



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

Foreign Intelligence Authorization



© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada



INTRODUCTION

On [REDACTED] the Communications Security Establishment Canada (CSE) was granted a Foreign Intelligence Authorization [REDACTED] (Authorization) under subsection 26(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 The Authorization was repealed and replaced on [REDACTED] CSE is required by the CSE Act to provide the Minister of National Defence with a written report on the outcome of the activities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 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



OUTCOMES

All of CSE's foreign intelligence activities, [REDACTED] are guided by the GC intelligence priorities, which are established by Cabinet.

[REDACTED] These activities also





[REDACTED]

In addition, all activities conducted under the Authorization are conducted by persons trained and certified² to undertake such activities.

Between [REDACTED] were acquired [REDACTED] to produce a variety of products. During the same period, CSE and the Canadian Forces Information Operations Group (CFIOG), a Canadian Armed Forces (CAF) entity that conducts SIGINT activities [REDACTED] used [REDACTED] communications to issue [REDACTED] foreign intelligence reports.

[REDACTED]

Of the [REDACTED] reports, the majority dealt with [REDACTED]

[REDACTED]

Of the [REDACTED] reports, [REDACTED] were shared with international partners:

- [REDACTED]
- [REDACTED]

² CSE has a comprehensive training and certification process that is based on curricula developed by [REDACTED]

[REDACTED]

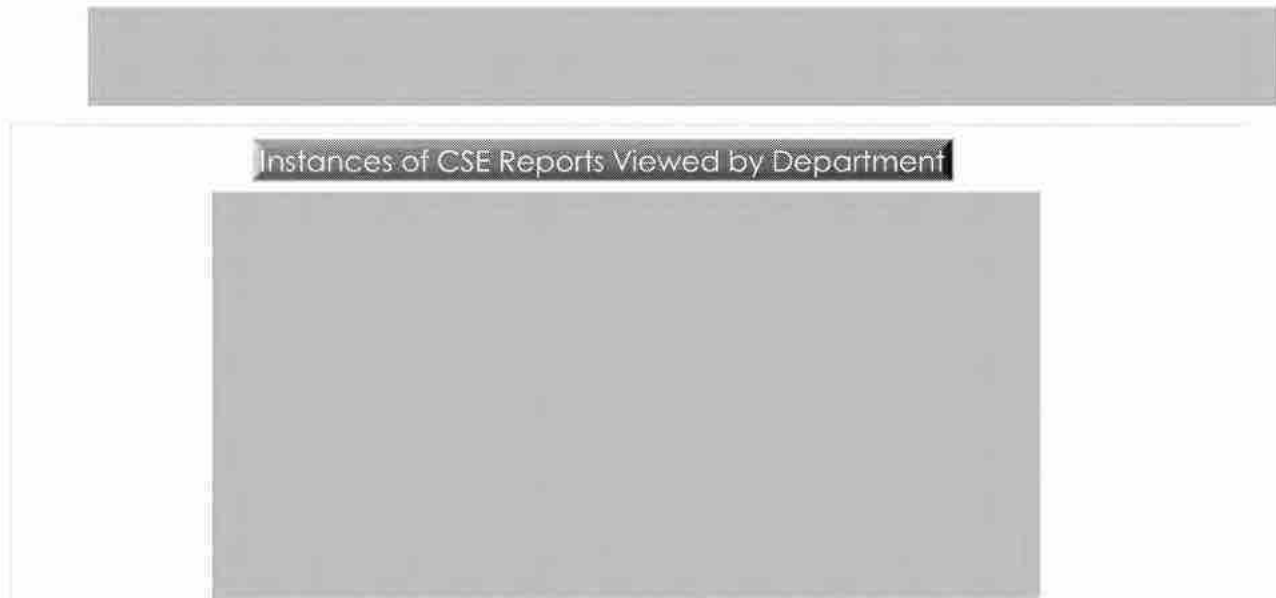


Figure 1: A single report may be viewed by multiple departments and multiple times by the same or different users within a department. These figures capture each instance of viewing.

Clients in [redacted] GC departments and agencies viewed the foreign intelligence reports

[redacted] accounting for the majority of reports accessed.



