Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

P.O. Box 9703
Terminal
Ottawa, Canada
K1G 3Z4

C.P. 9703
Terminus
Ottawa, Canada
K1G 3Z4

Our file Notre référence
A-2016-00101

MAR 2 0 2017

Mr. Matthew Braga
Senior Technology Reporter
CBC News
CBC Toronto Newsroom
205 Wellington St. West
Toronto, ON M5V 3G7

Dear Mr. Braga:

This is further to your request submitted under the *Access to Information Act* received on December 20, 2016 for:

> *"Briefing notes, memos, guidelines, presentations, privacy impact assessments, reports, and/or studies on policies pertaining to law enforcement agencies seeking electronic investigative assistance from intelligence agencies (under Mandate C). Limit search to last five years."*

Enclosed please find a portion of the requested records that could be located using the Department's best efforts, within the restraints of the *Act.* You will notice that certain information has been withheld from disclosure pursuant to sections 15(1) - DEF Defence of Canada, 15(1) - IA International Affairs, 16(1)(a) information obtained or prepared by an investigative body, 16(1)(b) investigative techniques or plans, 21(1)(a) advice or recommendations, and 23 solicitor-client privilege information of the *Act.*

Please note that the enclosed records are an interim release of a portion of the material relevant to your request. Additional documents will be provided on completion of their review.

Please be advised that you are entitled to file a complaint with the Office of the Information Commissioner concerning the processing of your request within sixty days of the receipt of this notice. In the event that you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3

Should you require any additional information or assistance regarding this request, please contact the CSEC ATIP Unit at (613) 991-8443.

Yours sincerely,

for

Dominic Rochon
Access to Information and Privacy Coordinator

Enclosure: 97 pages

Canada

15(1) - DEF DEFENCE OF CANADA
information the disclosure of which could reasonably be expected to be injurious to the conduct of the defence of Canada or any state allied or associated with Canada

---

15(1) - IA INTERNATIONAL AFFAIRS
information the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs

---

16(1)(a) INFORMATION OBTAINED OR PREPARED BY AN INVESTIGATIVE BODY
information obtained or prepared by any government institution, or part of any government institution, that is an investigative body specified in the regulations in the course of lawful investigations pertaining to

---

16(1)(b) INVESTIGATIVE TECHNIQUES OR PLANS
information relating to investigative techniques or plans for specific lawful investigations;

21(1)(a) ADVICE OR RECOMMENDATIONS
advice or recommendations developed by or for a government institution or a minister of the Crown,

---

21(1)(b) CONSULTATIONS OR DELIBERATIONS
an account of consultations or deliberations involving officers or employees of a government institution, a minister of the Crown or the staff of a minister of the Crown,

---

23 SOLICITOR-CLIENT PRIVILEGE INFORMATION
The head of a government institution may refuse to disclose any record requested under this Act that contains information that is subject to solicitor-client privilege.

---

25 April 2016

SECRET//SI
CERRID 26618433

MEMORANDUM FOR THE POLICY COMMITTEE

OPS-4: Policy on Assistance to Law Enforcement and Security Agencies under Part (c) of CSE's Mandate

(For Decision)

Summary

- *OPS-4* modernizes and clarifies existing policies governing CSE's assistance to LESAs, and outlines the governing principles for CSE's activities under Part (*c*).
- This new policy also satisfies OCSEC's recommendation from the 2015 review of CSE support to CSIS under section 16 of the *CSIS Act*.
- *OPS-4* has been reviewed by Directors SPR, DPR, ITS PMO and by DLS. It is recommended that you approve the attached draft.

