Annex 1

Communications Security Establishment | Centre de la sécurité des télécommunications

TOP SECRET//SI/CANADIAN EYES ONLY

COMMUNICATIONS SECURITY ESTABLISHMENT

END OF AUTHORIZATION REPORT

FOR THE MINISTER OF NATIONAL DEFENCE

Active Cyber Operations Authorization

[redacted]

Canada

INTRODUCTION

On [redacted] the Communications Security Establishment (CSE) was granted an Active Cyber Operations Authorization to [redacted] (Authorization) under subsection 30(1) of the *Communications Security Establishment Act* (*CSE Act*). The Authorization was repealed and replaced on [redacted] CSE is required by the *CSE Act* to provide the Minister of National Defence with a written report on the outcomes of the activities carried out under the Authorization within 90 days after its expiry/repeal.

This report is meant to satisfy that requirement, while including the following specifics that are required by the Authorization:

- the value of the activities conducted under the Authorization;
- metrics relating to activities conducted under the Authorization, including the number of activities conducted and the results produced;
- where an activity impacts section 2(b) of the *Canadian Charter of Rights and Freedoms (Charter)*, details of the assessments used to support that activity; and,
- confirmation that the conditions outlined in the Authorization concerning prohibited conduct have been met.

PROGRAM OVERVIEW

Active cyber operations (ACO) activities conducted pursuant to section 19 of the *CSE Act* aim 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 international affairs, defence, or security interests, including cybersecurity.

CSE is uniquely positioned to deliver ACO activities due to its capability to identify foreign threats as they manifest, and to covertly manipulate and exploit the global information infrastructure (GII) in order to design and launch tailored responses to the threats. The Authorization provided CSE with the authority to leverage its unique cyber capabilities to:

- degrade, disrupt, influence, respond to, or interfere with capabilities, intentions, or activities [redacted]
- [redacted]
- [redacted]

Those authorities were granted in a context whereby [redacted]

[redacted]

When planning for activities under the Authorization, CSE worked with Canadian and international partners in order to deconflict and coordinate to ensure that CSE's ACO activities were complementary to the activities of others. In addition, a Governance Framework has been developed with Global Affairs Canada (GAC) that includes a consultation protocol for the assessment of foreign policy risk, foreign policy coherence, and compliance with Canada's obligations under international law for ACO activities.

OUTCOMES

Between [redacted] CSE conducted the following [redacted] operations under the Authorization.

[redacted]

Page 4

is withheld pursuant to section

est retenue en vertu de l'article

15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Page 5

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - DEF, 15(1) - IA

of the Access to Information

de la Loi sur l'accès à l'information

Page 6

is withheld pursuant to section

est retenue en vertu de l'article

15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

COMPLIANCE WITH THE TERMS, CONDITIONS, AND RESTRICTIONS OF THE AUTHORIZATION

CSE has an internal compliance program that helps CSE meet its legal and policy obligations. CSE's internal compliance program is regularly consulted on operational planning for foreign cyber operations to validate that compliance requirements are met. The compliance program also conducts periodic assessments of operational activities and responds to compliance incidents when they occur. During this reporting period, no FCO-related incidents were reported to or discovered by the internal compliance team.

Charter Assessments

In addition, all operations under this Authorization were assessed for compliance with the *Charter*, and no activities infringed the *Charter*.

One section 2(b) assessment was conducted during the Authorization period. CSE renewed the section 2(b) assessment previously completed and approved by the Minister of National Defence in for an operation conducted under this Authorization. This assessment covered the ACO activity According to the current set of FCO Authorizations, the approval authority now rests with the Chief, CSE.

CONCLUSION

This report fulfills the requirement of paragraph 31 of the Authorization and subsection 52(1) of the *CSE Act* to report in writing on the outcomes of the Authorization.

As you are aware, you issued a new Authorization, which came into force on and will remain in effect for up to one year. A new end of authorization report will be provided to you within 90 days after the new Authorization's expiry/repeal.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

END OF AUTHORIZATION REPORT

FOR THE MINISTER OF NATIONAL DEFENCE

Active Cyber Operations Authorization [redacted]

[redacted]

[redacted]

Canada

INTRODUCTION

On [redacted] the Communications Security Establishment Canada (CSE) was granted an Active Cyber Operations Authorization [redacted] (Authorization) under subsection 30(1) of the *Communications Security Establishment Act* (*CSE Act*). The Authorization was repealed and replaced on [redacted] CSE is required by the *CSE Act* to provide the Minister of National Defence with a written report on the outcomes of the activities carried out under the Authorization within 90 days of its expiry/repeal.

This report is meant to satisfy that requirement while including the following specifics that are required by the Authorization:

- the value of the activities conducted under the Authorization;
- metrics relating to activities conducted under the Authorization, including the number of activities conducted and the results produced;
- where an activity impacts section 2(b) of the *Canadian Charter of Rights and Freedoms (Charter)*, details of the assessments used to support that activity; and,
- confirmation that the conditions outlined in the Authorization concerning prohibited conduct have been met.

PROGRAM OVERVIEW

Active cyber operations (ACO) activities conducted pursuant to section 19 of the *CSE Act* aim 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 international affairs, defence, or security interests, including cybersecurity.

