill for consistency with the Charter. A Statement identifies Charter rights and freedoms that may potentially be engaged by a bill and provides a brief explanation of the nature of any engagement, in light of the measures being proposed.

A Charter Statement also identifies potential justifications for any limits a bill may impose on Charter rights and freedoms. Section 1 of the Charter provides that rights and freedoms may be subject to reasonable limits if those limits are prescribed by law and demonstrably justified in a free and democratic society. This means that Parliament may enact laws that limit Charter rights and freedoms. The Charter will be violated only where a limit is not demonstrably justifiable in a free and democratic society.

A Charter Statement is intended to provide legal information to the public and Parliament. It is not intended to be a comprehensive overview of all conceivable Charter considerations. Additional considerations relevant to the constitutionality of a bill may also arise in the course of Parliamentary study and amendment of a bill. A Statement is not a legal opinion on the constitutionality of a bill.

Charter Considerations

The Minister of Justice has examined Bill C-59, *An Act respecting national security matters*, for consistency with the Charter pursuant to her obligation under section 4.1 of the *Department of Justice Act*. This review involved consideration of the objectives and features of the Bill.

What follows is a non-exhaustive discussion of the ways in which Bill C-59 potentially engages the rights and freedoms guaranteed by the Charter. It is presented to assist in informing the public and Parliamentary debate on the Bill.

Overview

Bill C-59 proposes a number of measures to enhance Canada’s national security framework with a view to keeping Canadians safe and also respecting and upholding Charter-protected rights and freedoms and the values of our free and democratic society. These proposals have been informed

by public consultations undertaken over the past year as well as by the need to ensure Canada's national security framework keeps pace with developments in the current threat environment.

Bill C-59's centerpiece is the proposed creation, in **Part 1**, of a new National Security and Intelligence Review Agency (NSIRA) through the *National Security and Intelligence Review Agency Act*. The NSIRA would be staffed by members appointed by the Governor in Council for a term not exceeding five years (with the possibility of a single re-appointment). The NSIRA would review and report in an integrated manner on the lawfulness of all national security and intelligence activities across government, thereby enhancing accountability, transparency and the safeguarding of human rights in Canada in relation to national security measures. The NSIRA would also investigate complaints in relation to actions by the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE), and the Royal Canadian Mounted Police (RCMP), and in relation to denials of security clearance.

The NSIRA would be required to review and report on certain matters on an annual basis, and would otherwise have full and independent authority to determine what other activities to review. Findings and recommendations from the NSIRA would be provided to relevant Ministers through classified reports, including on relevant agencies' compliance with the law and the reasonableness and necessity of the exercise of their powers. The NSIRA would also submit an annual report of its activities, findings and recommendations to the Prime Minister for tabling in Parliament. This new entity would complement the important work of the proposed National Security and Intelligence Committee of Parliamentarians. Together, they would provide comprehensive scrutiny of Canada's national security and intelligence activities.

In addition, **Part 2** of Bill C-59, the *Intelligence Commissioner Act*, would establish an independent, quasi-judicial Intelligence Commissioner, who would assess and review certain Ministerial decisions regarding intelligence gathering and cyber security activities. This would ensure an independent consideration of the important privacy and other interests implicated by these activities in a manner that is appropriately adapted to the sensitive national security context.

Several proposed new restrictions, safeguards and accountability measures in **Parts 3 and 4** would respond to concerns about the Charter-consistency of the mandates and powers of CSE and CSIS. In addition, these parts would provide these agencies with much-needed and updated intelligence gathering and threat reduction tools in order to address current and emerging threats to security. These new measures have been carefully tailored to respect privacy and liberty, while also enabling the effective protection of Canadians' safety and the security of Canada.

Part 5 would clarify disclosure and accountability provisions in the newly re-named *Security of Canada Information Disclosure Act*. This would facilitate the effective and responsible sharing of information already in the possession of the Government of Canada that would in turn help agencies respond to threats to national security, while respecting Canadians' rights to freedom of expression and privacy.

Proposed changes to the *Secure Air Travel Act* in **Part 6** would bring greater coherence and efficiency to Canada's secure air travel regime, while at the same time respecting privacy and

ensuring that persons who do not pose a risk to air safety can be de-listed in a timely manner in the event they are identified in error.

Changes to the *Criminal Code* proposed in **Part 7** would clarify and limit the scope of certain terrorism offences, as well as ensure that preventive anti-terrorism measures keep Canadians safe and respect their rights and freedoms.

The main Charter-protected rights and freedoms potentially engaged by the proposed measures include:

- ***Freedom of expression (section 2(b))*** – Section 2(b) of the Charter provides broad protection of all forms of expression. However, section 2(b)'s protection does not extend to expression that takes the form of violence or threats of violence.
- ***Right to life, liberty and security of the person (section 7)*** – Section 7 of the Charter guarantees to everyone the right to life, liberty and security of the person, and the right not to be deprived thereof except in accordance with the principles of fundamental justice. These principles require that laws which engage these rights must not be arbitrary, overbroad, grossly disproportionate or vague. An arbitrary law is one that impacts section 7 rights in a way that is not rationally connected to the law's purpose. An overbroad law is one that impacts section 7 rights in a way that, while generally rational, goes too far by capturing some conduct that bears no relation to the law's purpose. A grossly disproportionate law is one whose effects on section 7 rights are so severe as to be "completely out of sync" with the law's purpose. A vague law is so unintelligible as to be incapable of judicial interpretation. These principles also require that any measures that engage the right to life, liberty or security of the person respect basic principles of procedural fairness, including the right to be heard and the right to know the case against you.
- ***Right to be secure against unreasonable search or seizure (section 8)***: Section 8 of the Charter protects people against "unreasonable" searches and seizures of their person, property and private information. The purpose of section 8 is to protect individuals from unjustified intrusions upon their privacy. A search or seizure will be reasonable if it is authorized by a law, the law itself is reasonable in the sense of striking an appropriate balance between privacy interests and the state interest being pursued, and the search is carried out in a reasonable manner.

Part 3: The *Communications Security Establishment Act*.

CSE is Canada's national signals intelligence agency for foreign intelligence. CSE is also Canada's technical authority for cybersecurity and information assurance.

- Signals intelligence is the interception and analysis of communications and other electronic signals, including any form of electronic communications, such as telephone calls and text messages, computer and internet communications, and satellite signals.
- Cybersecurity and information assurance is about protecting government and other critical computer networks and systems from foreign states, hackers and criminals.

CSE is currently governed by the *National Defence Act*. Part 3 of Bill C-59 proposes to enact a stand-alone *Communications Security Establishment Act* to establish CSE in statute, and to authorize and regulate its activities. The proposed Act would modernize CSE's legal regime, and maintain the general restriction against CSE directing its activities at Canadians and persons in Canada. It would authorize CSE to use certain online techniques to collect foreign intelligence, to identify foreign threats to Canada and to take action online to proactively address threats. It would authorize CSE to extend its cyber protection activities to include private networks of importance to the Government of Canada, with the consent of the owner or operator of the network. It would enable CSE to provide technical and operational assistance to the Department of National Defence and the Canadian Forces. It would also add new privacy and accountability measures, including an approval role for the new Intelligence Commissioner.

Mandate

CSE's mandate would have five aspects according to section 16(2) of the proposed Act: (i) foreign intelligence; (ii) cybersecurity and information assurance; (iii) defensive cyber operations; (iv) active cyber operations; and (v) technical and operational assistance. Each aspect has the potential to affect Charter rights and freedoms in different ways, which will be addressed in turn.

(i) Foreign intelligence

The foreign intelligence aspect of CSE's mandate is to acquire information from the global information infrastructure (GII) (e.g., the Internet and telecommunications networks) for the purpose of providing foreign intelligence to the Government of Canada in accordance with its intelligence priorities. The acquisition of information from the GII must be authorized by the Minister where the activity to acquire it would otherwise be unlawful (subsection 23(3)) or where there is a privacy interest in it.

The Minister authorizes such activities under section 27 of the Act by issuing a Foreign Intelligence Authorization. This authorization must also be approved by the independent, quasi-judicial Intelligence Commissioner before it takes effect (section 29). Information that can be acquired includes the private communications of individuals and private information concerning individuals, including metadata with a privacy interest. Although CSE is prohibited by subsection 23(1) from directing its activities at Canadians or persons in Canada, the practical realities of acquiring information from the GII means that despite best efforts to avoid it, CSE may incidentally obtain private communications and other private information of Canadians and persons in Canada.

In order to provide foreign intelligence, CSE may need to acquire information in an unselected form due to technical and operational reasons. CSE would then apply selection terms or criteria to this unselected information in order to obtain information of foreign intelligence interest.

Section 8 of the Charter protects against "unreasonable" searches and seizures. Because the authority to acquire private information through the GII has the potential to interfere with privacy interests, it may engage section 8.