Background

- CSE's assistance activities are currently governed by two operational policies:
  - OPS-4-1: *Operational Procedures for Assistance to Law Enforcement and Security Agencies Under Part (c) of CSEC's Mandate;* and
  - OPS-4-3: *Procedures Related to the Section 16 Program.*
- The primary drivers for the need to refresh these policies are the introduction of the *Protection of Canada from Terrorists Act* and *the Anti-Terrorism Act, 2015,* and the need for clearer and more comprehensive policies and procedures.
- Corporate and Operational Policy is proposing to rescind *OPS-4-1* and *OPS-4-3*, and replace them with a policy that is more principles-based, relevant and adaptable to developments in the technological, political and legislative spaces. Concurrently, SPR is developing a new operational instruction, which will complement *OPS-4*, to provide better and updated direction on requests for assistance (RFAs).
- Reflecting legislative changes, s.16 requests are now subject to the RFA process. This satisfies OCSEC's recommendations from its review of s.16 activities to update the s.16 governance framework.

- The new policy:
    - Is broad in scope to ensure relevance to all Part (c) activities and to the diverse groups within SIGINT and ITS that undertake these activities;
    - Accommodates the changing operational environment;
    - Delegates detailed procedures (such as SLA procedures) to the operational instruction level;
    - Establishes the conditions for CSE assistance and defines the categories of assistance; and
    - Defines the principles for naming under Part (c), which are currently included in OPS-1-7: *Operational Procedures for Naming in SIGINT Reports*.

Recommendation

- It is recommended that you approve the attached draft of *OPS-4*.

Communications Security Establishment | Centre de la sécurité des télécommunications

OPERATIONAL POLICY

OPERATIONAL POLICY
OPS-4

Policy on Assistance to Law Enforcement and Security Agencies under Part (c) of CSE's Mandate

Effective Date:

2 August 2016

1. Introduction

1.1. Objectives

The objective of this policy is to provide the governing principles for CSE's activities under Part (c), including:

- Conditions for providing assistance to federal law enforcement and security agencies (LESAs); and
- Engaging LESAs and proper use of Part (c) material.

1.2. Context

As Canada's national cryptologic agency, CSE possesses unique capabilities to support LESAs in the performance of their lawful duties. All CSE assistance activities must comply with Canadian laws (including, but not limited to, the *National Defence Act* (*NDA*), the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*) and limitations imposed on the requesting LESA by their respective legislations.

CSE must adhere to agreements or arrangements signed with the respective LESAs (for details of these agreements, contact SPR1).

1.3. Authority to Assist

CSE's authority to assist LESAs comes from paragraph 273.64(1)(*c*) of the *NDA*, which states that CSE has the mandate to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. The requesting LESA must have the lawful authority to conduct the activity being requested before CSE can provide assistance.

Any CSE business line may be called upon to provide assistance and all business lines may collaborate on requests.

1.4. Application

This policy applies to CSE staff and other parties involved in providing assistance to LESAs.

All contractors' involvement in providing assistance to LESAs must be approved by the Director, SIGINT Policy and Review (SPR) (for SIGINT) or the Director, IT Security Programs, Education and Oversight (PEO) (for IT Security).

1.5. **Previous Procedures**

This policy supersedes the following procedures relating to Part (c):

- OPS-4-1: *Operational Procedures for Assistance to Law Enforcement and Security Agencies Under Part (c) of CSEC's Mandate*; and
- OPS-4-3: *Procedures Related to the Section 16 Program*[1].

1.6. **Review**

All CSE activities, including those conducted under Part (c) of its mandate, are subject to internal monitoring, including internal Audit and Evaluation, for policy compliance, and external audit and review by various government review bodies, including, but not limited to, the Office of the CSE Commissioner (OCSEC) and the Privacy Commissioner.

All CSE staff are required to fully comply with and facilitate reviews relating to this policy, and any activities conducted under its authority.

[1] Note that the Section 16 program is now subject to the standard request for assistance (RFA) process. Therefore, all principles for the RFA process also apply to s.16 activities.

s.15(1) - DEF

2. Assisting LESAs

2.1. **Defining LESA**

LESAs include the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP). As the CSE position responsible for administering the request for assistance (RFA) process, Director, SPR determines the LESA status of all other agencies seeking assistance on a case-by-case basis.

