- to assess the extent to which CSE protected the privacy of Canadians in assisting CSIS with s. 16 activities.

IV. SCOPE

In addition to acquiring detailed knowledge about CSE activities in providing assistance to CSIS with warranted s. 16 activities, the Commissioner's office examined:

- the legislative and policy framework under which CSE provides assistance to CSIS;
- policy and guidance, including the MoUs between CSE and CSIS for s. 16 co-operation;
- whether CSE's targeting, collection and associated activities were consistent with the requests for assistance from CSIS and associated warrants and authorities;
- associated technology, databases and systems used by CSE;
- a sample of communications collected and shared and the resultant FI and reporting;
- the extent to which technology was used and other efforts were applied to protect the privacy of Canadians; and
- CSE activities in response to previous associated findings and recommendations of Commissioners.

V. CRITERIA

A) Legal Requirements

The Commissioner expects CSE to conduct its activities in accordance with the *NDA*, the *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code*, and any other relevant legislation or authorities, and in accordance with Justice Canada legal advice.

B) Ministerial Requirements

The Commissioner expects CSE to conduct its activities in accordance with ministerial direction and to follow all requirements and limitations set out in such direction.

C) Policies and Procedures

The Commissioner expects CSE:

i) to establish appropriate policies and procedures to guide its activities and to provide sufficient direction on legal and ministerial requirements, including the protection of the privacy of Canadians;

ii) to ensure its employees are knowledgeable about and comply with policies and procedures; and

iii) to maintain the integrity of operational activities by applying an effective compliance validation framework to its activities, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

VI. METHODOLOGY

In November 2013, CSE provided a comprehensive overview briefing on its assistance to CSIS under s. 16 warrants and related activities. The Commissioner's office examined hard copy and electronic records, correspondence and other documentation relevant to CSE's assistance to CSIS on s. 16 warrants and related activities, including the warrants themselves, CSE policies and procedures, and legal advice. warrants issued and expired between February 2011 and October 2013 were examined. A sample warrants were chosen, be the subject of in-depth review and represented a review of only technical assistance by CSE to CSIS.

The Commissioner's office examined all records and documentation and then discussed them with CSE during interviews and briefings, and CSE provided answers to an extensive number of written questions.

The Commissioner assessed CSE's assistance and activities against the criteria and arrived at conclusions respecting the objectives. This report is the outcome. Annex A contains the review findings and recommendations and Annex B lists the interviewees for this review.

VII. BACKGROUND

Changes to the Approval Process

Section 16 of the *CSIS Act* explicitly vests authority for the initiation of s. 16 activities with the Ministers of Foreign Affairs and National Defence. Launching a s. 16 operation requires a personal request for assistance from the initiating minister (more commonly the Minister of Foreign Affairs or, on occasion, the Minister of National Defence) and the personal written consent of the Minister of Public Safety. Should the s. 16 operation CSIS wishes to undertake require a warrant from the Federal Court, the Minister of Public Safety must grant consent and approve the application before CSIS submits it to the Federal Court.

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 Community (S&I). 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.*

The Commissioner's office was provided with documentation on January 14, 2014, which outlined the changes made to the approval process for the collection of FI under s. 16 of the *CSIS Act,* which was approved on August 15, 2007, by the Deputy Ministers Intelligence sub-Group.[2] Included with this documentation was a copy of a letter (undated) signed by the then Ministers of Public Safety, National Defence and Foreign Affairs outlining the changes to the s. 16 approval process, and a memorandum indicating that the matter was reviewed by the Prime Minister on March 27, 2008.