Page 43

**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 44

**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**



Cybercrime

- Beginning in [redacted] activities revealed foreign intelligence about [redacted]



**Pages 46 to / à 47
are withheld pursuant to sections
sont retenues en vertu des articles**

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

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 48 to / à 49
are withheld pursuant to section
sont retenues en vertu de l'article

15(1) - DEF

of the Access to Information
de la Loi sur l'accès à l'information



Support to Other Aspects of CSE's Mandate

During the period of validity of the Authorization, [REDACTED] activities were used in support of other CSE activities, particularly activities conducted pursuant to ACO authorizations. In addition to the instances [REDACTED] the following [REDACTED] activities occurred in support of ACO.



Page 51

**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**



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 foreign intelligence activities. CSE's Mission Policy Suite (MPS) Foreign Intelligence 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 foreign intelligence activities while ensuring that information with a Canadian privacy interest is protected. A layered suite of privacy measures is built into CSE processes, training, and compliance programs. Broadly speaking, MPS Foreign Intelligence 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 the 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;
- access to use, analyse, and report data was subject to approval processes to ensure proper oversight and privacy considerations;
- privacy annotations were applied to track the number and foreign intelligence value of incidentally acquired private communications (PCs) retained and to automatically delete those that were not deemed to be essential to international affairs, defence, or security interests, including cybersecurity;
- Canadian identity information (CII) was suppressed in reporting; and,
- disclosure of suppressed CII was subject to strict requirements and tracking.

Additionally, CSE has an internal compliance team that helps CSE meet its legal and policy obligations with respect to the acquisition, use (analysis), 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. These compliance monitoring activities are conducted using a risk-based approach. During the period the Authorization was in place, the internal compliance team examined aspects of acquisition and handling of



data [REDACTED] through incident assessments. Where compliance issues were identified, required actions were prescribed to mitigate risks. Additionally, recommendations were made to further enhance practices and systems going forward.

PRIVATE COMMUNICATIONS, SOLICITOR-CLIENT COMMUNICATIONS, AND CANADIAN IDENTITY INFORMATION

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.

Of the [REDACTED] acquired [REDACTED] recognized as a PC, [REDACTED] not retained or used in a report. [REDACTED] was marked for deletion [REDACTED] did not include information essential to international affairs, defence, or security interests, including cybersecurity

CSE analysts may amend the annotations or markings associated with communications data held in CSE databases over time. These changes are normal and demonstrate that CSE continually reassesses the data it acquires as new information becomes available. Consequently, a snapshot of CSE's database holdings taken at one point in time may differ from the snapshot at a different point in time, even for the same reporting year.

For example, based on new information, a recognized PC deemed essential at one point in time could later be deemed non-essential and destroyed. This can produce variations in the number of PCs residing in CSE databases from one reporting period to another. The metrics provided in this report accurately reflect CSE's assessment of its data repositories as of [REDACTED]

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 international affairs, defence, or security interests, including cybersecurity. Before using, retaining, or disclosing the communication, the Chief, CSE, shall advise the Minister of National Defence and seek directions regarding its use, analysis, retention, and disclosure. Should Minister direct CSE to use, analyse, retain, or disclose any solicitor-client communications, the Chief, CSE, will also notify the Intelligence Commissioner. Should the Chief, CSE have reasonable grounds to believe that the information raises concerns that an individual or group is in imminent danger of death or serious bodily harm, the Chief, CSE, may use, analyse, retain or disclose the information to the extent necessary to address the imminent danger. The Chief, CSE,



shall advise the Minister of National Defence, in writing, no later than 48 hours after such a 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 of validity of the Authorization, CSE did not use, analyse, retain, or disclose any recognized solicitor-client communications.¹⁵

Foreign Intelligence Products Containing Suppressed Canadian Identity Information

When targeting foreign entities, CSE may incidentally acquire PCs or information about a Canadian entity. If the information about the Canadian entity or entity in Canada is deemed essential to international affairs, defence, or security interests, including cybersecurity, CSE has the authority under the CSE Act to retain that information for use and analysis. In these cases, CSE must apply measures to protect the privacy of the entity. The most common protection measure is the suppression of information with a privacy interest, whereby the CII is replaced by a generic term such as "Named Canadian Company 1." Other measures can include restricted dissemination and/or handling caveats.