2.2. **Conditions for Assisting**

In undertaking assistance activities, CSE must:

- Assist only those agencies that have demonstrated their status as a LESA;
- Receive a written RFA;
- Ensure the request states the LESA's authority to undertake the requested assistance and information contained in the request was lawfully obtained;
- Assess the legal, policy and disclosure risks prior to approving RFAs; and

2.3. **Defining Assistance**

CSE provides technical and operational assistance, which may include, but is not limited to: training; products and services related to

Note: Activities carried out by CSE in assistance to LESAs in conducting their lawful duties are subject to any limitations imposed by law on the LESAs.

s.15(1) - DEF

2.4. **Receiving Requests for Assistance**

CSE may only provide assistance as authorized in the *NDA* upon receipt of a written request. However, CSE operational elements are encouraged to collaborate with the requesting agency through all stages of the RFA, including providing feedback to help prepare the RFA.

Substantive changes to RFAs (e.g., changes to activities authorized under the RFA) requires the resubmission of the written request.

Some activities requested under Part (c) can be lawfully conducted under Parts (a) and/or (b) of CSE's mandate. Director SPR may consult with the requesting agency prior to making a determination.

Attention: CSE must comply with all conditions stipulated in the approved RFA.

2.5. **Tracking RFAs**

CSE must regularly review the status of RFAs.

If…	Then…
The RFA has an expiry date (i.e., a warrant)	The RFA must be renewed and reviewed completely to be considered valid.
The RFA does not have an expiry date	The RFA should be reviewed annually by the requesting officer and the operational area to confirm validity and renew dates.

When an active RFA expires, assistance must be discontinued and requests closed unless the LESA submits a new RFA to renew or continue the assistance.

Any activity taken under the authority of an expired RFA is a compliance incident and must be assessed accordingly.

2.6. **Provincial, Territorial or Municipal Law Enforcement**

CSE cannot support provincial, territorial or municipal law enforcement agencies under Part (c) of its mandate. The RCMP can participate in joint operations with these agencies, and CSE can assist the RCMP with those activities the RCMP lawfully contributes to in these joint operations.

2.7. **ELINT Requests from DND and CAF**

CAF and DND are not considered LESAs. Consult *CSOI-3-6: Instructions for the Provision of ELINT Information to the Department of National Defence and the Canadian Forces on Entities* for more information on ELINT assistance.

3. Approving Requests for Assistance (RFAs)

3.1. **Approval Process**

Prior to accepting or denying a request, CSE must assess the risk, feasibility and resources required to provide assistance. CSE may seek additional policy and/or legal evaluations of the proposed activities.

Director, SPR is accountable for the approval of all RFAs and responsible for administering the RFA process. When approving RFAs, Director, SPR should assess the following:

- CSE's ability to commit to providing the requested assistance;
- Any policy and compliance risks; and
- How the requested assistance might affect CSE's obligations to its partners.

CSE reserves the right to implement stricter privacy protection measures when fulfilling an RFA than what was stipulated by the requesting LESA.

An RFA may cover a broad series of activities not requiring individual approval.

3.2. **Determining Lawfulness**

To meet its obligations under the *NDA,* CSE must be satisfied that LESAs have the lawful authority to conduct the activity requested. CSE must take measures to assess this lawfulness.

CSE must receive written assurances that:

1. Any information the LESA provides in support of its RFA has been lawfully obtained; and
2. The LESAs have the legal authority to undertake the requested assistance. Documentation proving this authority may include (but are not limited to):
    - A statement of the applicable legislative authority;
    - A judicial authorization; or
    - Individual written consent.

3.3. **Advice and Responsibility**

The responsibility for the RFA approval process lies with Director, SPR and the business lines named in the RFA. The CSE teams providing assistance are responsible for all activities conducted in fulfilling the RFA.

Corporate and Operational Policy (D2) will provide advice and guidance on new types of activities, but is not an approval authority for RFAs.

s.15(1) - DEF

4. Protecting Intelligence Information

4.1. Corporate Files and Record Keeping

For audit and review purposes, CSE is expected to maintain records of its Part (c) activities.