CSE is uniquely positioned to deliver ACO activities due to its capability to identify foreign cyber threats as they manifest, and to covertly manipulate and exploit the global information infrastructure (GII) in order to design and launch tailored responses to the threats. The Authorization provided CSE with the authority to leverage its unique cyber capabilities to:

- degrade, disrupt, influence, respond to, or interfere with capabilities, intentions, or activities [redacted]
- [redacted]
- [redacted]

[redacted] poses one of the most significant threats to Canada's international affairs, defence, and security interests, including cybersecurity, as it engages in a range of hostile activities. Canada, its partners, and like-minded countries are increasingly targeted by hostile, pervasive, evolving, and far-reaching non-cyber, cyber, and hostile influence campaigns carried out by [redacted] notably with the aim of interfering with [redacted]

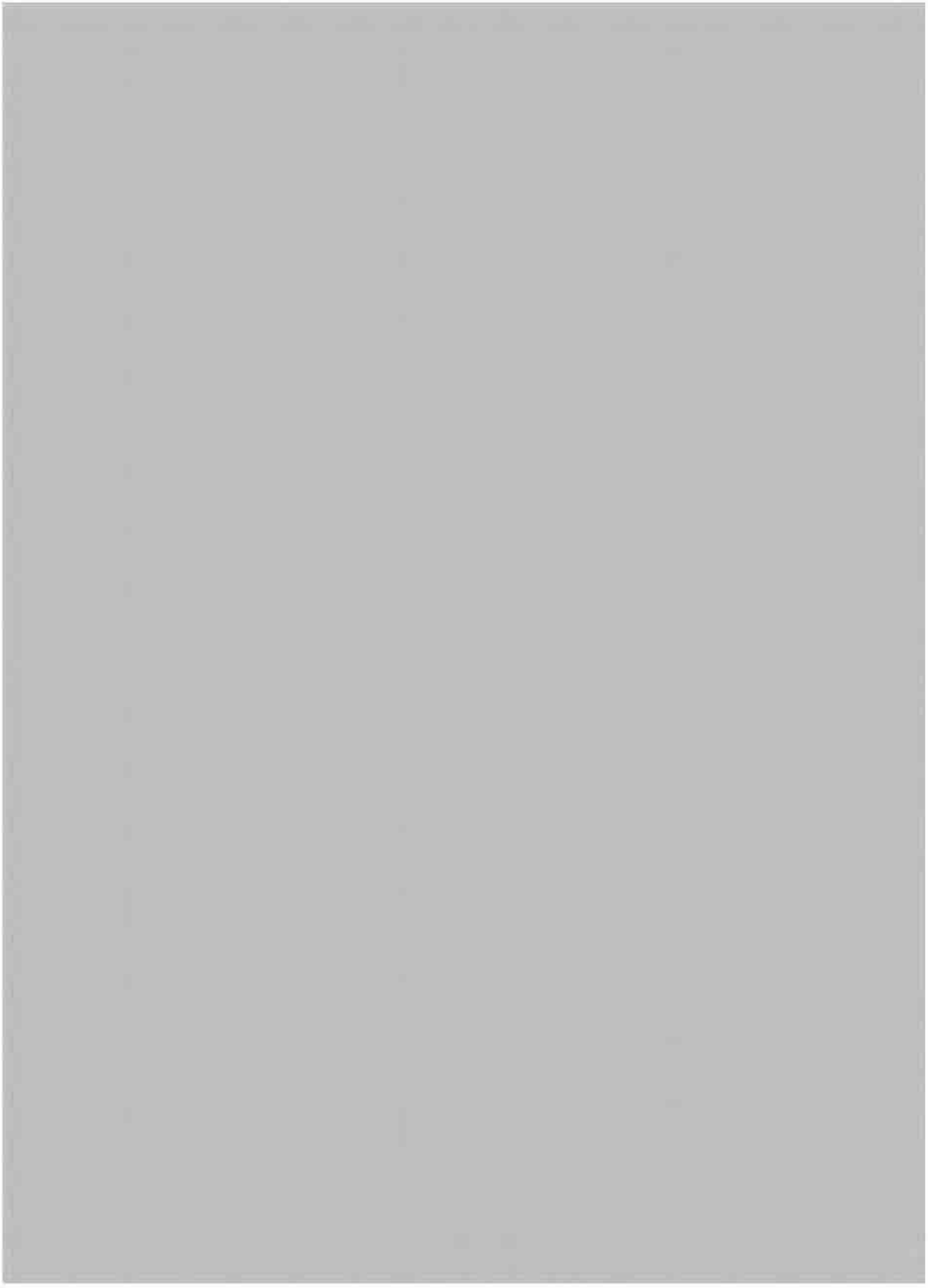
[redacted] In addition, has been engaging in a range of activities that undermine Canada's interests [redacted]

When planning for activities under the Authorization, CSE worked with Canadian and international partners to deconflict and coordinate, ensuring that CSE's ACO activities were complementary to the activities of others. In addition, the Governance Framework that CSE has with Global Affairs Canada includes a consultation protocol for the assessment of foreign policy risk, foreign policy coherence, and compliance with Canada's obligations under international law for ACO activities.

OUTCOMES

Between [redacted] CSE conducted the following [redacted] operations under the Authorization.