The following considerations support the consistency of the foreign intelligence mandate with section 8 of the Charter. The acquisition of information from the GII would serve the compelling purpose of providing foreign intelligence to the Government of Canada. This would include information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as it relates to Canada's international affairs, defence or security. This information on its own or in combination with other classified and unclassified information can help provide a comprehensive view and unique insight to the government on potential threats and issues facing Canada.

Generally, before foreign intelligence activities could interfere with privacy interests, they would first have to be authorized by the Minister upon written application by the Chief of the Communications Security Establishment. A key change proposed in Bill C-59 is that the activities would also have to be approved in advance by the independent Intelligence Commissioner, who is a retired superior court judge with the capacity to act judicially.

Authorized activities would be directed outside Canada at foreign individuals and entities; no activities could be directed at Canadians or persons in Canada (section 23). In order to issue an Authorization, the Minister would have to have reasonable grounds to believe that it would be reasonable and proportionate to do so having regard to the nature of the activities and of their objective (subsection 35(1)). This would require taking into account the benefits to be achieved by the activities and any anticipated impact on privacy interests.

In addition, the Act imposes several other requirements aimed at mitigating privacy impacts. In order to issue an authorization, the Minister would have to have reasonable grounds to believe that the information to be acquired could not reasonably be acquired by other means, and that it would not be retained longer than reasonably necessary. With respect to any Canadian information incidentally collected, the Minister would also need reasonable grounds to believe that measures would be in place to ensure that it would only be used or retained if "essential" to CSE's foreign intelligence mandate.

Finally, in order to approve the issuance of an Authorization to make it valid so that it can legally authorize any activities, the Intelligence Commissioner would have to find the Minister's conclusions in the foregoing respects to be "reasonable" (subsection 21(1) of the *Intelligence Commissioner Act*).

In addition, section 25 of the Act would impose an overall obligation on CSE to have measures in place to protect the privacy of Canadians and of persons in Canada in the use, retention and disclosure of information related to them that would be acquired in the furtherance of the foreign intelligence aspect of the mandate.

(ii) Cybersecurity and information assurance

CSE's mandate would also continue to be to access and acquire information from the GII for the purpose of providing advice, guidance and services to the Government of Canada to help protect its electronic information and information infrastructure, as well as any other electronic information or information infrastructure designated by the Minister as being of importance to the Government of Canada. As with the foreign intelligence mandate, any acquisition of

information from the GII would have to be authorized by the Minister where the activity to acquire it would otherwise be unlawful (subsection 23(3)) or where there is a privacy interest in it.

The Minister authorizes such activities under section 28 of the Act by issuing a Cybersecurity Authorization. This authorization would also have to be approved by the independent, quasi-judicial Intelligence Commissioner before it takes effect (section 29). Information that could be acquired includes the private communications of individuals and private information concerning individuals, although CSE would be prohibited by subsection 23(1) from directing its activities at Canadians or persons in Canada. Nonetheless, given the practical realities of acquiring information from the GII, in particular as it relates to information concerning Government of Canada institutions and infrastructure, CSE may incidentally obtain private communications and other private information of Canadians and persons in Canada.

These activities have the potential to engage section 8 of the Charter. The following considerations support the consistency of the cybersecurity and information assurance mandate with the Charter. Information acquired from the GII would serve the compelling purpose of providing advice, guidance and services to protect Government of Canada and designated electronic information and information infrastructure. These critical networks are under a constant state of attack from cyber threats at the same time as their importance to the security and prosperity of Canada is ever increasing. Both the integrity of the networks, and the security of the valuable governmental information accessible through them, including personal information, must be protected.

As with foreign intelligence activities, before cybersecurity activities could interfere with privacy interests, they would first have to be authorized by the Minister upon written application by the Chief, and then approved by the independent, quasi-judicial Intelligence Commissioner.

Authorized activities would not be directed at Canadians or persons in Canada (section 23). Nor could an authorization be issued for activities in relation to a non-government network without the written request of the network owner (subsection 34(3)).

In order to issue an Authorization, the Minister would have to have reasonable grounds to believe that it would be reasonable and proportionate to do so, having regard to the nature of the activities and of their objective (subsection 35(1)). This would require taking into account the benefits to be achieved by the activities and any anticipated impact on privacy interests.

In addition, the Act imposes several other requirements aimed at mitigating privacy impacts (subsection 35(3)). The Minister would have to have reasonable grounds to believe that information acquired would be retained no longer than reasonably necessary and that consent could not be reasonably obtained for the acquisition of any information. In addition, the Minister could only issue an authorization if they conclude that there are reasonable grounds to believe that any information to be acquired is “necessary” to identify, isolate, prevent or mitigate harm to Government of Canada or designated electronic information or infrastructure. Necessity is a stringent standard that ensures that privacy interests are not invaded unless required to protect cybersecurity. With respect to any Canadian information incidentally collected, the Minister

would also need reasonable grounds to believe that measures would be in place to ensure that it would only be used or retained if “essential” to the cybersecurity aspect of the mandate.

Finally, in order to approve the issuance of an Authorization to make it valid so that it can legally authorize any activities, the Intelligence Commissioner would have to find the Minister’s conclusions in the foregoing respects to be “reasonable” (subsection 21(1) of the *Intelligence Commissioner Act*).

Again, section 25 of the Act would impose an overall obligation on CSE to have measures in place to protect the privacy of Canadians and of persons in Canada in the use, retention and disclosure of information related to them that would be acquired in the furtherance of the cybersecurity aspect of the mandate.

(iii) Defensive cyber operations

Another aspect of CSE’s mandate would be to carry out activities on or through the GII to protect the Government of Canada’s electronic information and information infrastructure, and other designated electronic information or information infrastructure. In pursuing this defensive cyber operations aspect of its mandate, the Act would prohibit CSE from directing its activities at Canadians or persons in Canada, or at any portion of the GII in Canada (section 23). Defensive cyber activities would have to be authorized by the Minister, in consultation with the Minister of Foreign Affairs (section 30).

The provisions authorizing defensive cyber operations would not by definition engage Charter rights or freedoms. However, specific activities authorized under this scheme could potentially engage rights or freedoms.

The following considerations support the consistency of this aspect of the mandate with the Charter. First, the purpose of defensive cyber operations would be to further the government’s compelling need to protect critical infrastructure. Also, the nature of any potential effects on Charter rights and freedoms would be limited by the prohibition on activities that would cause, intentionally or by criminal negligence, death or bodily harm, or that would willfully attempt in any way to obstruct, pervert or defeat the course of justice or democracy in any country (section 33). Further, no activities directed at Canadians or persons in Canada could be authorized; only activities aimed outside Canada at foreign individuals, entities and the GII outside of Canada would be permitted. Following the decision of the Supreme Court of Canada in *Doré v. Barreau du Québec* (2012), the Charter may also require the Minister to take relevant “Charter values” into account in exercising a discretion to issue an authorization.

As with other authorizations, the Minister would have to meet the reasonable grounds to believe standard in relation to the following factors that serve to mitigate potential rights impacts: that any activity to be authorized is reasonable and proportionate in light of its nature and objective (subsection 35(1)); that “the objective of the cyber operation could not reasonably be achieved by other means”; and that no information would be acquired through the activities unless otherwise authorized under a Foreign Intelligence, Cybersecurity or Emergency Authorization (subsection 35(4)).

As the acquisition of a Canadian's or person in Canada's private information would not be authorized under this mandate, the prior approval of the Intelligence Commissioner is not required. However, activities under the authorization would be subject to review by the NSIRA (paragraph 8(1)(a) of the *National Security and Intelligence Review Agency Act*), which can make findings with respect to CSE's compliance with the law and the reasonableness and necessity of CSE's exercise of its powers (paragraphs 8(3)(a) and (b)).

(iv) Active cyber operations

Another aspect of CSE's mandate would be to carry out activities on or through the GII to degrade, disrupt, influence, respond to or interfere with foreign individuals, states, organizations or terrorist groups to further the government's international affairs, defence, or security objectives. As with defensive cyber operations, the Act would prohibit CSE from directing its activities at Canadians or persons in Canada, or at any portion of the GII in Canada (section 23). Active cyber activities would also have to be authorized by the Minister, with the consent of the Minister of Foreign Affairs or at the request of that Minister (section 31).

The provisions authorizing active cyber operations would not by definition engage any Charter rights or freedoms. However, specific activities authorized under this scheme could potentially engage rights or freedoms. The considerations that support the consistency of this aspect of the mandate with the Charter are very similar to those supporting the consistency of the defensive cyber operations mandate. One difference is the distinct purpose of active cyber operations, which would be to further the government's compelling objectives in relation to Canada's international affairs, defence or security (section 20).