CSE must maintain records that demonstrate:

- The LESA supplied CSE with a request in writing;
- The LESA has the lawful authority to conduct the activity requested;
- The information provided to CSE for the purpose of rendering assistance was lawfully obtained by the LESA; and
- The activities CSE approved and conducted in response to the RFA.

These records include the RFA,
confirming or clarifying authorized activities.

The Director, SPR is responsible for coordinating the retention of these corporate files. Operational directors overseeing activities pursuant to the approved RFA are accountable for maintaining records of these activities.[2]

SPR1 is responsible for maintaining all documentation associated with processing RFAs (including, but not limited to, drawings, diagrams, specifications, legal opinions, responses and completion times), regardless of which business line provided the assistance.

4.2. Safeguarding Sensitive LESA Material

CSE staff processing RFAs must ensure that sensitive material (e.g., warrants) provided by the LESAs is adequately protected in accordance with terms set out in the RFA.

Note: Contact the Security Secretariat (S4) for guidance on applying the need-to-know principle.

[2] IM Governance and Compliance (CIO-E1B) manage the retention schedules.

s.15(1) - DEF

4.3. **Retaining and Destroying LESA Material**

Upon completion of a request for assistance, CSE must follow the LESA's instructions for the return, retention or destruction of LESA supplied material and any recovered data or information that CSE may hold.

All CSE administrative records associated with the request must be retained in accordance with CSE's SIGINT Records disposition authority and schedule.

Note: Individual programs operating under Part (c) may have their own operational instructions for
Please refer to those policy instruments for more detailed instructions.

4.4.

When operating under LESA authorities, CSE is still responsible for

CSE must take measures to protect

Note: All information and intelligence provided to LESAs by CSE that bears the Special Intelligence (SI) marking must be handled and protected in accordance with *CSSS-100*.

4.5. **Risk of Legal Disclosure**

CSE assistance to LESAs may risk the possible disclosure of sensitive information or assets in legal proceedings such as criminal prosecutions.

To address these concerns, CSE must assess and mitigate disclosure risks in accordance with *ORG-4: Evidentiary Disclosure Risk Management Policy*.

CSE must notify the National Security Advisor (PCO) and the Minister of National Defence when the role of CSE may be revealed or when CSE intends to request that legal proceedings be halted due to the likelihood of disclosure of sensitive information.

4.6. **Using Part (c) Information for Parts (a) or (b)**

Unless the requesting LESA specifies that the use is permitted under Parts (a) and (b), CSE **may not** otherwise use information obtained through its Part (c) assistance activities.

5. Reporting

5.1.	**Report Dissemination**	Dissemination of reports produced under Part (c) must be limited to those organizations and individuals specified by the requesting agency.
5.2.		
5.3.	**Write-to-Release (WTR)**	Part (c) reports may be candidates for write-to-release (WTR) reporting. See *CSOI-4-5: Write-to-Release (WTR) Guidelines* for more information.
5.4.		

s.15(1) - DEF

6. CSE Roles and Responsibilities

6.1. Roles and Responsibilities

This table describes the key responsibilities with respect to CSE's activities in support of LESA RFAs.

Who	Responsibility
Directorate of Legal Services (DLS)	Providing legal advice, as required
Director, Disclosure, Policy and Review (DPR)	• Acting as authority for Disclosure Risk Management (DRM) issues, on behalf of the Chief • Advising the Chief on issues related to DRM
Director, SIGINT Policy and Review (SPR)	• Approves RFAs (under normal circumstances). • Confirming whether the GC departments or agencies have LESA status • Determining whether SIGINT can proceed with LESA requests • Coordinating, maintaining and accounting for corporate files relating to Part (c) activities
Director, IT Security PEO	Determining whether IT Security can proceed with LESA requests
Relevant operational directors	• Approving or denying the provision of assistance based on (This responsibility may be delegated down, in writing, to relevant operational managers) • Maintaining corporate files • Approving release of tools to LESAs
SIGINT Policy and Review	• Managing the RFA process • Reviewing the status of all requests • Validating requests annually with LESAs • Maintaining all documentation associated with requests for assistance
Relevant CSE Offices (via SPR1 or IPOC)	• Providing assessment during the RFA approval process • Providing assistance • Maintaining records of Part (c) activities
Corporate and Operational Policy (D2)	Providing advice and guidance on new assistance types and privacy-related questions, as required