[redacted]



[redacted]

COMPLIANCE WITH THE TERMS, CONDITIONS, AND RESTRICTIONS OF THE AUTHORIZATION

CSE has an internal compliance program that helps CSE meet its legal and policy obligations. CSE's internal compliance program is regularly consulted on operational planning for foreign cyber operations (FCO) to validate that compliance requirements are met. The compliance program also conducts periodic assessments of operational activities and responds to compliance incidents when they occur. During this reporting period, no FCO-related incidents were reported to or discovered by the internal compliance team.

Charter Assessments

In addition, all operations under the Authorization were assessed for compliance with the *Charter*, and no activities infringed the *Charter*.

No 2(b) assessments were required for ACO activities under the Authorization during this reporting period.

CONCLUSION

This report fulfills the requirement of paragraph 30 of the Authorization and subsection 52(1) of the *CSE Act* to report in writing on the outcomes of the Authorization.

As you are aware, you issued a new Authorization, which came into force on [redacted] A new end of authorization report will be provided to you within 90 days after the new Authorization's expiry/repeal.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

END OF AUTHORIZATION REPORT

FOR THE MINISTER OF NATIONAL DEFENCE

Active Cyber Operations Authorization [redacted]

Canada

INTRODUCTION

On [redacted] the Communications Security Establishment (CSE) was granted an Active Cyber Operations Authorization [redacted] (Authorization) under subsection 30(1) of the *Communications Security Establishment Act* (*CSE Act*). The Authorization was repealed and replaced on [redacted] CSE is required by the *CSE Act* to provide the Minister of National Defence with a written report on the outcome of the activities carried out under the Authorization within 90 days after its expiry/repeal.

This report is meant to satisfy that requirement, while including the following specifics that are required by the Authorization:

- the value of the activities conducted under the Authorization;
- metrics relating to activities conducted under the Authorization, including the number of activities conducted pursuant to the Authorization and the results produced;
- where an activity impacts section 2(b) of the *Canadian Charter of Rights and Freedoms (Charter)*, details of the assessments used to support that activity; and,
- confirmation that the conditions outlined in the Authorization concerning prohibited conduct have been met.

PROGRAM OVERVIEW

Active cyber operations (ACO) activities conducted pursuant to section 19 of the *CSE Act* aim 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 international affairs, defence, or security interests, including cybersecurity.

CSE is uniquely positioned to deliver ACO activities due to its capability to identify foreign cyber threats as they manifest, and to covertly manipulate and exploit the global information infrastructure (GII) in order to design and launch tailored responses to the threats. Under the Authorization, CSE's activities were directed at foreign targets for the purpose of:

- disrupting foreign [redacted] that target Canada's [redacted] and the institutions that support them;
- countering global [redacted] of foreign origin; and,
- disrupting the use of the GII by foreign threat actors to recruit, plan, fund, communicate, or carry out [redacted] operations.

When planning for activities under the Authorization, CSE coordinated with Canadian and international partners toensure that CSE's ACO activities were complementary to the activities of others. In addition, the Governance Framework CSE has with Global Affairs Canada includes a consultation protocol for the assessment of foreign policy risk, foreign policy coherence, and compliance with Canada's obligations under international law for ACO activities.

OUTCOMES

Between [redacted] CSE conducted the following [redacted] operations under the Authorization.

[redacted]

COMPLIANCE WITH THE TERMS, CONDITIONS, AND RESTRICTIONS OF THE AUTHORIZATION

CSE has an internal compliance team that helps CSE meet its legal and policy obligations. CSE's internal compliance program is regularly consulted on operational planning for ACO activities to validate that compliance requirements are met. The compliance program also conducts periodic assessments of operational activities and responds to compliance incidents when they occur. During this reporting period, no ACO-related incidents were reported to or discovered by the internal compliance team.

Charter Assessments

In addition, all operations under the Authorization were reviewed for compliance with the *Charter*. No activities were found to have infringed the *Charter*.

No section 2(b) assessments were required for ACO activities conducted under the Authorization during this reporting period.

CONCLUSION

This report fulfills the requirement of paragraph 31 of the Authorization and subsection 52(1) of the *CSE Act* to report in writing on the outcomes of the Authorization.

As you are aware, you issued a new Authorization, which came into force on [redacted] for CSE to conduct ACO activities to [redacted] A new end of authorization report will be provided to you within 90 days after the new authorization's expiry/repeal.

Communications Security Establishment | Centre de la sécurité des télécommunications

SECRET//CANADIAN EYES ONLY

COMMUNICATIONS SECURITY ESTABLISHMENT

END OF AUTHORIZATION REPORT

FOR THE MINISTER OF NATIONAL DEFENCE

Cybersecurity Authorization Activities on Federal Infrastructure

[redacted]

Canada

GCDocs 80784340

INTRODUCTION

On [redacted] the Communications Security Establishment (CSE) was granted a Cybersecurity Authorization for Activities on Federal Infrastructures (Authorization) under subsection 27(1) of the *Communications Security Establishment Act* (*CSE Act*). The Authorization was repealed and replaced on [redacted] CSE is required by the *CSE Act* to provide the Minister of National Defence a written report on the outcome of the activities carried out under the Authorization within 90 days after its expiry/repeal.

This report is meant to satisfy that requirement by providing details on the activities undertaken under the Authorization, the value of those activities, the measures taken to protect the privacy of Canadians while engaging in those activities, and relevant metrics regarding the use of information that may have a privacy interest.