Prior to the changes implemented in 2007–2008, the signatures of the ministers of National Defence and Foreign Affairs were both required on any request being put forward to the Minister of Public Safety. In addition, the previous process did not require approved and explicit criteria against which the value of the collection was assessed. The letter signed by the previous ministers to the Prime Minister stated that, "The requirement for two signatures, the increased scrutiny of the Federal Court, and the absence of approved and explicit criteria against which the value of collection is assessed, have contributed to a cumbersome, inflexible and lengthy process."[3]

The process currently in place includes the following:

1. **Explicit Criteria**: linked to government approved intelligence priorities, against which potential targets are assessed;

---

[2] See page 6 for more details on this group.
[3] Letter to the Prime Minister signed by then ministers of Foreign Affairs, National Defence and Public Safety. Undated, but it was attached to a memorandum dated July 13, 2008, from PCO that indicated the letter was reviewed by the Prime Minister on March 27, 2008.

2. **Oversight**: a permanent committee structure, up to the deputy head level, reviews all requests against criteria and intelligence priorities on an ongoing basis;

3. **Removal of Concurrence**: only the requesting minister (either Foreign Affairs or National Defence) will sign the letter to the Minister of Public Safety seeking CSIS assistance under s. 16 of the *CSIS Act*. Both will be copied on all requests (as will the National Security Advisor) for information purposes.

CSE's Role in the Process

CSE has a representative on each of the committees related to the s. 16 process. These committees, their representation and functions are broken down as follows:[4]

Deputy Ministers Intelligence Sub-group:

- comprises the National Security Advisor (Chair), Department of Foreign Affairs and Trade Development (DFATD), Department of National Defence (DND), CSIS, CSE, Privy Council Office/Security and Intelligence Directorate (PCO/S&I), Public Safety, Justice Canada, and the Royal Canadian Mounted Police; and

- receives regular updates from the Assistant Deputy Minister (ADM) Collections Committee and reviews target list on an ongoing basis in the context of broader intelligence priorities.

ADM Collections Committee:

- comprises PCO/S&I Chair, DFATD, DND, CSIS, CSE and Public Safety; and

- authorizes requests for new or renewed targets based on recommendations of the management committee — agreement triggers the exchange of letters between ministers.

Director General (DG) Management Committee:

- comprises PCO/S&I Chair, DFATD, DND, CSIS, CSE and Public Safety; and

- reviews recommendations of requirements committee against priorities and criteria.

Committee:

- comprises DFATD, CSIS and CSE;

[4] Process change document appended to letter signed by then ministers of Foreign Affairs, National Defence and Public Safety.

- is a subgroup of the DG Management Committee; and

Requirements Committee:

- comprises PCO/S&I Chair, DFATD, DND, PCO, CSIS, CSE;
- agrees on specific requirements for proposed new and /or renewed targets, including the review of rationale against priorities;
- refines tasking for collectors; and
- evaluates the value of information collected.

Those personnel responsible for DFATD and CSIS develop an individual rationale for each warrant application identifying the requirement and intended collection plan, to which CSE contributes by providing a detailed Feasibility of Collection outline of the operational capabilities for DFATD, CSIS and the Court's consideration. This outline includes:

- the rationale for the warrant;
- the target overview;
- foreign intelligence (FI) requirements against the target;
- and
- verifying included in the warrant. CSE verifies what it has received from CSIS, which remains ultimately responsible for

Overview

At the Commissioner's office request, CSE advised that for specific warrants being reviewed in detail, within the Directorate General of SIGINT Intelligence (DGI), there are areas that handle work related to s. 16 warrants. The roles and responsibilities related to each of the areas are similar with respect to its support to CSIS under s. 16.[6] Each area reviews the warrants, confirms the continued target association, analyzes traffic, prepares reports, refines requirements

[6] Details of CSE's role in the s. 16 warrant process can be found in OPS-4-3, *Procedures Related to the Section 16 Program*, 11 February 2009.

through feedback received from client(s) and detargets selectors on expiration of warrant or as directed by CSIS.

The area handles related to both parts (a) and (c) of CSE's mandate. Any reporting it compiles is and focused on

In accordance with Government of Canada intelligence priorities, focuses on:

These priorities relate to aspects of each of the s. 16 warrants CSE handled during the review period.