7. Accountability for OPS-4

7.1.	**Accountability**	Refer to *ORG-1-1: Procedures for the Approval of CSE Policy Instruments* for details on accountabilities and approvals for this policy.
7.2.	**Policy Approval**	This policy was approved by the Policy Committee on (Day/Month/Year). Minor amendments may be approved by Director, Disclosure, Policy and Review.
7.3.	**Amendments**	Situations may arise where amendments to these procedures are required because of changing or unforeseen circumstances. Such amendments will be communicated to relevant staff appropriately.
7.4.	**Exceptional Authorization**	The Policy Committee may approve exceptions to this policy. Requests for exceptional authorizations must be submitted to Corporate and Operational Policy and will include rationales outlining: • The reason for the exception (e.g., why the request falls outside the scope of this policy); • The operational need that justifies the exception; and • The impact of the request on the privacy interests of Canadians (or persons in Canada).
7.5.	**Consequences of Not Complying**	Failure to comply with OPS-4 could have serious consequences, including damage to CSE's reputation or the reputation of its Government of Canada partners, or the cessation of CSE activities. The Chief is accountable for ensuring that appropriate corrective measures have been taken with those CSE personnel found to have acted in non-compliance with this policy. Corrective measures can range from training, to the suspension or removal of delegated authority, to taking disciplinary action, up to and including termination of employment, or any combination of these measures.
7.6.	**Questions**	Questions regarding this policy should be addressed to @cse-cst.gc.ca.

Communications Security Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean - Pierre Plouffe, C.D.

TOP SECRET // SI // **// CEO**

Our file # 2200–87

March 6, 2015

The Honourable Jason Kenney, P.C., M.P.
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Dear Minister:

The purpose of this letter is to provide you with the results of my review of CSE activities conducted under section 16 of the *Canadian Security Intelligence Service Act* (*CSIS Act*) and subsection 273.64(1)(*c*) of the *National Defence Act* (*NDA*). This review was undertaken under my general authority as articulated in Part V.1, paragraph 273.63(2)(*a*) of the *NDA*.

The primary objectives of this review were to acquire detailed knowledge of and to document CSE assistance to CSIS for s. 16 activities and any changes since the last in-depth review (2004), to assess whether the activities complied with the law, including the terms of the warrants issued to CSIS, and to assess the extent to which CSE protected the privacy of Canadians in carrying out the assistance to CSIS.

Section 16 of the *CSIS Act* authorizes CSIS to assist the ministers of Foreign Affairs and National Defence in foreign intelligence collection activities, within Canada, in support of the foreign and defence interest of the Government of Canada. Section 16 activities involving interception require the approval of a Federal Court judge in accordance with s. 21 of the *CSIS Act*. CSE may provide CSIS with technical and operational assistance for s. 16 warrants.

Based on the information reviewed and the interviews conducted, I have concluded that CSE's assistance to CSIS under s. 16 of the *CSIS Act* was conducted in accordance with the law, Ministerial Directives and CSE policy and procedures. CSE also conducted its activities in a manner that includes measures to protect the privacy of Canadians. However, I did make a number of recommendations, which are set out below.

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
T: 613-992-3044 F: 613-992-4096

In 2007 and early 2008, the Privy Council Office (PCO) led interdepartmental discussions related to changes in how the s. 16 process worked within the Security and Intelligence (S&I) Community. One of the changes made was the elimination of the 1987 Tri-Ministerial MoU, formally titled, *Memorandum of Understanding on Section 16 of the CSIS Act*. I was provided with a copy of the letter (undated) signed by the then Ministers of Public Safety, National Defence and Foreign Affairs outlining the changes to the s. 16 approval process. I was also provided a copy of a memorandum indicating that the matter was reviewed by the Prime Minister on March 27, 2008. The results and impact of these changes is detailed in the report.