PROGRAM OVERVIEW

CSE conducts three different types of cybersecurity activities on federal infrastructure under the Authorization:

- deploying solutions at the host level, known as host-based solutions (HBS);
- deploying solutions at the network level, known as network-based solutions (NBS); and,
- deploying solutions at the cloud level, known as cloud-based solutions (CBS).

HBS, NBS, and CBS are complementary cybersecurity activities. They are applied at different levels of the information infrastructures being protected: [redacted] These activities leverage similar principles and techniques for detecting malicious cyber activity. Each activity involves assessing a federal institution's electronic information and information infrastructure, and acquiring any information originating from, directed to, stored on, or being transmitted on or through that infrastructure.

Alongside advanced malware analysis tools and automated cybersecurity capabilities, these activities allow CSE to provide a comprehensive defence framework for detecting and preventing unauthorized access to federal institutions' electronic information and intrusion into their information infrastructures. In order to meet those objectives, CSE must conduct activities that may contravene other Acts of Parliament or acquire information from the global information infrastructure that interferes with a reasonable expectation of privacy of a Canadian or person in Canada. The Authorization enabled CSE to perform these critical activities, while also ensuring that they were reasonable and proportionate.

OUTCOMES

New Agreements

During the period of the Authorization, CSE entered into [redacted] agreements to provide cybersecurity and information assurance services to the following federal institutions:

[redacted]

As of [redacted] CSE provided cybersecurity and information assurance services to [redacted] of 217[1] federal institutions.

Host-Based Solutions

[redacted]

[1] During the previous reporting period, it was reported that CSE provided services to [redacted] federal institutions. As noted above, the total number of federal institutions, as a result of the creation of new agencies, as well as some agencies expanding or dividing into two agencies, is currently 217.

During the Authorization period, CSE federal institutions[2] to HBS, federal institutions receiving HBS services. As of CSE's HBS installed base[3] across the Government of Canada (GC) infrastructure exceeded endpoints. compared to the period in which the previous Authorization was in place.

Network-Based Solutions

As of is providing CSE's NBS services to federal institutions, and CSE has bilateral agreements with others, federal institutions receiving CSE's NBS services.

[3] Throughout this section, references are made to both new deployments and new partners. New deployment refers to new sensors installed to an already existing partner's infrastructure, expanding the total installed base, whereas a new partner refers to novel engagement between CSE and a federal institution. Furthermore, the total installed base refers to the total number of sensors deployed on all federal infrastructures.

Cloud-Based Solutions

During the Authorization period, CSE deployed CBS across its federal client base and CBS partners.[4] As of CSE had federal CBS partners and a total installed base of CBS.[5] compared to the period of the previous Authorization.

DETECTION AND DEFENCE

CSE cybersecurity analysts have created algorithms and automated processes to recognize malicious activity. The information collected under HBS, NBS, and CBS triggers an action either on the host, on the network, or on the cloud to mitigate malicious activities and/or compromises. Through its HBS, NBS, and CBS deployments, CSE's network dynamic defence capability blocked an average of over 6 billion malicious inbound connection attempts per day throughout the Authorization period. This indicates a compared to the period of the previous Authorization.

All federal institutions receiving NBS benefit from NBS dynamic services. federal entities receiving NBS services through direct agreements with CSE,

[4] During the Authorization period, CSE onboarded the following new CBS partners:

[5] During the previous reporting period, CSE reported a total installed base of for CBS. As a result of the decommissioning of some CBS entities, CSE's total installed base for CBS is currently

[6] While dynamic defence provides the capability to block malicious activity almost instantly, sometimes manual intervention is also required.

benefit from NBS dynamic services.[7] Additionally, there are federal institutions who are benefitting from HBS dynamic services. CSE will notify the Minister of National Defence and the Intelligence Commissioner when per the requirements of the Authorization.

The information acquired under the Authorization allowed CSE to detect malicious events[8] on federal entities' systems and mitigate them by working collaboratively with the host departments to respond to these incidents. When doing so, CSE abided by the requirements of the *CSE Act* and the Authorization by only retaining and using information that helped identify, isolate, prevent, or mitigate harm to the federal institutions' information infrastructures.

As outlined below, there was a significant number of which during the period the Authorization was in place.

From were the most frequently affected sectors.

[7] The federal entities who receive NBS through direct agreement with CSE are: Of those is the only entity not benefitting from NBS dynamic.

[8] A malicious event in this case is defined as a breach of government security. It includes, but is not limited to,

Total Malicious Events Observed by Sector

Source: CSE's Threat Assessment, Reporting and Planning team

These malicious events can be further categorized by the type of activity that was detected. The table below shows the definitions of each categorization that is made, and the following pie chart shows the corresponding distribution.

Event	Description

[redacted]

Malicious Events by Event Type

Source: CSE's Threat Assessment, Reporting, and Planning team

State-Sponsored Activity Against the Government of Canada

[redacted]

[redacted]

State-Sponsored Activity Against the GC

Source: CSE's Threat Assessment, Reporting and Planning team

The state-sponsored activity has been further categorized below by event type.