(v) Technical and operational assistance

The final aspect of CSE's mandate would be to provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence. In so doing, CSE's legal authority to act would be the same as the authority of the agency or entity it is assisting. Although these assistance activities have the potential to engage Charter rights and freedoms, this would be pursuant to existing legal authorities such as *Criminal Code* or *Canadian Security Intelligence Service Act* warrants, or the Crown's prerogative to deploy Canadian Forces on international military operations.

Emergency authorizations

Section 41 of the proposed Act would enable the Minister to issue, on an exception basis, an emergency Foreign Intelligence Authorization or Cybersecurity Authorization without the prior approval of the Intelligence Commissioner. This could be done where the Minister has reasonable grounds to believe that the time required to obtain the Intelligence Commissioner's approval would defeat the purpose of issuing an Authorization.

Because the activities that could be authorized under section 41 have the potential to acquire private communications and private information, including incidentally about Canadians and persons in Canada, section 8 of the Charter is potentially engaged.

The following considerations support the consistency of the emergency authorization power with the Charter. The authority would be exceptional, its use confined to narrow circumstances where important government objectives would be at stake that would not be furthered without timely action. Except for the independent, quasi-judicial Intelligence Commissioner's prior approval, all other privacy protecting and mitigating conditions for the issuance of an ordinary Foreign Intelligence or Cybersecurity Authorization would have to be met by the Minister in issuing an Emergency Authorization. To enable accountability, NSIRA and the Intelligence Commissioner would both need to be promptly notified of any use of the power (section 42). Finally, an Emergency Authorization would be valid for no more than five days (section 43).

Publicly available information

The general prohibition against CSE directing its activities at Canadians or persons in Canada would not prevent it from acquiring and using "publicly available information", including information about Canadians (paragraph 24(1)(a)). Such information includes what has been published or broadcast, and what is available to the public upon request or by purchase or subscription (section 2). Considering the information about individuals that can be aggregated, and the things that can be learned from such aggregations using modern technologies and then offered for sale by data-brokers, CSE's acquisition and use of such information, for example, has the potential to affect privacy interests protected by section 8 of the Charter.

The following considerations support the consistency of the authority to acquire and use publicly available information. The acquisition and use of information already in the public realm would generally not intrude upon protected privacy interests. Where it would, the level of privacy expectation that could be affected would generally be low by virtue of the fact of prior public exposure. In any event, publicly available information could only be acquired and used for compelling purposes in support of CSE's mandate. Any such information acquired would be subject to appropriate measures to protect privacy (section 25).

Disclosure of Canadian identifying information

Section 44 of the proposed Act would authorize CSE to disclose to designated persons, including government clients and allies, information that could be used to identify a Canadian or a person in Canada if it concludes that doing so "is necessary to international affairs, defence, security or cybersecurity". The disclosure of potentially private information has the potential to engage section 8 of the Charter.

The following considerations support the consistency of this disclosure authority with the Charter. The Canadian identifying information in question would have been incidentally acquired following the approval of the Intelligence Commissioner -- an independent, quasi-judicial decision-maker -- and retained following a determination by CSE that it is "essential" to CSE's mandate. Disclosures would be made on a case-by-case basis. Although the information in question is already in the possession of the government, the Supreme Court of Canada has indicated that individuals may nonetheless retain a "residual" privacy interest in relation to such information and its treatment by the government. If a residual privacy interest is retained in relation to a Canadian's or person in Canada's identity, its disclosure under this authority could

be considered proportionate to CSE's compelling foreign intelligence and cybersecurity objectives. The requirement that the disclosure be "necessary" to CSE's pressing objectives is a stringent one that ensures that any residual privacy interests are only affected if it furthers the government's important international affairs, defence, security or cybersecurity interests.

Disclosure of information from cybersecurity and information assurance activities

Section 45 of the proposed Act would authorize CSE to disclose information acquired in the course of cybersecurity and information assurance activities to designated persons, including government clients, allies and owners of information infrastructure of importance to the Government of Canada, if necessary to help protect federal or designated electronic information or information infrastructure. Such information could include incidentally intercepted private communications of Canadians or persons in Canada. The disclosure of such communications in particular has the potential to engage section 8 of the Charter.

The following considerations support the consistency of this disclosure authority with the Charter. The disclosure would include information acquired under Ministerial authorization following the approval of the Intelligence Commissioner – an independent quasi-judicial decision-maker – and retained following a determination by CSE that it is "essential" to CSE's mandate, as well as information provided to CSE by cybersecurity clients for the purpose of cybersecurity and technical assurance activities. Disclosures would be made on a case-by-case basis. Any effect on an individual's residual privacy interest could be considered proportionate to CSE's compelling cybersecurity and information assurance objectives. The requirement that the disclosure be "necessary" to CSE's pressing objectives is a stringent one that ensures that any residual privacy interests are only affected if it furthers the government's important interests in protecting federal or designated electronic information and information infrastructure.

Urgent circumstances

The restriction against CSE directing its activities at Canadians or persons in Canada would not prevent it from using and analyzing Canadian information if it has reasonable grounds to believe that there is an imminent danger of death or serious bodily harm to any individual, and that the information will be relevant to that imminent danger (section 47). It may also disclose the information to an appropriate person to help prevent the death or serious bodily harm. The information giving rise to the reasonable grounds to believe may have been incidentally discovered by CSE in the course of authorized activities, or may be provided by another agency or individual. The use and disclosure of potentially private information in these circumstances may engage section 8 of the Charter.

The following considerations support the consistency of the proposed authority with the Charter. The purpose of any invasion of privacy would be of the utmost importance, namely to prevent imminent death or serious bodily harm. Such an objective may serve to justify the use of information already in CSE's possession. To enable accountability for such use or disclosure of Canadian information, the Minister and the NSIRA would be notified (subsection 47(3)).

Role of the National Security and Intelligence Review Agency (NSIRA)

Under the new *National Security and Intelligence Review Agency Act*, the NSIRA would have the authority to review all of CSE's activities, including for compliance with the law, and for compliance with any authorizations issued by the Minister and any approved by the Intelligence Commissioner. It would be broadly empowered to access information to conduct its reviews (section 9). The NSIRA would report annually to the Minister on CSE's activities, including CSE's compliance with the law and the reasonableness and necessity of the exercise of its powers (section 33). In the case of any observed non-compliance with the law, the NSIRA would have to report to the Minister, and to the Chief (section 35). The Minister would then have to inform the Attorney General of Canada. The NSIRA would also have to report annually to the Prime Minister on its activities, findings and recommendations, including any reviews and findings in relation to CSE's activities (section 38). The Prime Minister in turn would have to cause that report to be laid before each House of Parliament.

The creation of the NSIRA with authority to review and publicly report on CSE's compliance with the law is an important accountability measure. This may be particularly relevant to the Charter consistency of CSE activities that potentially engage privacy interests, such as those authorized under Foreign Intelligence, Cybersecurity, and Emergency Authorizations, as well as disclosures of information in urgent circumstances and to advance foreign intelligence and cybersecurity objectives. Any such privacy effects would occur in circumstances in which persons affected may be unaware of the intrusion and so unable to bring potential concerns to court. Enabling an independent body to review and, in particular, publicly report on CSE's compliance with the law supports the reasonableness of the law authorizing CSE's activities.

Apart from privacy-related considerations, NSIRA's mandate may contribute to the constitutionality of any other potential Charter effects. To the extent that individuals may be unaware of effects on their rights and freedoms due to the covert nature of CSE's activities, the NSIRA's ability to review activities and publicly report on any observed non-compliance would create an effective accountability measure to secure compliance with the law.

Prohibition on disclosure

With certain exceptions, section 56 would prohibit the disclosure, in a proceeding before a court, person, or body with jurisdiction to compel the production of information, of the identity of a person or entity that has assisted or is assisting CSE on a confidential basis, or any information from which the identity of such a person or entity could be inferred.

A designated judge of the Federal Court would be able to authorize disclosure of the information in two instances; (1) if the judge is of the opinion that the individual is not a person or entity that is assisting or has assisted CSE or if the identity of such a person could not be inferred from such information; and (2) in the case of a proceeding that is a prosecution of an offence, where disclosure of the identity or information from which the identity could be inferred is essential to establish the accused's innocence.

The purpose of the section is to ensure that the identity of persons or entities that assist CSE would be kept confidential in order to protect their security and to encourage individuals or

entities to provide assistance to CSE. The intention is to protect the identity of persons who provide assistance to CSE and any information from which their identity could be inferred.

The prohibition on disclosure has the potential to engage section 7 of the Charter where the identity of the individual or information from which identity can be determined is being relied upon in a proceeding that engages the liberty interest of an individual, such as a criminal prosecution or those related to certain proceedings under the *Immigration and Refugee Protection Act*. Specifically, the prohibition could engage section 7's guarantee of procedural fairness.