The Tri-Ministerial MoU of 1987 contained specific procedures related to the process to be followed, including the roles and responsibilities of each of the parties to the agreement. CSE has captured much of this process as it relates to its assistance under s. 16 in its own internal policies and procedures, which is still relevant today. However, these policies and procedures still make reference to the 1987 MoU despite the fact the MoU was eliminated. The introduction of the new process noted above did not include any formal procedures and associated roles and responsibilities as had been included in the 1987 MoU. Therefore, **I recommend** that CSE initiate discussions with CSIS and the other related parties to ensure that the processes, roles and responsibilities contained in the former Tri-Ministerial MoU are formalized in a document that reflects the current process. **I also recommend** that CSE remove all references to the 1987 MoU in its policies and procedures, and at the same time ensure all its internal policies are consistent with and reflect the new approval process.

A review of this activity in 2008 by one of my predecessors included a recommendation that the operational assistance MoUs, dated November 1990 (CSE-CSIS s. 16 MoU as well as the CSE-CSIS s. 12 MoU), be updated to reflect the then current practices. CSE accepted this recommendation and responded that it would agree to work with CSIS to update the MoU. In 2010 and 2011, CSE indicated that after a new General Framework MoU was signed between CSE and CSIS, it would undertake the modernization of the s. 16 and s. 12 MoUs and that they would be included as appendices to the new agreement. This General Framework MoU was signed by both parties in December 2011. The updating of the s. 16 and s. 21 MoUs have not yet occurred. Therefore, **I recommend** that CSE ensure that these MoUs be updated and finalized in a timely manner to reflect current practices, processes and agreements between CSE and CSIS.

Given that CSIS is implicated in the updates of these MoUs, I am informing the Chair of the Security Intelligence Review Committee (SIRC) of my recommendations. Our co-ordination with SIRC of activities involving both CSE and CSIS helps ensure more comprehensive review.

CSE's activities in providing assistance to CSIS under s. 16 of the *CSIS Act* are subject to all conditions outlined in the warrants issued by the Federal Court, including the same legal requirement to protect the privacy of Canadians. As part of the agreement with

CSIS, CSE produces and disseminates foreign intelligence reports, based on s. 16 collection, to Government of Canada clients. All the reports produced from the sample of warrants that were reviewed found that all appropriate policy and procedures related to protecting privacy, such as the suppression of Canadian identity information, were followed and applied.

CSE has operational policies and procedures for assistance to s. 16 activities in place. I found that these policies and procedures provide appropriate direction to CSE employees for the protection of the privacy of Canadians. The activities reviewed that were conducted by CSE in support of CSIS under s. 16 of the *CSIS Act* were found to be in compliance with CSE's operational policy.

CSE employees interviewed were knowledgeable about and complied with policies and procedures related to CSE assistance to CSIS under s. 16 of the *CSIS Act*. CSE managers routinely monitored employees' work carried out for these activities.

As part of the overall s. 16 activities,
data it has collected. In these cases, CSE data
and requests to do so. If so, and given that the
data may contain Canadian identity information, **I recommend** that CSE develop a
caveat to indicate
that the information

CSE officials were provided an opportunity to review and comment on the results of the review, for factual accuracy, prior to finalizing the enclosed report.