Event	Description

State-Sponsored Activity Event Types

Source: CSE's Threat Assessment, Reporting and Planning team

VALUE OF CYBERSECURITY AND INFORMATION ASSURANCE ACTIVITIES

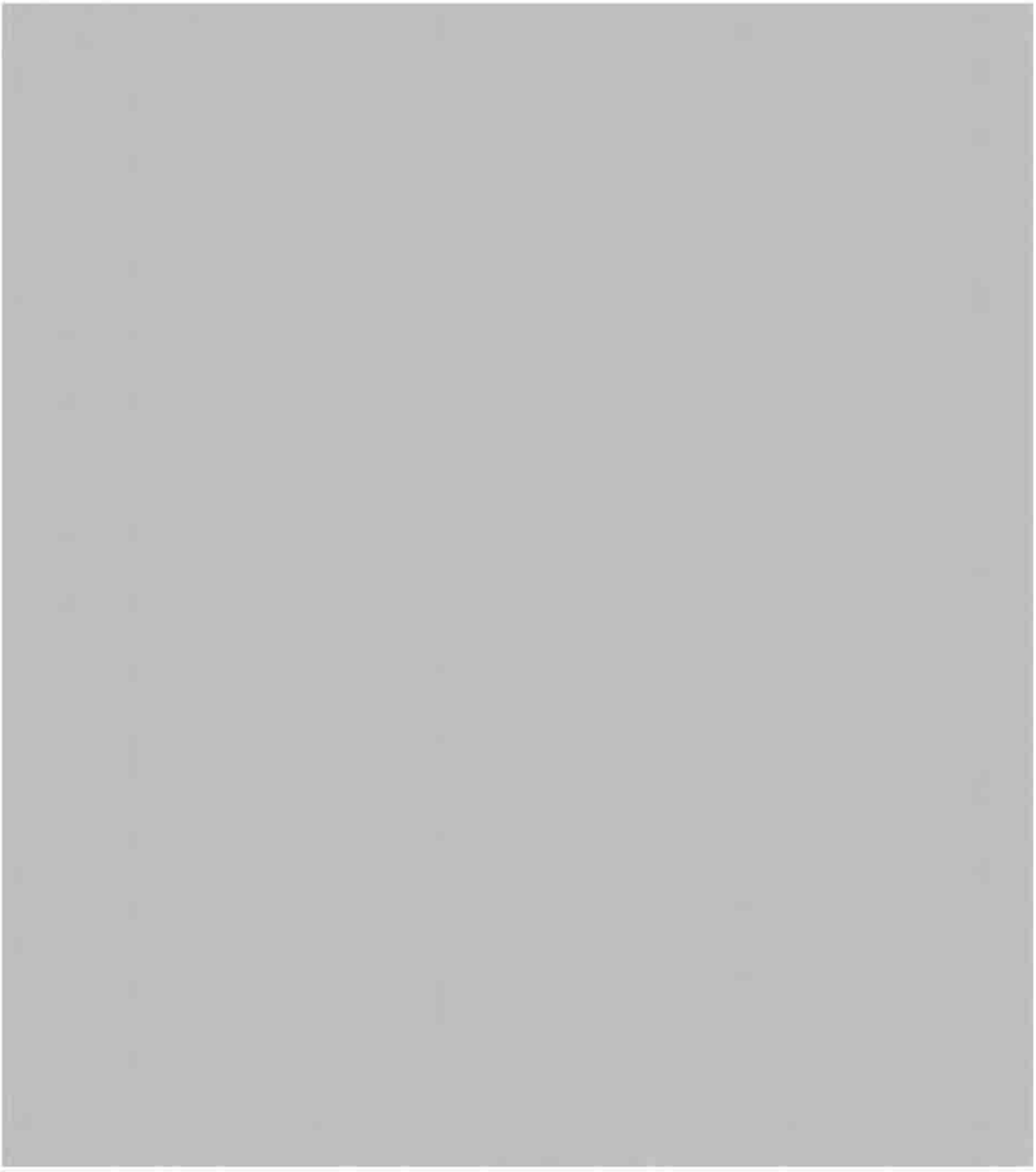
Canadians depend on the GC and its institutions for a wide range of essential services including health, national security and defence, banking and financial assistance, education, and food safety. Canadians expect and trust the GC and its institutions to protect their personal information and information that impacts their security, as well as their financial and social well-being.