The following considerations support the consistency of the prohibition with section 7 of the Charter. In the case of a criminal proceeding, the disclosure of the identity of a person or entity that has assisted or is assisting CSE may be disclosed where it is essential to establish the accused's innocence. This is similar to the common law police informer privilege rule, which has been held to be constitutional as it relates to fair trial rights protected under the Charter. As well, section 38.14 of the *Canada Evidence Act* would apply to give trial judges the authority to order whatever remedy would be required to protect an accused's right to a fair trial, where confidentiality is invoked. If the right of an accused to a fair trial is compromised as a result of the application of the section 38 scheme, the trial judge can use their discretion to put an end to the prosecution.

In the case of certain proceedings under Division 9 (Certificates and Protection of Information) of the *Immigration and Refugee Protection Act*, the Federal Court judge has the obligation to ensure the confidentiality of the information regarding the identity of the person or entity. The judge would need to fulfill this obligation while ensuring that the person named in a security certificate is reasonably informed of the case to meet. This could include, for example the provision of a summary of the information, without disclosing the identity of the entity who has provided assistance to CSE or any information from which the identity could be inferred.

Part 4: *Canadian Security Intelligence Services Act* Amendments

Datasets

The ability to acquire, retain and analyze data is important to CSIS in exercising its mandate. Datasets, comprised of sets of personal information stored as an electronic record and characterized by a common subject matter, can include information that is not directly and immediately related to threats to the security of Canada. Analysis of these datasets nevertheless can be of significant assistance to CSIS in investigating such threats.

Recent Federal Court jurisprudence, *Re X* (2016), indicates that the existing provisions of the *CSIS Act* do not provide CSIS with the authority to collect and retain data that has no direct connection with a security threat. The Court indicated, however, that the Act is showing its age and suggested renewed consideration of the proper tools CSIS needs for its operations.

Proposed amendments at clauses 94, 96-97, and 107-108 would amend the *CSIS Act* to provide CSIS the authority to collect, retain and use datasets. Subsection 11.05(1) provides a general

authority for CSIS to collect datasets that contain personal information that does not directly and immediately indicate activities representing a threat to the security of Canada. Where a dataset is publicly available, section 11.11 provides a general authority to retain and use it and to retain the results of its use. For datasets that are not publicly available, additional requirements apply.

If the personal information in a dataset predominately relates to Canadians or non-Canadians within Canada (“Canadian datasets”), sections 11.03, 11.07(2), 11.08, and 11.12(2) require that it can only be retained if it falls within a category authorized by the Minister of Public Safety and approved by the independent, quasi-judicial Intelligence Commissioner. Judicial authorization is required to retain any Canadian dataset, as provided under sections 11.12-11.15. If the personal information in a dataset relates to non-Canadians outside of Canada (“foreign datasets”), retention requires authorization by the Minister of Public Safety and Emergency Preparedness or the Minister’s designate and approval by the Intelligence Commissioner, as provided under sections 11.16-11.19.

Other safeguards apply to the authority to retain Canadian and foreign datasets. These include a requirement to delete any private information about physical or mental health and, for Canadian datasets, to delete any information subject to solicitor-client privilege, at section 11.1. The safeguards also include a requirement to remove information from foreign datasets that relates to Canadians and persons in Canada.

In addition to the requirements that apply in connection to retention, conditions apply to the use of Canadian and foreign datasets. Section 11.2 requires that use of these datasets through specific queries (in relation to a person or entity) or by exploitation (analysis of trends) must respect a “strictly necessary” standard, or be required to assist the Minister of Defence or the Minister of Foreign Affairs under existing section 16 of the *CSIS Act* (relating to information or intelligence about foreign states and about persons who are not Canadians or permanent residents of Canada). Foreign datasets also may be used to the extent that this is “strictly necessary” for the purpose of section 15 of the CSIS mandate (security clearances). Analogous standards apply to the communication and retention of the results of such use. Under subsection 11.24(3), CSIS must take reasonable measures to ensure that designated employees communicate information held in a dataset – or resulting from the querying or exploitation of a dataset – only in accordance with the *CSIS Act*. Use of datasets prior to authorization for retention is subject to a strictly-controlled exception in exigent circumstances, at sections 11.22-11.23, to preserve the life or safety of an individual or to gain intelligence of significant importance to national security that otherwise would be lost or diminished by the delay.

Section 11.24 obligates CSIS to establish record keeping requirements for the querying and exploitation of a Canadian or foreign dataset and the results of this use; it also obliges CSIS to establish such requirements for the exploitation of a publicly available dataset and for the results of querying and exploitation of such datasets. This information must be made available to the NSIRA. If the NSIRA is of the opinion that CSIS actions in querying or exploiting datasets may not be in compliance with the law, including the Charter, section 27.1 requires the Director to provide a copy of that report to the Chief Justice of the Federal Court. The Court is to review the information filed and determine if CSIS use of datasets complied with the law. The Court may issue a direction, make an order or take any other measure the Court deems appropriate.

In addition, clause 102, amending section 21 of the *CSIS Act*, would allow information incidentally collected under an existing section 21 warrant to be retained under judicial authorization and to be deemed a dataset that has been collected, but which then becomes subject to the other requirements of the Act for retention and use.

The proposed dataset measures could engage privacy interests protected by section 8 of the Charter.

The following considerations support the consistency of the dataset provisions with the Charter. The overall reasonableness of the datasets regime must be considered within the context in which it operates, namely intelligence gathering for national security purposes (not law enforcement). The new provisions give CSIS clear authority to collect datasets relevant to its mandate and subjects their retention and use to a number of accountability and review mechanisms. The initial collection authority requires CSIS to assess the privacy interests engaged by the datasets. During this assessment period, the datasets cannot be used except in exigent circumstances. The information in datasets is otherwise strictly segregated during this period, with access only by designated CSIS employees conducting the assessment. Retention of Canadian datasets requires judicial authorization. Retention of a foreign dataset requires Ministerial authorization. The distinction in the authorization approach to foreign datasets, as compared with that of Canadian datasets, is analogous to the established model for foreign information acquired by CSE, which is also addressed in Part 3 of Bill C-59. Control on retention is further strengthened by the approval role played by the independent, quasi-judicial Intelligence Commissioner.

Although dataset use is not subject to judicial pre-authorization, it is subject, where appropriate, to the requirement that the use of datasets be “strictly necessary” to enable CSIS to perform its intelligence gathering or threat reduction mandates. Information on use is made available to the NSIRA. If the NSIRA makes a finding or recommendation that CSIS actions in this use are contrary to statute or the Charter, the dataset measures provide that the Director must give this portion of the report to Federal Court, which then can consider the matter and provide a remedy. Key controls, including a judicial role and accountability requirements, are incorporated in the dataset provisions so as to limit impacts on privacy interests.

Threat Reduction Measures

Bill C-51, enacted by a previous Parliament (S.C. 2015, c. 20), provided a new power for CSIS to take measures to reduce threats to the security of Canada. This included a requirement, at existing subsection 12.1(3) of the *CSIS Act*, that “The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1.” Section 21.1 was also enacted under previous Bill C-51 to provide authority for such a warrant.

These provisions have been viewed as potentially giving authority for warrants that would authorize violations of the Charter or other Canadian law. Clauses 98 and 99 propose amendments to the Act’s threat reduction provisions to clarify that any threat reductions

measures undertaken by CSIS must be Charter-compliant and also that, as authorized under warrant, they must comply with other Canadian law.

To this end, a new provision would be added, reciting that the Charter is part of the supreme law of Canada and that all threat reduction measures taken by the Service must comply with it. Further, the existing provision for judicial oversight of threat reduction measures would be strengthened by a warrant provision that clearly requires CSIS to obtain a warrant before taking any measures that would limit rights or freedoms under the Charter or otherwise be contrary to other Canadian law. Before a warrant could be issued, the judge would have to be satisfied that the measures authorized would be consistent with the Charter. These new provisions are found in subsections 12.1(3.1) to 12.1(3.4) of the CSIS Act.

To further strengthen Charter protections, the warrant provision at section 21.1 would also be amended, at clause 103. Pursuant to existing section 21.1, the judge must be satisfied of the reasonableness and proportionality of the measures. Subsection 21.1(1.1) would add a further requirement expressly restricting the measures that can be taken under warrant to those in a defined list.

Additional new requirements would apply to all threat reduction measures – whether or not under a warrant – including a requirement, as part of the reasonable and proportional standard, that CSIS consider the foreseeable effects on the rights of third parties, including their right to privacy (subsection 12.1(2)). There is also a new requirement to consult, as appropriate, other federal departments and agencies in respect of their ability to reduce the threat.