CSE may only release CII suppressed in foreign intelligence reporting to partners or other GC departments upon request. The disclosure must also be considered essential to international affairs, defence, or security interests, including cybersecurity. Furthermore, these recipients must have been designated by the Minister of National Defence under section 45 of the CSE Act, and must submit a rationale for the request to receive unsuppressed CII. For example,

Between [REDACTED] were acquired [REDACTED]
[REDACTED] During the same timeframe, CSE and CFIOG used [REDACTED] of these
[REDACTED] to issue [REDACTED] foreign intelligence reports. [REDACTED] reports contained CII.

Examples of the types of CII shared in these reports includes [REDACTED]

Of those reports, none were derived from a PC. CSE approved [REDACTED] disclosure requests for CII based on those reports to [REDACTED] During the Authorization period, no disclosures of CII from these reports were shared with international partners.

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

¹⁵ During the period of validity of the Authorization, CSE incidentally acquired one solicitor-client communication that was immediately deleted and was not retained (used or analysed).

¹⁶ Total approved disclosure requests as of [REDACTED] Requests can include multiple suppressed identities that are found in the report.



privacy of Canadians. This report fulfills the requirement of paragraph 63 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] following the Intelligence Commissioner's approval, 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

TOP SECRET//SI//CANADIAN EYES ONLY

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

END OF AUTHORIZATION REPORT

FOR THE MINISTER OF
NATIONAL DEFENCE

Foreign Intelligence Authorization



© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada



INTRODUCTION

On [REDACTED] the Communications Security Establishment Canada (CSE) was granted a Foreign Intelligence Authorization [REDACTED] (Authorization) under subsection 26(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 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



These activities enable CSE to gain access to the GII and acquire information for the purpose of providing the Government of Canada (GC) with foreign intelligence. The information acquired is necessary for creating intelligence reporting, for conducting research, and for developing new capabilities. [REDACTED] are a critical source of foreign intelligence for CSE and also provide significant benefits to Canada's international partners who provide intelligence, technology, and capabilities to CSE in return.





OUTCOMES

All of CSE's foreign intelligence activities, [REDACTED] are guided by GC intelligence priorities, which are established by Cabinet.

Between [REDACTED] total communications¹ were acquired [REDACTED] to produce a variety of products. During the same period, CSE and the Canadian Forces Information Operations Group (CFIOG), a Canadian Armed Forces (CAF) entity that conducts SIGINT activities [REDACTED] used [REDACTED] of those communications to issue [REDACTED] foreign intelligence reports.

Of the [REDACTED] CSE and CFIOG reports the majority dealt with [REDACTED]

Of the [REDACTED] reports issued, [REDACTED] were shared with international partners.

- [REDACTED]
- [REDACTED]



Instances of CSE Reports Viewed by Department

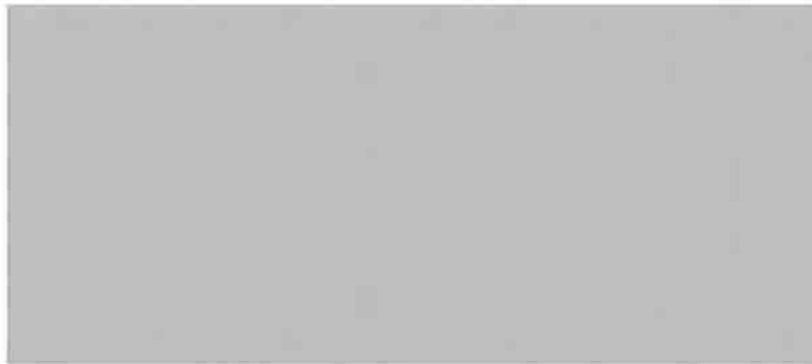


Figure 1: A single report may be viewed by multiple departments and multiple times by the same or different users within a department. These figures capture each instance of viewing.