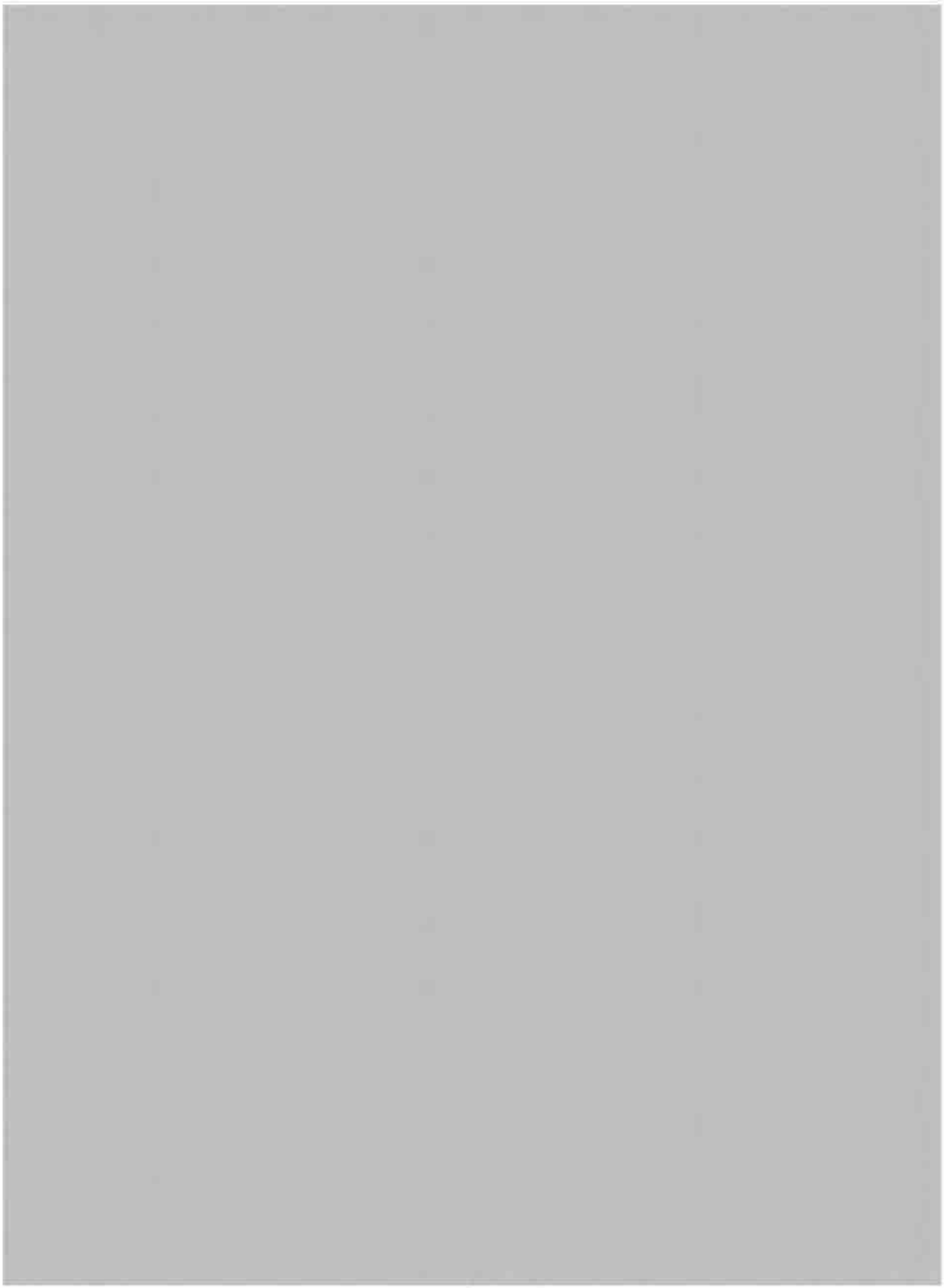
Federal institutions are continuously targeted by a range of sophisticated cyber threat actors, including cyber criminals and state-sponsored actors. To counter these threat actors and ensure that Canadians' information and services are protected, the GC maintains robust defences to deter and detect malicious activities and increase the time and resources required by threat actors to penetrate federal information infrastructures.

Federal institutions employ best-of-breed commercially available measures to detect malicious activities directed against their information infrastructures. CSE's capabilities complement these commercially available solutions by leveraging foreign intelligence on cyber threats, threat intelligence feeds, and CSE's interconnected sensors that it deploys across federal institutions to establish a more comprehensive threat picture and enable responses. As permitted by the Authorization, CSE used HBS, NBS, and CBS collected information to feed advanced intrusion detection and analysis solutions. CSE took mitigative actions based on this information, including routinely blocking over 6

billion malicious actions aimed at federal systems every day during the period the Authorization was in place. These activities enabled CSE to isolate and prevent harm to the electronic information and information infrastructures of federal institutions to a far greater degree than commercial solutions alone would permit. Additionally, once a threat is detected and mitigated on one federal system, the information is then used to protect all federal infrastructure.

Recent Successes





MEASURES TO PROTECT THE PRIVACY OF CANADIANS

CSE has a comprehensive program in place to protect the privacy of Canadians and persons in Canada in the conduct of its cybersecurity activities. CSE's Mission Policy Suite Cybersecurity (MPS Cybersecurity) is a foundational policy document based on the *CSE Act*, the *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, and other applicable laws, that guides how CSE conducts its cybersecurity and information assurance activities while ensuring that information with a Canadian privacy interest is protected. MPS Cybersecurity applies to all CSE employees conducting operational activities under the cybersecurity aspect of CSE's mandate. A layered suite of privacy measures is built into CSE processes, training, and compliance programs. Broadly speaking, MPS Cybersecurity governs the acquisition, use (analysis), retention, and disclosure of information in the conduct of CSE's operations.

The privacy protection measures applied to data acquired under this Authorization included, but were not limited to, the following:

- information was tagged and tracked throughout its life-cycle, including for retention and disposition schedules;
- access to data was restricted to a limited number of personnel who demonstrated knowledge of CSE's legal and policy framework;
- prior to accessing unassessed information, analysts must pass an annual graded test, covering the legal and policy requirements that apply to handling this type of information;
- the conduct of cybersecurity activities under this Authorization and access to unassessed data was limited to those authorized to conduct or support cybersecurity activities;
- access to use, analyse, and report data was subject to approval processes to ensure proper oversight and privacy considerations, as outlined in MPS Cybersecurity;
- privacy annotations were applied to track the number of private communications (PCs) retained and to automatically delete those that were not deemed to be essential to identify, isolate, prevent or mitigate harm to federal institutions' electronic information or information infrastructures;
- disclosure of PCs was subject to strict requirements and tracking;
- information relating to a Canadian or person in Canada was only retained when it was determined that the information was essential to identify, isolate, prevent or mitigate harm to federal systems or those of systems of importance;
- information relating to a Canadian or person in Canada was only disclosed outside CSE when it was determined that the disclosure was necessary to help protect federal systems or systems of importance; and,
- disclosure of information relating to a Canadian or person in Canada was subject to strict handling and privacy protection measures.