The list of specifically prohibited threat reduction measures at subsection 12.2(1) would be expanded to include acts of torture or cruel, inhuman and degrading acts, detention of an individual, and causing the loss of or any serious damage to property that would endanger the safety of an individual.

The threat reduction provisions could potentially engage various Charter rights and freedoms, including freedom of expression (section 2(b)) and mobility rights (section 6).

The following considerations support the consistency of the threat reduction regime with the Charter. The new restrictions placed on what types of threat reduction measures may be pursued would significantly limit the potential for any measures to engage Charter protections. Whenever contemplated measures could limit rights and freedoms, their scope would be clearly restricted by section 21.1(1.1). Finally, the requirement of prior judicial authorization would apply and require judicial satisfaction of Charter compliance under a core standard of reasonableness and proportionality.

Framework for justifying CSIS activities

CSIS employees engaged in national security information and intelligence gathering, and those acting at their direction, may sometimes undertake conduct that would constitute offences if not otherwise permitted by law.

Bill C-59 would create a statutory authority for CSIS to engage in reasonable and proportional activities of this nature. The new authority would be similar in nature to section 25.1 of the *Criminal Code*, but adapted to the national security context. For police and other law enforcement officers, and persons acting at their direction, section 25.1 of the *Criminal Code* provides a limited statutory justification regime for “reasonable and proportional” activities that would otherwise constitute offences. That regime does not apply to CSIS employees or to those directed by them. Currently, CSIS relies on Crown immunity as a legal foundation for such activities.

Clause 101 would create the proposed national security justification regime. Sections 20.1(6)-20.1(7) provide for the designation of employees engaging in activities under the regime by the Minister of Public Safety. In emergency situations, temporary designations could be made by the CSIS Director or a designated senior employee, under subsections 20.1(8)-20.1(9). The classes of acts and omissions that could be justified under the regime must be determined in advance by the Minister and approved by the new independent, quasi-judicial Intelligence Commissioner, under subsections 20.1(3)-20.1(5).

Subsection 20.1(11) is the core provision that outlines the justification regime applicable to designated employees. The designated employee must be engaged in information and intelligence collection activity and believe on reasonable grounds that the commission of the act or omission is reasonable and proportional.

Analogous requirements apply to a designated employee directing another person to commit an act or omission that would otherwise constitute an offence (subsection 20.1(15)). Direction of such an act or omission must also be authorized by the Director of CSIS or a designated senior employee. Further, the person directed would be required to believe on reasonable grounds that the employee providing the direction has the authority to do so.

Specific categories of conduct that could **never** be justified are listed at subsection 20.1(18):

- intentionally or with criminal negligence causing death or bodily harm;
- wilfully attempting to obstruct justice;
- violating sexual integrity;
- acts of torture or cruel, inhuman and degrading acts;
- detention of an individual; and
- causing the loss of or any serious damage to property that would endanger the safety of an individual.

Subsections 20.1(21) and (22) also specify that nothing relieves an employee from a requirement to obtain a warrant, or authorizes the infringement of a right or freedom guaranteed by the Charter.

To further strengthen accountability and transparency, the justification regime includes reporting and review provisions, at subsections 20.1(23)-20.1(26). Designated employees must make a report to the Director or a designated senior employee about each instance where an act or omission that would otherwise be an offence was committed or directed by the employee. There

must be a public annual report giving general information about the use of the justification regime. Notice must be given to the NSIRA about identified matters. As with other powers under the *CSIS Act*, the justification measures are subject to review by the NSIRA and to the power of the NSIRA to report on the activities taken under the measures.

Clause 100 would also establish separate exemptions applicable to CSIS employees and persons acting at their direction for particular offences. No employee would be guilty of an offence by reason only that the employee, in the course of their duties and for the sole purpose of establishing a covert identity, makes a false statement about the covert identity or takes specified actions in respect of a false document. The analogous exemption would apply to persons acting at the direction of a CSIS employee. A related exemption from section 368.1 of the *Criminal Code* would be provided for possession and other specified actions with instruments, devices or other things used to commit forgery.

The new justification regime has the potential to engage section 7 of the Charter's guarantees of the right to life, liberty and security of the person, and the right not to be deprived thereof except in accordance with the principles of fundamental justice.

The following considerations support the constitutionality of the justification measures. The nature of any potential effects on Charter rights and freedoms would be limited by the listing of activities that could never be justified. The similar justification for law enforcement officers found at section 25.1 of the *Criminal Code* has existed for many years and has been upheld as constitutional. Notably, in *R. v. Lising* (2010) the British Columbia Court of Appeal found that the Charter did not require prior judicial authorization to ensure the constitutionality of the justification regime. The proposed justification regime is similarly narrow in scope. It incorporates the key limitations of the existing section 25.1 regime, as well as additional restrictions and accountability measures appropriate to the national security context.

Part 5: *Security of Canada Information Disclosure Act*

Bill C-59 proposes amendments to the *Security of Canada Information Sharing Act*, including to clarify the definition of "activity that undermines the security of Canada", to clarify and strengthen the authority to disclose, and to increase accountability for activities carried out under the Act.

The *Security of Canada Information Sharing Act* enacted by Bill C-51, which would be renamed the *Security of Canada Information Disclosure Act*, takes a whole-of-government approach to the dissemination of information already in the possession of the Government of Canada where such dissemination would help respond to activities that undermine the security of Canada. The Act is intended to close gaps in legal authorities, and to facilitate the responsible disclosure of information within the federal government for national security purposes. To this end, Parliament enacted an express authority to disclose information in specified circumstances to those federal government institutions responsible for dealing with activities that undermine the security of Canada.

Clause 115(4) would amend section 2 of the Act to clarify that “advocacy, protest, dissent or artistic expression” are not by themselves “an activity that undermines the security of Canada”. They are only an activity of concern when carried on in conjunction with other activities that meet the definition. This makes clear that information solely about “advocacy, protest, dissent or artistic expression” would not be subject to disclosure under the Act.

Clause 118 would amend section 5 of the Act, which remains the key provision. Section 5 provides the authority for a Government of Canada institution to disclose information in its possession to another Government of Canada institution with jurisdiction or responsibilities in relation to activities that undermine the security of Canada. Clause 118 would strengthen the existing disclosure standard. It would improve upon and replace the existing “relevance” standard, with a new standard stipulating that a government institution may disclose information where satisfied that it would “contribute to the exercise of” the recipient’s jurisdiction or the carrying out of the recipient’s responsibilities. In addition, the amendment would impose a new obligation that when disclosing information the government institution be satisfied that the disclosure “will not affect any person’s privacy interest more than is reasonably necessary in the circumstances.” Finally, clause 118 would require a disclosing institution to inform the recipient as to the accuracy of the information being disclosed and the reliability of its manner of collection.

Clause 119 would impose a record-keeping obligation on disclosing institutions to require the creation and retention of records for each disclosure under the Act, and a further obligation to provide all such records to the NSIRA on an annual basis. Under section 39 of the *National Security and Intelligence Review Agency Act*, the NSIRA would be required to report annually on activities under the *Security of Canada Information Disclosure Act*, informed by the records provided to it by disclosing institutions. These reports would be made public through their tabling in Parliament by the Minister of Public Safety.

To the extent that any expressive activity may also constitute “an activity that undermines the security of Canada”, the disclosure within government of information concerning such an activity may potentially engage section 2(b) of the Charter.

The following considerations support the consistency of the Act with the Charter. Clause 115(4) makes clear that only information concerning an expressive activity that otherwise comes within the definition of “an activity that undermines the security of Canada” could be disclosed. This would clearly narrow the scope of information about expressive activity that could potentially be disseminated within government. The disclosure of information about expressive activity taking the form of violence, directed towards violence, or being intimately connected to violence, would not be considered to limit section 2(b), as such activity falls outside the scope of the Charter’s protection. Information in the possession of the Government of Canada concerning any remaining expressive activity conducted “in conjunction with an activity that undermines the security of Canada” and attracting section 2(b) protection would be liable to disclosure within government for the compelling purpose of protecting the security of Canada. Only information contributing to that purpose would be authorized for disclosure.

The Act may also engage section 8 of the Charter, since it would continue to authorize the disclosure within government of information relevant to responding to activities that undermine the security of Canada. This could include information in which persons have a reasonable expectation of privacy.

The following considerations support the consistency of these powers with the Charter. The purpose of the Act is of the most compelling nature, namely to enable the disclosure within government of information relevant to responding to activities that undermine the security of Canada, in order to make it available to those government institutions mandated to address threats to the security of Canada. The Act does not grant any new authority to collect such information to any institution, and under Bill C-59 would continue to be limited to information that is already in the government's possession. The Act therefore only potentially affects residual privacy interests that may have survived the initial lawful collection of the information under authorities outside of the Act.