Clients in GC departments and agencies viewed the foreign intelligence reports



**Pages 60 to / à 64
are withheld pursuant to sections
sont retenues en vertu des articles**

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

**of the Access to Information
de la Loi sur l'accès à l'information**



Support to Other Aspects of CSE's Mandate

In addition to helping meet the foreign intelligence aspect of CSE's mandate, [REDACTED] activities under the Authorization facilitated the execution of foreign cyber operations conducted pursuant to separate authorizations issued under section 29 and 30 of the CSE Act, respectively. This includes [REDACTED]

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 foreign intelligence activities. CSE's Mission Policy Suite (MPS) Foreign Intelligence 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 foreign intelligence activities while ensuring that information with a Canadian privacy interest is protected. A layered suite of privacy measures is built into CSE processes, training, and compliance programs. Broadly speaking, MPS Foreign Intelligence 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 the Authorization included, but were not limited to the following:

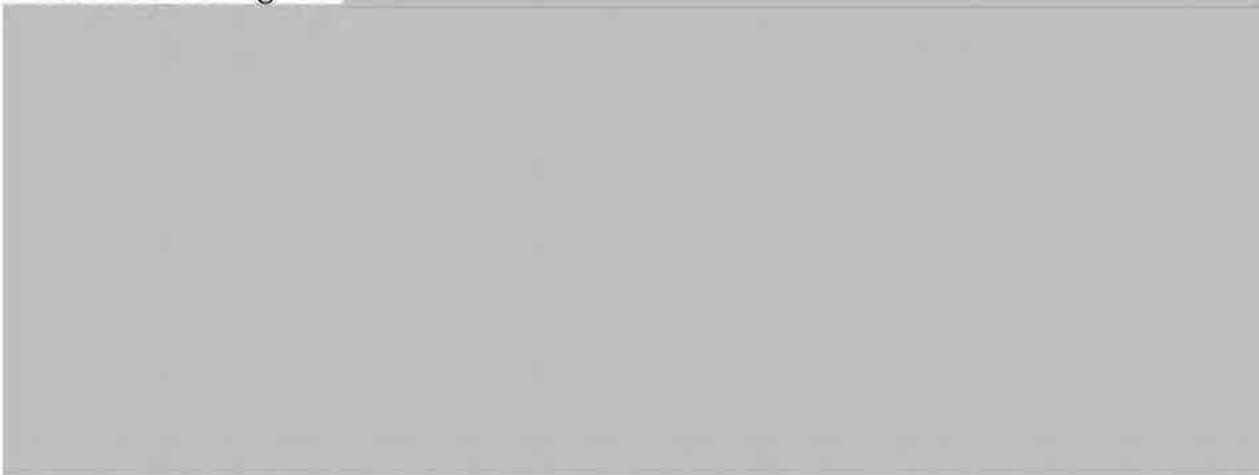
- information was tagged and tracked throughout its life-cycle, including for retention and disposition schedules;
- access to data was restricted to a limited number of personnel who demonstrated knowledge of CSE's legal and policy framework;
- access to use, analyse, and report data was subject to approval processes to ensure proper oversight and privacy considerations;
- privacy annotations were applied to track the number and foreign intelligence value of incidentally acquired private communications (PCs) retained and to automatically delete those that were not deemed to be essential to international affairs, defence, or security interests, including cybersecurity;
- Canadian identity information (CII) was suppressed in reporting; and,
- disclosure of suppressed CII was subject to strict requirements and tracking.

Additionally, CSE has an internal compliance team that helps CSE meet its legal and policy obligations with respect to the acquisition, use (analysis), 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. These compliance monitoring activities are conducted using a risk-based approach. During the period the Authorization was in place, the internal compliance team examined aspects of acquisition and handling of data [REDACTED] Where compliance



issues were identified, required actions were prescribed to mitigate risks. Additionally, recommendations were made to further enhance practices and systems going forward.

In [REDACTED] the internal compliance team began an operational compliance incident assessment looking into [REDACTED]



PRIVATE COMMUNICATIONS, SOLICITOR-CLIENT COMMUNICATIONS, AND CANADIAN IDENTITY INFORMATION

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.