In addition, before deploying its cybersecurity solutions to protect federal systems, CSE required that the system owners of these institutions request CSE's services in writing and were fully informed of, and consented to, the provision of those services. In accordance with standard government practice, federal institutions advised authorized users of these information infrastructures that their device and/or network activity were being monitored for cybersecurity purposes.

These privacy protection measures are also demonstrated in the following sections of this report. CSE's tagging and tracking of information throughout its lifecycle ensures that information acquired under the Authorization is only retained when assessed as necessary or essential, and that information relating to a Canadian or person in Canada is disclosed outside CSE only when it is necessary.

Additionally, CSE's internal compliance team helps CSE meet its legal and policy obligations with respect to the collection, handling, use, retention, and disclosure of information. The team's work is guided by an annual work plan to ensure that it monitors key activities on a regular basis, including, but not limited to: the compliance of systems, tools and services, appropriate access controls, data retention, releasable cybersecurity product approvals and documentation, cross-mandate activities, information sharing, including sharing with eligible recipients, as well as the compliance of new or substantially modified activities and pilot projects. These compliance monitoring activities are conducted using a risk-based approach.

In CSE's internal compliance program was notified of a potential incident involving

During the period the Authorization was in place, the internal compliance team conducted several activities to measure the compliance of cyber defence systems, including assessments of sharing documentation, the development and sharing of threat assessments, and data deletion compliance in Cyber Centre's systems.

The team identified no instances where persons, other than those authorized, intentionally accessed cybersecurity architectures, equipment, or unassessed information while conducting cybersecurity activities pursuant to the Authorization.

PRIVATE COMMUNICATIONS AND SOLICITOR-CLIENT COMMUNICATIONS

Private Communications

PCs are communications that originate or terminate in Canada where the originator has a reasonable expectation of privacy. As part of its compliance and reporting regime, CSE uses a marking system to annotate recognized PCs.

During the period the Authorization was in place, PCs were retained as they were deemed essential to identify, isolate, or prevent harm to federal systems or systems of importance; of those, were disclosed outside CSE in reports. PCs disclosed in reports outside CSE included

Solicitor-Client Communications

A solicitor-client communication is defined as a communication relating to the seeking, formulating, or giving of legal advice between a client and a person authorized to practice as an advocate or notary in Quebec or as a barrister or solicitor in any territory or other province in Canada, or any person employed in the office of such advocate, notary, barrister or solicitor.

In accordance with the Authorization, solicitor-client communications shall be destroyed unless the Chief, CSE has reasonable grounds to believe the communication is essential to identify, isolate, prevent or mitigate harm to federal systems. Before using, analysing, retaining, or disclosing the communication, the Chief, CSE shall advise the Minister of National Defence and seek direction regarding its use, analysis, retention, and disclosure. Should the Minister direct CSE to use, analyse, retain, or disclose any solicitor-client communication, the Chief, CSE will also notify the Intelligence Commissioner. Should the Chief, CSE have reasonable grounds to believe that the information raises concerns about an imminent threat which would compromise the ability of a federal institution to mitigate that imminent threat to federal systems, the Chief, CSE may use, analyse, retain, or disclose the communication to the extent necessary to address the imminent threat. The Chief, CSE shall advise the Minister of National Defence, in writing, no later than 48 hours after such determination, so that the Minister can decide its further use, retention, and disclosure. The Chief, CSE will also notify the Intelligence Commissioner.

During the period the Authorization was in place, CSE did not use, analyse, retain or disclose any recognized solicitor-client communications.

Information Relating to a Canadian or Person in Canada

Information relating a Canadian or person in Canada refers to any information recognized as having reference to a Canadian or person in Canada, regardless of whether that information could be used to identify that Canadian or person in Canada. In the context of cybersecurity and information assurance activities, this information includes both identifying and non-identifying information, such as domain names, email addresses, business information, or usernames. In accordance with the Authorization, CSE may undertake activities that could include the incidental acquisition of information relating to a Canadian or person in Canada, as well as the use, analysis, retention, and disclosure of this information. CSE may disclose information relating to a Canadian or person in Canada that has been acquired, used, and analysed in the course of the activities carried out under the Authorization, to persons or classes of persons designated under section 45 of the *CSE Act*, where the disclosure of that information is necessary to help protect federal systems and other systems of importance.

During the period the Authorization was in place, CSE issued [redacted] cyber defence reports based on malicious activity and vulnerabilities identified through CSE's cybersecurity solutions. Of these, [redacted] contained information relating to a Canadian or person in Canada, such as [redacted] all of which were acquired from federal systems and systems of importance receiving cybersecurity services from CSE. When deemed necessary to help protect federal systems or systems of importance, CSE disclosed these reports to designated recipients as authorized by the Minister of National Defence under section 45 of the *CSE Act*.