Although the Act would continue to enable the disclosure of information without prior judicial or quasi-judicial authorization, proposed amendments would clarify and strengthen the disclosure authority in section 5. In particular, the disclosing institution would need to be satisfied that any disclosure of information would not affect privacy interests more than reasonably necessary in the circumstances, thus minimizing privacy impacts. Also, new accountability measures proposed in clause 119 and in the *National Security and Intelligence Review Agency Act* would enable the independent and external NSIRA to review activities under the Act for lawfulness and to report any findings of non-compliance to Parliament.

Part 6: *Secure Air Travel Act* Amendments

The *Secure Air Travel Act* (SATA) aims to ensure the security of air transportation and to prevent the travel of persons who intend to commit a terrorism act. The main impact of the proposed amendments to SATA would be to centralize the process for collecting passenger information to facilitate accurate screening of persons suspected of posing a threat to aviation security, while also enhancing respect for privacy interests.

Clauses 127 (subsections 6(2) and (3)) and 130 (paragraph 10.2(a)) of Bill C-59 would amend SATA to allow the Minister of Public Safety and Emergency Preparedness to collect information from air carriers or, in certain cases, operators of aviation reservation systems, about each person who is on board or expected to be on board an aircraft for any flight prescribed by regulation in order to screen passengers against the list established under SATA. The targeted information includes the surname, first and middle names, date of birth, gender and any other prescribed information.

Clause 127 (subsection 6(4)) would amend SATA to allow the Minister, the Minister of Transport or any other person or entity mentioned under paragraphs 10(b) to (f) of SATA to ask the air carriers or, in certain cases, operators of aviation reservation systems for information about the person who is on board or expected to be on board an aircraft. Subsections 6(5) and (6) would provide limitations as to what may be requested depending on whether the request comes from one of the Ministers or another person or entity.

Clause 134 would reverse the current rule regarding a deemed decision to keep a person on the SATA list, meaning that a person who applies to be removed from the list would now be deemed removed within 120 days of filing their application, unless the Minister takes one of the prescribed steps.

Section 8 of the Charter protects against “unreasonable” searches and seizures. As this Part of the Bill will apply to the collection, disclosure, and retention of personal information, it has the potential to affect privacy interests and therefore may engage section 8 of the Charter.

The following considerations support the consistency of these provisions with the Charter. The centralization of the screening process in order to identify listed persons would enhance the fulfilment of Parliament's pressing objective, which is to ensure the safety of air transportation. The centralized process would enhance the confidentiality of the list and the protection of privacy, since the list would no longer be transmitted systematically to airline companies in order for them to screen and identify listed persons. This would also ensure greater consistency in the screening process and could reduce the number of individuals erroneously identified as being listed and who, as a result, are delayed in their air travels.

The proposed amendments would establish additional rules to protect privacy interests. With regard to the information collected under subsections 6(2) and (3), the Minister could only disclose such information in order to obtain assistance in identifying listed persons who are on board or are expected to board an aircraft if it relates to a person the Minister has reason to believe is a listed person (paragraph 10.3(1)(a)). Under subsection 10.3(2), the Minister could again only disclose information provided under subsections 6(2) and (3) for the purpose of ensuring transportation security or preventing travel to commit a terrorist act if the information relates to a listed person.

With regard to other information obtained under SATA, section 11 would only authorize the Minister to disclose information in order to ensure transportation security or to prevent the travel of a person who intends to commit a terrorist act. Additionally, section 12 would authorize the Minister to enter into a written agreement with a foreign state or international organization relating to the disclosure of any information he or she is permitted to disclose under subsection 10.3(2) and section 11.

Clause 134 would enhance the reasonableness and fairness of the administrative process for those who consider they have been listed in error by making recourse to correct the situation more efficient and transparent.

Lastly, clause 136 would enact a new section 18 to require the destruction of any document or record containing information collected under subsections 6(2), (3) and (4) unless the information is reasonably required for the purposes of SATA. This information must otherwise be destroyed within seven days after the day on which the flight departs or the flight is cancelled.

Part 7: *Criminal Code* Amendments

Counselling commission of terrorism offence

Clause 143 would amend the existing offence of advocating or promoting the commission of terrorism offences in general, to create a more targeted general counselling offence for terrorism offences, whether or not a specific terrorism offence is committed or a specific terrorism offence is counselled.

Section 7 of the Charter guarantees to everyone the right to life, liberty and security of the person, and the right not to be deprived thereof except in accordance with the principles of fundamental justice. Because the revised offence gives rise to the possibility of imprisonment, it engages the section 7 right to liberty and so must respect the principles of fundamental justice. These principles require that laws not be arbitrary, overbroad or grossly disproportionate.

The following considerations support the consistency of the offence with section 7. The offence of counselling requires that the statements, when viewed objectively, actively encourage the commission of a terrorism offence described in them. Courts are familiar with the term “counsel” in the context of criminal law such that the term is not vague. The Supreme Court of Canada has interpreted the act of counselling to be the deliberate encouragement or active inducement of the commission of a criminal offence. Further, the accused must either have intended that the offence be committed or knowingly counselled the commission of the offence while aware of the unjustified risk that the offence counselled was likely to be committed as a result of the accused’s conduct. Clarifying that the offence targets the counselling of the commission of a terrorism offence ensures that the offence is carefully tailored to the government’s objective of deterring and punishing conduct that poses a real risk of harm to Canadians.

The revised offence has the potential to affect freedom of expression as protected by section 2(b) of the Charter, to the extent that it prohibits communications by a person. However, expression taking the form of violence, directed towards violence, or being intimately connected to violence is not protected by section 2(b). The Supreme Court in *R. v. Khawaja* (2012) was clear that this includes threats of violence. The statements covered by this revised offence can, in many cases, be considered as falling within the violence exception to the freedom of expression guarantee. For any other statements that may be caught by the offence, the prohibition may be viewed as a proportional response to the objective of addressing the threat posed by the terrorism offences.

Terrorist propaganda

Clause 144 would amend the definition of terrorist propaganda in subsection 83.222(8) to reflect the wording of the new counselling offence in section 83.221. The ability of a judge to issue a warrant authorizing seizure of any publication where the judge is satisfied that there are reasonable grounds to believe that the publication is terrorist propaganda would remain in the *Criminal Code*.

The provisions could potentially engage expressive activity since the provisions capture any writing, sign or visible representation that meets the definition of “terrorist propaganda”. However, since the definition of “terrorist propaganda” will be restricted to writings, representations or signs that counsel the commission of a terrorism offence, the material to which the provision would apply can, in many cases, be considered as falling within the violence exception and so outside the otherwise broad protection for freedom of expression provided by

section 2(b) of the Charter. For any other statements that may be caught by the offence, the prohibition may be viewed as a proportional response to the objective of addressing the threat posed by the terrorism offences.

Recognizance with conditions and preventive arrest

Clause 146 would amend the recognizance with conditions provision in section 83.3 of the *Criminal Code* to require that a peace officer suspect on reasonable grounds that the recognizance “is necessary” to prevent the carrying out of a terrorist activity. This would change that part of the threshold back to what it had been previous to Bill C-51.

The subsection regarding arrest without a warrant would require a peace officer, before arresting a person without a warrant, to suspect on reasonable grounds that the detention of the person in custody “is necessary” to prevent a terrorist activity. The effect of this amendment would be to revert to the threshold for preventative arrest as it had been prior to Bill C-51.

A person subject to a recognizance is required to keep the peace and be of good behaviour and to comply with any other reasonable conditions imposed by the judge, including the requirement to remain within a specified geographic area or to surrender his or her passport. A breach of the conditions in a recognizance may be punishable by a term of imprisonment. The recognizance can be for a period of up to 12 months, unless the person has previously been convicted of a terrorism offence, in which case the recognizance may be for up to two years.

A law that imposes restrictions or prohibitions affecting one’s ability to move freely – including a recognizance – has the potential to engage the right to liberty protected by section 7 of the Charter. As well, any criminal prohibition that gives rise to the possibility of imprisonment engages the section 7 right to liberty. Any deprivation of liberty must accord with the principles of fundamental justice, which include the principles against arbitrariness, overbreadth and gross disproportionality. They also include the principle that laws not be vague in the way that they are written.

The following considerations support the consistency of the revised scheme with section 7 of the Charter. The purpose of the recognizance scheme is to allow law enforcement to take preventive measures earlier in the investigative process against terrorist acts and to protect the security of Canadians. The threshold that must be met by a peace officer for a judge to issue a recognizance order is proof on a balance of probabilities that there are (a) reasonable grounds to believe that a terrorist activity may be carried out and (b) reasonable grounds to suspect that the recognizance is necessary to prevent the carrying out of that activity. These terms are well understood in Canadian criminal law and courts are capable of interpreting and applying the provisions in a Charter-consistent manner. The pressing preventive objective of the scheme, along with the burden that must be met by the peace officer in order for the order to be made, mean the scheme is carefully tailored to capture only those individuals who pose a real threat of committing (including by participating in) a terrorist activity. Similarly, imposing a threshold of “necessity” for preventive arrest without a warrant mirrors the test for the issuance of the recognizance and ensures that only those individuals who pose a substantial risk of committing a terrorist activity are arrested without a warrant.