Of the [REDACTED] communications acquired through [REDACTED] activities, [REDACTED] were recognized as incidentally acquired PCs under the Authorization. Incidental acquisition of information relating to Canadians or persons in Canada is provided for subsection 23(4) of the CSE Act. Of the [REDACTED] incidentally acquired PCs, [REDACTED] were retained [REDACTED] were used in a report and [REDACTED] were retained for future use). The remaining [REDACTED] incidentally acquired PCs were marked for deletion as they did not include information essential to international affairs, defence, or security interests, including cybersecurity.

In total, there were [REDACTED] PCs used in [REDACTED] reports issued between [REDACTED] of the PCs were acquired during this timeframe; the other [REDACTED] PCs used in a report were acquired prior to [REDACTED]

CSE analysts may amend the annotations or markings associated with communications data held in CSE databases over time. These changes are normal and demonstrate that CSE continually reassesses the data it acquires as new information becomes available. Consequently, a snapshot of CSE's database holdings taken at one point in time may differ from the snapshot at a different point in time, even for the same reporting year.



For example, based on new information, a recognized PC deemed essential at one point in time could later be deemed non-essential and destroyed. This can produce variations in the number of PCs residing in CSE databases from one reporting period to another. The metrics provided in this report accurately reflect CSE's assessment of its data repositories as of [REDACTED]

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 international affairs, defence, or security interests, including cybersecurity. Before using, 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 that an individual or group is in imminent danger of death or serious bodily harm, the Chief, CSE, may use, analyse, retain, or disclose the information to the extent necessary to address the imminent danger. The Chief, CSE, shall advise the Minister of National Defence, in writing, no later than 48 hours after such a 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.¹¹

Foreign Intelligence Products Containing Suppressed Canadian Identity Information

When targeting foreign entities, CSE may incidentally acquire PCs or information about a Canadian entity. If the information about the Canadian entity or entity in Canada is deemed essential to international affairs, defence, or security interests, including cybersecurity, CSE has the authority under the CSE Act to retain that information for use and analysis. In these cases, CSE must apply measures to protect the privacy of the entity. The most common protection measure is the suppression of information with a privacy interest, whereby the CII is replaced by a generic term such as "Named Canadian Company 1." Other measures can include restricted dissemination and/or handling caveats.

¹¹ During the Authorization period, CSE incidentally acquired one solicitor-client communication that was immediately deleted and was not retained (used or analysed).



CSE may only release CII suppressed in foreign intelligence reporting to partners or other GC departments upon request. The disclosure must also be considered essential to international affairs, defence, or security interests, including cybersecurity. Furthermore, these recipients must have been designated by the Minister of National Defence under section 45 of the CSE Act, and must submit a rationale for the request to receive unsuppressed CII. For example, [REDACTED]

Between [REDACTED] communications were acquired [REDACTED] During the same timeframe, CSE and CFIOG used [REDACTED] of these communications to issue [REDACTED] foreign intelligence reports. [REDACTED] reports contained CII.

Examples of the types of CII shared in these reports includes [REDACTED]

[REDACTED] Of those reports, [REDACTED] were derived from a PC. CSE approved [REDACTED] disclosure requests for CII based on those reports, primarily to [REDACTED] one approved disclosure request based on those reports was to [REDACTED] The approved disclosure request to [REDACTED] was for [REDACTED]

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 70 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] following the Intelligence Commissioner's approval, 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.

¹² Total approved disclosure requests as of [REDACTED] Requests can include multiple suppressed identities that are found in the report.