Reports shared outside CSE containing information relating to Canadians or persons in Canada primarily consist of reports containing information from those systems and networks, where CSE is sharing the information back to the system owner. For example, CSE will share a report with a federal institution which contains their own compromised [redacted] in order to identify vulnerabilities and propose mitigations to help protect those federal systems and networks. In some cases, CSE shares reports containing information relating to a Canadian or person in Canada to other designated recipients authorized under section 45 of the *CSE Act*, such as [redacted] who have cyber defence coordination, mitigation, or victim notification mandates as identified in the Ministerial Order, where the information will be used to further protect federal institutions and systems of importance.

CONCLUSION

The details in this report demonstrate the outcomes and value of the activities undertaken as part of the Authorization, as well as the measures taken to safeguard the

privacy of Canadians. This report fulfills the requirement of paragraph 60 of the Authorization and subsection 52(1) of the *CSE Act* to report in writing on the outcomes of the Authorization.

A new Authorization was issued, which came into force on [redacted] following the Intelligence Commissioner's approval, which will remain in effect for [redacted] A new end of authorization report will be provided to you within 90 days after the new Authorization's expiry/repeal.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

TOP SECRET//SI//CANADIAN EYES ONLY

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

END OF AUTHORIZATION REPORT

FOR THE MINISTER OF NATIONAL DEFENCE

Defensive Cyber Operations Authorization

[redacted]

Canada

INTRODUCTION

On [redacted] the Communications Security Establishment (CSE) was granted a Defensive Cyber Operations Authorization (Authorization) under subsection 29(1) of the *Communications Security Establishment Act (CSE Act)*. The Authorization was repealed and replaced on [redacted] CSE is required by the *CSE Act* to provide the Minister of National Defence with a written report on the outcome of the activities carried out under the Authorization within 90 days after its expiry/repeal.

This report is meant to satisfy that requirement, while including the following specifics that are required by the Authorization:

- the value of the activities conducted under the Authorization;
- metrics relating to activities conducted under the Authorization, including the number of activities conducted pursuant to the Authorization and the results produced;
- where an activity impacts section 2(b) of the *Canadian Charter of Rights and Freedoms (Charter)*, details of the assessments used to support that activity; and,
- confirmation that the conditions outlined in the Authorization concerning prohibited conduct have been met.

PROGRAM OVERVIEW

Defensive cyber operations (DCO) conducted pursuant to section 18 of the *CSE Act* aim to help protect federal institutions' electronic information and information infrastructures (federal systems), and the electronic information and information infrastructures designated as being of importance to the Government of Canada (GC) (systems of importance).

CSE is uniquely positioned to deliver DCO activities as it can leverage the information it acquires in accordance with other aspects of its mandate to identify and characterize threats with precision.

The Authorization provided CSE with the authority to leverage its unique cyber capabilities to:

- protect against foreign entities' activities that threaten federal systems, or systems of importance, by degrading, disrupting, or interfering with their capabilities, intentions, or activities; and,
- influence or interfere with foreign targets' capabilities, intentions, or activities by [redacted]

Under the terms of the Authorization, DCO activities were authorized to be undertaken when one of the following circumstances arose:

1. the threat was of a nature that CSE's cybersecurity tools, capabilities, and resources would be insufficient to protect the electronic information or information infrastructures in a timely manner;

2. the threat had progressed to such an advanced stage of compromise that deploying CSE's cybersecurity tools, capabilities, and resources may no longer be sufficient to mitigate the threat; or,
3. the scope and scale of the anticipated threat was so widespread, impacting so many federal systems and systems of importance, that deploying CSE's cybersecurity tools, capabilities, and resources needed to mitigate this threat in a timely manner was not possible.

When planning for activities under the Authorization, CSE coordinated with Canadian and international partners to ensure that CSE's DCO activities were complementary to the activities of others. In addition, a Governance Framework has been developed with Global Affairs Canada that includes a consultation protocol for the assessment of foreign policy risk, foreign policy coherence, and compliance with Canada's obligations under international law for DCO activities.

OUTCOMES

Between [redacted] CSE conducted [redacted] to help protect federal systems and systems of importance.

[redacted]

COMPLIANCE WITH THE TERMS, CONDITIONS, AND RESTRICTIONS OF THE AUTHORIZATION

CSE has an internal compliance team that helps CSE meet its legal and policy obligations. CSE's internal compliance program was consulted on the standing operational plan for DCO to validate that compliance requirements were met. The compliance program also conducts periodic assessments of operational activities and responds to compliance incidents when they occur. During this reporting period, no DCO-related incidents were reported to or discovered by the internal compliance team.

[redacted]

Charter Assessments

In addition, all operations under the Authorization were assessed for compliance with the *Charter*. No activities were found to have infringed the *Charter*.

No 2(b) assessments were required for DCO activities conducted under the Authorization during this reporting period.

CONCLUSION

This report fulfills the requirement of paragraph 34 of the Authorization and subsection 52(1) of the *CSE Act* to report in writing on the outcomes of the Authorization.

As you are aware, you issued a new Authorization, which came into force on [redacted] for CSE to conduct DCO activities. A new end of authorization report will be provided to you within 90 days after the new Authorization's expiry/repeal.