Witness protection measures

Clause 154 would amend the *Criminal Code* to indicate that a court may order any of the testimonial aids, publication bans or other measures in sections 486-486.5 and 486.7 to protect a witness or participant in a recognizance with conditions or peace bond hearing. The *Criminal Code* already provides this range of measures to protect witnesses in criminal proceedings, including proceedings involving national security or intelligence information or criminal intelligence information. These include provisions allowing for non-disclosure of a witness's identity, orders permitting a witness to testify behind a screen, or the exclusion of the public from the court room.

This amendment would permit the use of these measures in hearings regarding peace bonds or recognizances, including peace bond hearings that do not involve national security or organized crime. In addition to facilitating the truth-seeking function of these processes, this is a safety enhancing measure for those who will benefit from the expanded availability of witness protection measures.

Section 2(b) of the Charter protects freedom of expression, including the open court principle. Under this principle, there is a presumption that court proceedings are open to both the public and the media. The use of a witness protection measure that limits the openness of, or access to, court proceedings could engage section 2(b).

The following considerations support the consistency of any measures restricting access to court proceedings with the Charter. Except where such measures are mandatory, such as where the victim is under the age of 18 years (subsection 486.4(2.2)), the decision as to what, if any, measures should be taken to protect witnesses would be left to the discretion of the court. In deciding whether to permit the use of witness protection measures, the court would have to balance the competing interests at stake and be of the opinion that the order is in the interest of the proper administration of justice. In determining whether to make an order, the court shall consider a number of factors including: the right to a fair and public hearing; the nature of the offence; whether the witness needs the order to protect their security or identity; whether effective alternatives to the making of the proposed order are available; and the negative versus beneficial effects of the proposed order. Any order by the court would also have to take into consideration the judgments of the Supreme Court in *Dagenais v. Canadian Broadcasting Corp.* (1994) and *R. v. Mentuck* (2001), which govern the discretionary imposition of measures that may interfere with the open court principle, such as a publication ban.

Witness protection measures are designed to facilitate the truth-seeking function of the Court and to encourage witnesses to come forward without fear of recrimination. This may be particularly important in cases involving threats to national security and terrorism, although they also would apply in cases that do not involve national security or organized crime, for example in cases of domestic violence.

Section 7 of the Charter may also be implicated by the use of witness protection measures in hearings for recognizance orders or peace bonds, since these hearings can lead to a restriction on the defendant's liberty, as explained above. Any deprivation of the right to liberty must accord with the principles of fundamental justice, which include the right to a fair hearing, the

opportunity to know the case one has to meet, the opportunity to present evidence and the right to a decision on the facts and the law.

The following considerations support the consistency of these witness protection measures with section 7. The use of witness protection measures is meant to protect the safety and security of witnesses, including persons who work in the area of national security. This facilitates the proper administration of justice by enabling a court to make a determination regarding a peace bond or recognizance on the basis of a full and complete record. The defendant would still be able to cross-examine the witness to test the reliability of their evidence to ensure that the Crown has met its burden of proof in the case. The court would retain the discretion to ensure that the individual's right to a fair hearing is protected when deciding whether to grant a request for various witness protection measures.

Part 8: *Youth Criminal Justice Act* Amendments

Bill C-59 would make a number of amendments to the *Youth Criminal Justice Act* (YCJA) to ensure that all youth who are involved in the criminal justice system due to terrorism-related conduct are afforded the enhanced procedural and other protections that the YCJA provides. Consistent with Canada's international human rights law obligations under treaties such as the United Nations *Convention on the Rights of the Child*, the YCJA recognizes that young people lack the maturity of adults, and incorporates principles and measures that are consistent with this reduced level of maturity. The YCJA encourages the use of measures outside of the formal court system for less serious offences in recognition of the fact that such measures are often the most appropriate and effective way to respond to youth offending. Where formal charges are pursued and a young person is found guilty of an offence, the YCJA provides for flexibility in sentencing, including the option of reprimanding the young person, and imposes limits on the retention and use of criminal records.

Clause 167 would amend the YCJA to specifically permit access to youth records for the purpose of administering the Passport Program. The *Canadian Passport Order* contemplates that passports can be denied or revoked in certain instances of criminality or national security concerns. For example, section 10.1 of the *Canadian Passport Order* provides that the Minister of Public Safety and Emergency Preparedness may decide to deny or revoke a passport if there are reasonable grounds to believe that it is necessary to prevent the commission of a terrorism offence, or for the national security of Canada or a foreign country or state.

Section 8 of the Charter protects against "unreasonable" searches and seizures. Because the disclosure of youth criminal justice records has the potential to interfere with a youth's privacy interests, it may engage section 8.

The following considerations support the consistency of these powers with the Charter. The new provision would specify that youth record information could be shared solely for the purpose of administering the *Canadian Passport Order*. This limited purpose strikes an appropriate balance between any privacy interests at stake and the state interest in protecting the safety and security of Canadians, as well as the integrity of the passport program. It would also enable Canada to

participate more effectively in the global fight against terrorism, notably travel by youth for purposes of engaging in terrorist activities.

CSE ACT MANDATES - EXAMPLES

New Foreign Signals Intelligence Tools

- Gather information that provides an advantage to military commanders leading CAF missions and other Canadian officials charged with mitigating threats to terrorism, espionage, kidnapping and cyber intrusions.
- Interact with hostage takers and other players to extract information to aid kidnapped Canadians.

Protective Services for Non-GoC Clients

- Share information about specific cyber threats with the owners of critical infrastructure, like telecommunications companies or the banking sector.
- Deploy its unique cybersecurity tools on non-government systems at the request of the owners of those systems.

Defensive Active Cyber Operations

- Disrupting systems of state-sponsored attacks targeting government and critical infrastructure.
- Degrading foreign systems during state-sponsored cyber operations against North American financial institutions, or against Canadian democratic institutions.
- Disable a foreign server attempting to steal information from the Government of Canada.
- Corrupt information sitting on foreign servers that was stolen from a Government of Canada network.
- Impede the ability of a cyber-criminal to install ransomware on Government of Canada computers.

Active Cyber Operations

- Disabling or interfering with terrorist devices and infrastructure used for media and communications.
- Assisting in covertly dismantling foreign-based systems used to disrupt the democratic process.
- Preventing a terrorist entity from using a mobile communication device to detonate a car bomb.

Assistance to DND/CAF

-
-

Assistance (more broadly):

- Collecting and processing communications, providing linguistic support, decrypting a hard drive, or designing technical solutions.

National Security Act, 2017 (Bill C-59)

A. The CSE Act

- It is crucial for CSE to keep pace with emerging technologies to better protect Canada's sensitive information.
- Bill C-59 proposes changes to CSE's governing legislation with the introduction of a CSE Act.
- This legislation would:
 - Clarify how we are authorized to operate in cyberspace, authorizing CSE to use advanced techniques to access foreign networks to collect intelligence.
 - Authorize CSE to be able to defend important networks outside of the Government of Canada at the request of the system owner.
 - CSE would also be authorized to take action online to disrupt foreign cyber threats targeting important networks.
- All of these activities would be subject to review by the National Security and Intelligence Review Agency (NSIRA).
- The Intelligence Commissioner would have a mandate to approve foreign intelligence and cybersecurity authorizations issued by the Minister of National Defence.
- This legislation is focused on authorities and accountabilities and not on CSE resources

B. Cybersecurity and Information Assurance

- Canada is an attractive target for cyber threat actors. Our national security, well-being, and economic prosperity depend on the Internet and the smooth functioning of our cyber systems.
- Under current legislation, we are authorized to provide advice, guidance, and services to protect information and information infrastructures of importance to the Government of Canada. However, we can only deploy our unique cyber defence tools onto federal systems.
- Under proposed legislation, upon request and when designated by the Minister of National Defence as a system of importance to the Government of Canada, CSE would be authorized to provide more robust cyber defence services to a critical non-Government network.
- Under current and proposed legislation, we cannot and do not direct our activities at Canadians or anyone in Canada.
- Under the proposed legislation, CSE would be subject to additional transparency and accountability measures.

C. Foreign Signals Intelligence

- Under the proposed legislation CSE would be able to use a broader range of SIGINT capabilities to acquire foreign intelligence.
- Specifically, this new authority would allow CSE to interact with foreign targets operating on computer networks and systems.
- Under current and proposed legislation, we cannot and do not direct our activities at Canadians or anyone in Canada.
- D. Under the proposed legislation, CSE would be subject to additional transparency and accountability measures.