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

Foreign Intelligence Authorization



© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

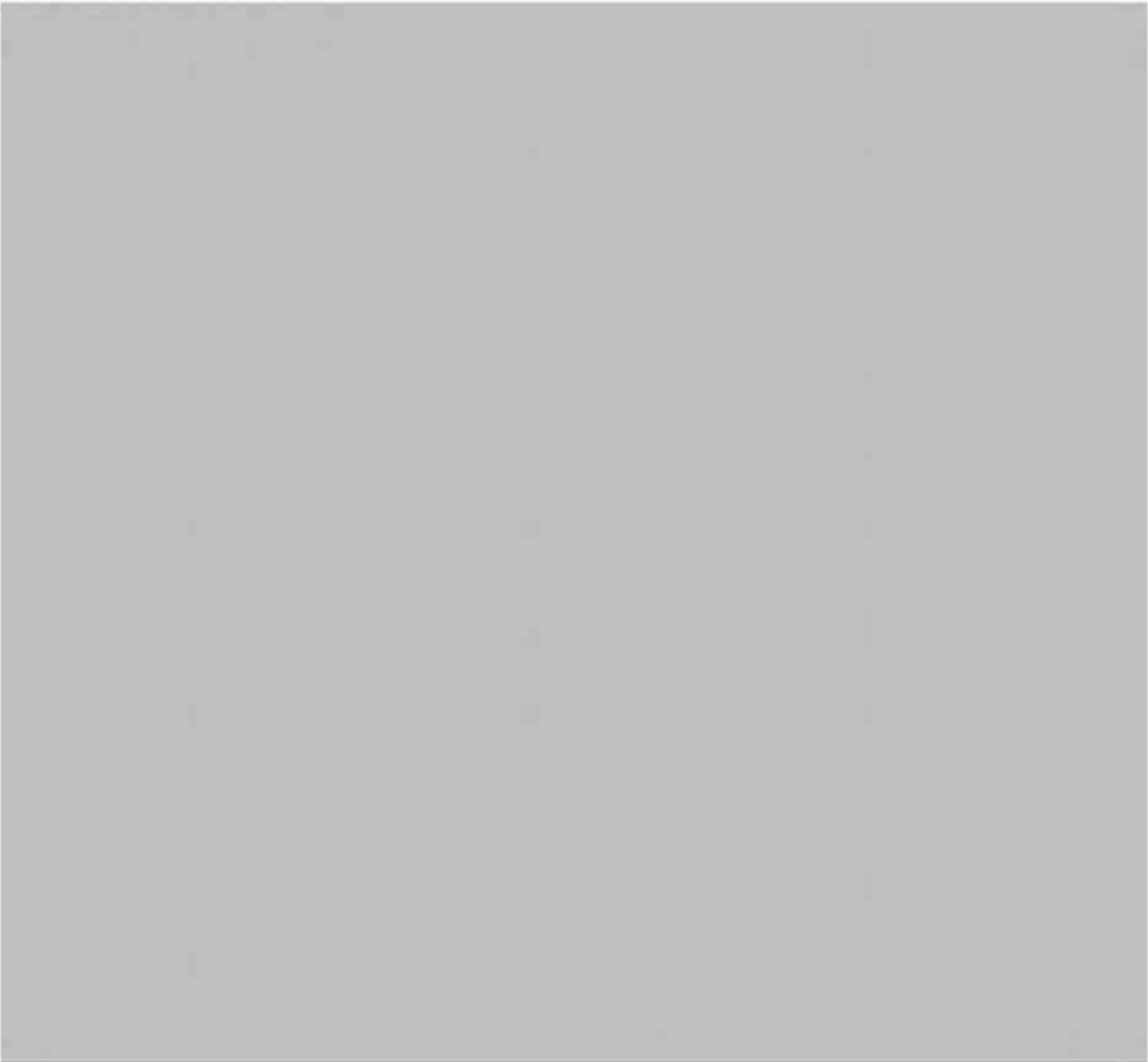


INTRODUCTION

the Communications Security Establishment (CSE) was granted a Foreign Intelligence Authorization (Authorization) under subsection 26(1) of the *Communications Security Establishment Act* (CSE Act). The Authorization was repealed and replaced on 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 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





OUTCOMES OF THE ACTIVITIES CONDUCTED UNDER THE AUTHORIZATION

[REDACTED] CSE analysts viewed or assessed [REDACTED] activities to produce a variety of products.