If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,

Jean-Pierre Plouffe

c.c. Ms. Greta Bossenmaier, Chief, CSE

Enclosure

Office of the
Communications Security
Establishment Commissioner

CANADA

Bureau du
Commissaire du Centre de la
sécurité des télécommunications

TOP SECRET // SI //
//CEO

Our File # 2200–87

Review of Communications Security Establishment Canada's Assistance to CSIS Under Part (c) of CSEC's Mandate and Section 16 of the *CSIS Act*

March 6, 2015

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096
info@ocsec-bccst.gc.ca

TABLE OF CONTENTS

I. AUTHORITIES

This report was prepared on behalf of the Communications Security Establishment Commissioner under his authority as articulated in Part V.1, paragraph 273.63(2)(*a*) of the *National Defence Act* (*NDA*).

II. INTRODUCTION

Section 16 of the *Canadian Security Intelligence Service Act* (*CSIS Act*) authorizes CSIS to assist the ministers of Foreign Affairs and National Defence in foreign intelligence (FI) collection activities, within Canada, in support of the foreign and defence interests of the Government of Canada. Section 16 activities require a personal request for assistance from one of the above Ministers

Section 16 activities — those assessed as intrusive, like interception — require a warrant from a Federal Court judge in accordance with s. 21 of the *CSIS Act*. In these instances, CSIS must obtain a warrant from the Court authorizing the use of specific powers of collection to be directed against specific targets. The Minister of Public Safety must grant personal written consent prior to CSIS submitting a warrant application to the Court.

Communications Security Establishment Canada (CSE) may provide CSIS with technical and operational assistance for s. 16 activities under its mandate "to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties" (ss. 273.64(1)(*c*) of the *NDA*, or "part (c)" of CSE's mandate). In such cases, CSE acts as an agent of CSIS in the intercept, processing and analysis of information collected pursuant to the warrants. When carrying out activities under part (c) of its mandate for s. 16 warrants, CSE must abide by the legal limitations imposed on CSIS, such as the limitations found in the CSIS Act and the s. 16 warrants (ss. 273.64(3) of the *NDA*). Not all s. 16 activities involve warrants, or participation by CSE.

CSE assists CSIS with s. 16 activities under the authority of:

- paragraph 273.64(1)(*c*) of the *NDA*;
- the ministerial directive (MD) on *Support to Law Enforcement and Security Agencies* (December 16, 2011);
- the MD on *Accountability Framework* (November 20, 2012); and
- the MD on the *Privacy of Canadians* (November 20, 2012).

CSE s. 16 assistance to CSIS is governed by the terms and conditions of each warrant.

Additionally, CSE is also guided by the terms and conditions of:

- the new s. 16 process approved August 15, 2007, by the Deputy Ministers Intelligence Sub-Group, which replaced the former process under the 1987 Tri-Ministerial Memorandum of Understanding (MoU);
- a CSE-CSIS MoU specifically covering operational co-operation in relation to s. 16 activities (1990); and
- a framework MoU between CSE and CSIS (December 2011), which did not rescind or modify the MoUs specific to s. 16 co-operation.

During the time this review was conducted, CSE was involved warrants issued by the Federal Court pursuant to s.16 and 21 of the *CSIS Act*. CSE, during the period of review, produced s. 16 reports related to Government of Canada intelligence priorities which provided FI on subjects such as:

Although the number of s. 16 warrants CSE provides assistance on has in 2011–2012 2012–2013, CSE advised that the FI acquired through this warrant process continued to meet Government of Canada requirements.

On November 5, 2013, CSE provided the Commissioner's office with an overview briefing on its assistance to CSIS for s. 16 activities.

Rationale for conducting this review

Since the inception of the Commissioner's office in 1996, Commissioners have reviewed CSE s. 16 assistance to CSIS seven times. However, these activities have not been reviewed since 2004. This assistance to CSIS may involve the communications of Canadians and therefore can impact their privacy. As this assistance is carried out under part (c) of CSE's mandate, it is subject to any limitations imposed by law on CSIS. It is for these reasons that the Commissioner selected s.16 activities for review.

III. OBJECTIVE

The objectives of the review were:

- to acquire detailed knowledge of and to document CSE s. 16 assistance to CSIS and any changes since the last in-depth review (2004);
- to assess whether the activities complied with the law, including the terms of the warrants issued to CSIS; and