E. Foreign Cyber Operations

- Defensive cyber operations would involve taking action to protect the information and networks of the federal government and designated systems of importance to the Government of Canada.
- Active cyber operations would involve carrying out activities to degrade, disrupt, influence, respond to, or interfere with the capabilities, intentions, or activities of a foreign threat actor.
- These operations would take place within a strict approval process.
- CSE would be prohibited from directing its active and defensive cyber operations at Canadians, any person in Canada, or the global information infrastructure in Canada.
- These activities must also be reasonable and proportionate.
- CSE also cannot cause death or bodily harm, or wilfully attempt to obstruct, pervert, or defeat the course of justice or democracy.
- Under the proposed legislation, CSE would be subject to additional transparency and accountability measures.

F. Assistance to Federal Security and Intelligence Partners

- As Canada's national cryptologic and signals intelligence agency, CSE possesses unique capabilities and expertise.
- Under current legislation, we assist federal law enforcement and security agencies in the performance of their lawful duties.
- Under proposed legislation, we would be permitted to assist the Department of National Defence (DND) and the Canadian Armed Forces (CAF).
- CSE would continue to have the same authority to carry out an activity as the agency requesting the assistance.
- CSE would also be subject to any restrictions or conditions placed on the agency requesting that assistance.
- Under the proposed legislation, CSE would be subject to additional transparency and accountability measures.

G. Transparency and Accountability

- CSE is currently reviewed by the Office of the Communications Security Establishment Commissioner.
- CSE's review and accountability framework will evolve to enhance the way in which CSE is reviewed, alongside the broader security and intelligence community.
- The legislation also strengthens CSE's Ministerial Authorization regime.
- The NSIRA would assume responsibility for reviewing all national security activities across the Government of Canada, including all of CSE's activities.
- The IC would have a mandate to approve foreign intelligence and cybersecurity authorizations.
- Commissioner approval would be required for these authorizations to come into effect.

H. Metadata

- The CSE Act clarifies CSE's authorities related to metadata by requiring that CSE obtain a Ministerial Authorization to acquire metadata that has a privacy interest.
- Ministerial Authorizations would not come into effect until approved by the independent Intelligence Commissioner, a retired judge.
- The CSE Act also includes specific provisions on the use, retention and disclosure of information, including metadata.

I. Publicly Available Information

- The intent of this provision is to allow CSE to conduct basic research in support of its mandate without fear of the restriction that it not direct its activities at Canadians or persons in Canada.
- This is not an authority to conduct investigations, or a means of collecting intelligence.
- For example, CSE may use publicly available information to provide useful context or background information to an intelligence or information assurance report.
- CSE must ensure that measures are in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and disclosure of publicly available information.

J. SIGINT Operations

- CSE is a foreign signals intelligence agency authorized to collect information from the global information infrastructure, based on intelligence priorities set by Cabinet.
- Under current and proposed legislation, we cannot and do not direct our activities at Canadians or anyone in Canada.
- Activities are carried out in a highly complex operating environment in which global communications technologies, networks, and systems are rapidly evolving.
- Use a range of innovative collection methods and techniques.
- Have strong privacy protection measures.

National Security Act, 2017 (Bill C-59)

K. Equities

CSE takes the security of Canadian systems and networks very seriously. CSE has a rigorous process in place to review and assess software vulnerabilities.

These reviews ensure that decisions are in the best interests of Canada's security which includes protecting Canada's critical information systems and networks, and protecting Canadians from foreign threats at home and abroad.

CSE uses appropriate channels to disclose software vulnerabilities.

L. Ministerial Direction

CSE has a longstanding, rigorous process in place to assess the risk of mistreatment associated with disclosing and requesting information. This risk continues to be considered whenever CSE information is shared. It was formalized for CSE with a Ministerial directive that was first issued on November, 2011.

I can confirm that the Minister provided an updated Ministerial Direction to CSE that will increase transparency and accountability, and provide the additional guidelines and explicit restrictions and reporting requirements for sharing and using information with and from foreign entities.

The Minister is best placed to confirm whether or when the MD will be released publicly.

M. Employee Behavior

CSE employees are expected to follow the Government of Canada's Policy on Acceptable Network and Device Use and internal CSE policies relating to using government electronic networks and devices in an acceptable manner.

This is extremely important to us, and is the case nearly 100% of the time. When, in the rare circumstance, an employee is found to be using government devices in an unacceptable manner there are consequences.

The activities in noted in the labour relations report found on page 44 of file A-2016-00040 relate to research activities undertaken by a CSE employee. Employees on a team in this specific area of CSE are permitted to dedicate 10% of their work week to researching topics of interest that could be of benefit to CSE. In this particular case, the employee in question did not follow the appropriate approval process for this kind of research and engaged in activities which exceeded the scope of what CSE considered acceptable.

These activities did not involve any of CSE's classified technology or capabilities, nor were they put at risk. CSE conducted an internal investigation and determined that this matter could be sufficiently dealt with by CSE's internal procedures and that it did not warrant further external review. The disciplinary measures recommended by CSE's Labour Relations office were implemented.

N. SS7

(Français)

Signalling System 7 (SS7) est un protocole de télécommunications largement utilisé depuis nombre d'années par les fournisseurs de télécommunication du Canada et du monde entier.

En outre, ce système présente un certain nombre de problèmes de sécurité qui, du reste, ont été rapportés publiquement à maintes reprises depuis qu'ils ont été mis au jour, en 2008.

Le CST a pour rôle de fournir des avis et des conseils visant à protéger les systèmes importants du gouvernement du Canada. C'est d'ailleurs dans cette optique que le CST travaille activement avec divers intervenants de l'industrie des télécommunications dans le but d'élaborer des pratiques exemplaires et de prodiguer des conseils qui auront notamment pour effet d'atténuer les risques posés par SS7.

En plus de formuler des recommandations sur des problèmes particuliers comme le protocole SS7, le CST fournit des conseils en matière de cybersécurité et propose des pratiques exemplaires aux utilisateurs du gouvernement du Canada relativement à l'emploi sécuritaire des communications mobiles.

Il y a peine quelques mois, le CST rencontrait les partis politiques fédéraux, les membres du Parlement, des représentants des gouvernements provinciaux et certains corps électoraux provinciaux pour leur communiquer de précieuses informations concernant l'utilisation des dispositifs mobiles.

English

Signalling System 7, or SS7 is a legacy telecom protocol widely used by telecom service providers not only in Canada, but around the world.

The security issues surrounding SS7, have been known for some time and have been reported on publicly since they emerged in 2008.

CSE's role is to provide advice and guidance to help protect systems of importance to the Government of Canada. With this in mind, CSE has been actively working with Canada's telecom industry to address issues related to SS7 to develop best practices, advice and guidance that can help mitigate the risks associated with SS7.

In addition to advice and guidance related to specific issues such as SS7, CSE provides the government of Canada with extensive cyber security advice and best practice recommendations including, for using mobile communications devices safely.

As recently as this past summer, CSE met with federal political parties, Parliamentarians, provincial governmental officials and provincial electoral bodies to provide guidance and advice on mobile device usage.

O. DI Report/Fake News

Earlier this year, CSE took the unprecedented step of releasing an unclassified threat report on threats to our democratic institutions. We found that it is highly probable that Canada's 2019 federal election process will see increase cyber threat activity.

CSE's reporting on cyber threats that could affect Canada's democratic processes is an ongoing effort. As new threat information emerges, CSE will continue to share as much information as possible with the public and the many stakeholders in Canada's democratic processes.

Since releasing our report on Cyber Threats to Canada's Democratic Process in June this year, CSE has held productive meetings with political parties, parliamentarians and electoral officials to discuss the report, its findings and to offer cyber security advice and guidance. For example, at the federal level, CSE officials have met with parliamentarians, representatives from all parties with standing in the House of Commons, and in partnership with Elections Canada, CSE met with a majority of the federally registered political parties in Canada. CSE has also met with representatives from all of Canada's provincial electoral bodies to discuss the cyber security challenges related to Canada's democratic process.

Cyber security, including protecting Canada's democratic processes, needs to be a team effort and it is important for government, academia and industry to work together. We have noted and commend the recent efforts by some social media service providers to help ensure the integrity of the democratic process in Canada. We have not yet worked directly with any social media service providers, however we are open to, as far as our mandate allows, sharing our assessments, advice and guidance with as many democratic process stakeholders as possible.

P.

Security of information

CSE takes security, and specifically the security of our information, extremely seriously.

CSE works closely with our partners both domestically and internationally on enhancing security around the information we protect and use to help ensure Canada's security.

s.15(1) - DEF