Foreign Intelligence Reports

- CSE and the Canadian Forces Information Operations Group (CFIOG), which is a CAF entity that conducts SIGINT activities [REDACTED] issued [REDACTED] regular foreign intelligence reports [REDACTED]

- Of the [REDACTED] regular foreign intelligence reports:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]

- [REDACTED]



[REDACTED]

Indications and Warnings

- [REDACTED] reports were issued by CSE and CFIOG to provide indications and warnings

[REDACTED]

Cyber Threat Tips

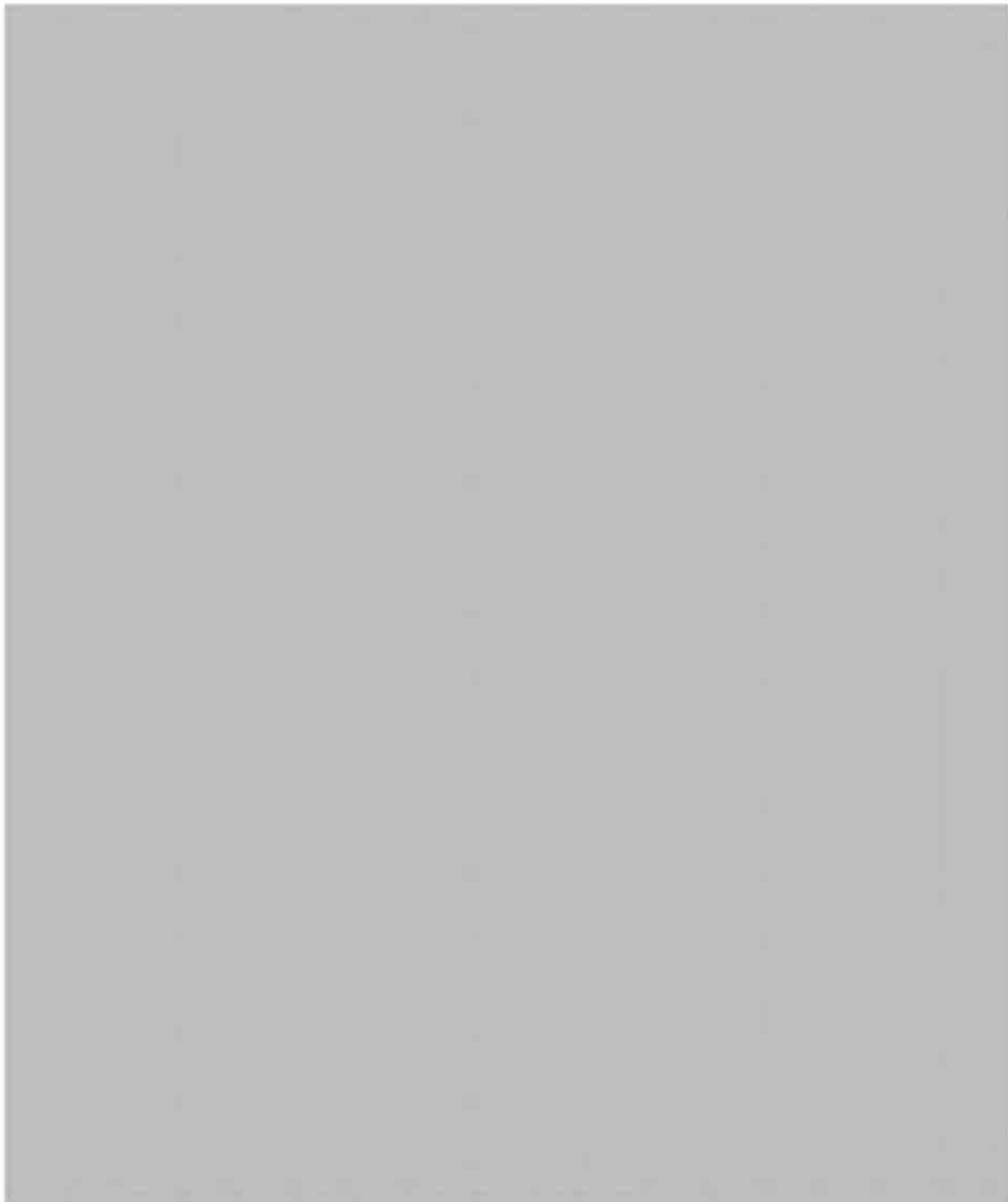
- [REDACTED]
- [REDACTED]

[REDACTED]

**Pages 73 to / à 80
are withheld pursuant to sections
sont retenues en vertu des articles**

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

**of the Access to Information
de la Loi sur l'accès à l'information**



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 foreign intelligence activities. CSE's Mission Policy Suite (MPS) Foreign Intelligence 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 foreign intelligence activities while ensuring that information with a Canadian privacy interest is protected. A layered suite of privacy measures is built into CSE processes, training, and compliance programs. Broadly speaking, MPS Foreign Intelligence 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 the 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;
- access to use, analyse, and report data was subject to approval processes to ensure proper oversight and privacy considerations;
- privacy annotations were applied to track the number and foreign intelligence value of incidentally acquired private communications (PCs) retained and to automatically delete those that were not deemed to be essential to international affairs, defence, or security interests, including cybersecurity;
- Canadian identity information (CII) was suppressed in reporting; and,
- disclosure of suppressed CII was subject to strict requirements and tracking.

Additionally, CSE has an internal compliance team that helps CSE meet its legal and policy obligations with respect to the acquisition, use (analysis), 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. These compliance monitoring activities are conducted using a risk-based approach. During the period the Authorization was in place, the internal compliance team examined aspects of querying, handling, and sharing data involving passive accesses. Where compliance issues were identified, required actions were prescribed to mitigate risks. Additionally, recommendations were made to further enhance practices and systems going forward.

PRIVATE COMMUNICATIONS, SOLICITOR-CLIENT COMMUNICATIONS, AND CANADIAN IDENTITY INFORMATION

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.

Of the [REDACTED] communications assessed by CSE, [REDACTED] were recognized as incidentally acquired PCs under the Authorization. Incidental acquisition of information relating to Canadian or persons in Canada is provided for in the CSE Act at subsection 23(4). Of the [REDACTED] incidentally acquired PCs, [REDACTED] were retained, including [REDACTED] used in [REDACTED] foreign intelligence reports. The remaining [REDACTED] PCs were marked for deletion as they



did not include information essential to international affairs, defence, or security interests, including cybersecurity.

CSE analysts may amend the annotations or markings associated with communications data held in CSE databases over time. These changes are normal and demonstrate that CSE continually reassesses the data it acquires as new information becomes available. Consequently, a snapshot of CSE's database holdings taken at one point in time may differ from the snapshot at a different point in time, even for the same reporting year.

For example, based on new information, a recognized PC deemed essential at one point in time could later be deemed non-essential and destroyed. This can produce variations in the number of PCs residing in CSE databases from one reporting period to another. The metrics provided in this report accurately reflect CSE's assessment of its data repositories as of [REDACTED]

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 international affairs, defence, or security interests, including cybersecurity. Before using, 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 that an individual or group is in imminent danger of death or serious bodily harm, the Chief, CSE, may use, analyse, retain, or disclose the information to the extent necessary to address the imminent danger. The Chief, CSE shall advise the Minister of National Defence, in writing, no later than 48 hours after such a 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.

Foreign Intelligence Products Containing Suppressed Canadian Identity Information

When targeting foreign entities, CSE may incidentally acquire PCs or information about a Canadian entity. If the information about the Canadian entity or entity in Canada is deemed essential to international affairs, defence, or security interests, including cybersecurity, CSE has the authority under the CSE Act to retain that information for use



and analysis. In these cases, CSE must apply measures to protect the privacy of the entity. The most common protection measure is the suppression of information with a privacy interest, whereby the CII is replaced by a generic term such as "Named Canadian Company 1." Other measures can include restricted dissemination and/or handling caveats.

CSE may only release CII suppressed in foreign intelligence reporting to partners or other GC departments upon request. The disclosure must also be considered essential to international affairs, defence, or security interests, including cybersecurity. Furthermore, these recipients must have been designated by the Minister of National Defence under section 45 of the *CSE Act*.

[REDACTED] CSE and CFIOG analysts viewed or assessed [REDACTED] unique communications [REDACTED]. During the same timeframe, CSE and CFIOG used [REDACTED] of these communications to issue [REDACTED] reports. [REDACTED] reports contained CII.

Examples of the types of CII shared in these reports includes [REDACTED]

Of those reports, [REDACTED] were derived from a PC. CSE approved [REDACTED] disclosure requests for CII based on those reports, [REDACTED]

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 72 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] following the Intelligence Commissioner's approval, 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.

¹⁶ Total approved disclosure requests as of [REDACTED] Requests can include multiple suppressed identities that are found in the same report.