All these activity areas deal with the s. 16 program.

In general,

The main focus of this group is:

This section focuses on:

This section focused on:

Technical Assistance

A background briefing was requested on the warrant as this warrant was to a s. 16 warrant. CSE indicated that general operational assistance to the s. 16 warrant for CSIS's request for technical assistance.

This request for technical assistance involves CSE providing processing decryption for a specific to make the traffic legible and to disclose the results of that processing or decryption to CSIS. The works with

[8] For the purpose of this review, only were reviewed in detail.
[9] For the purpose of this review, only were reviewed in detail.
[10] For the purpose of this review, only were reviewed in detail.

the CSE Support to Lawful Access (SLA) Coordinator to prepare an operational plan that is reviewed annually by legal services and senior management at CSE. Typically, once the operational plan is approved,

CSIS personnel examine and analyze the traffic for FI and CSIS is responsible for the dissemination of any resulting intelligence.

Databases and Computer Systems

System

CSE launched its system in February 1999. This system is used to record, track and manage CSE's operational support to CSIS, under the authority of warrants issued pursuant to s. 16 of the *CSIS Act*. is managed and maintained by CSE's continues to be CSE's system of record for all information received from CSIS.

The database records warrant details such as

CSE provided the Commissioner's office with a demonstration of the system. We observed different elements of the database and how CSE officials responsible for its administration and management could make additions or modifications to the information held on all s. 16 database can also be accessed by those CSE employees responsible for producing written intelligence reports from the s. 16 warranted traffic. Access is controlled by user-access accounts and is in read-only format for analysts. Analysts can only access information that directly relates to the target they are working on.

CSE provided the Commissioner's office with a sample of four different months of reports which list all the related to s. 16 warrants. During the demonstration of the system the Commissioner's office randomly chose from the reports provided for warrants to see the details concerning each one. We were advised that the We were also advised that are never used.

Since previous reviews of CSE's support to CSIS under s. 16 were conducted before the creation or implementation of some databases, we requested that CSE provide a demonstration of a tool used by analysts to view and mark stored traffic forms of traffic collected under Section 16 warrants) in the This allowed the Commissioner's office to obtain a better understanding of the systems used by CSE analysts when working on s. 16 activities, and to verify information provided by CSE.

For the purpose of this demonstration, we viewed traffic intercepted under the warrant, which was related to one EPR produced during the review period. CSE demonstrated the other forms of traffic that relate to its current work on the warrant. CSE provided screenshots traffic related to the warrant.

For s. 16 activities, all data is segregated by its classification and the analyst/user is only permitted access to what he or she has specific clearance to see. This is controlled by the Our study of *CSE Policy Compliance Monitoring Framework and Activities*[13] indicated that access to operational information is tightly regulated and monitored through appropriate policies, procedures and various levels of compliance monitoring activities. Within the system itself, all s. 16 traffic can be retained If the data is marked for retention in accordance with proper policy parameters or is used in an EPR, The information received under a warrant maintains all the details of the status of that warrant, which is not displayed to the user.

All regular s. 16 traffic

CSE. Section 16 content that is assessed to have foreign intelligence value is retained if marked for retention or used in an End Product Report (EPR) by an analyst. Traffic that has no foreign intelligence value is not retained. If there are any other sources of traffic

[13] Study submitted to Minister of National Defence, January 20, 2014.

In addition, we were advised that there are a number of other CSE systems[14] that may also be used when providing assistance to s. 16 activities. These are listed in Annex C with a short description of each.

The activities undertaken are in accordance with the various s. 16 warrants authorized by the Federal Court.

CSE advised that there are no legal opinions directly related to operations. These operations are undertaken based on specific authorities contained in the Federal Court warrants and CSE's legal department would have been consulted only if new activities were being contemplated that did not clearly fall within the authorities granted to CSIS.

an SLA request is completed and submitted to the Director General SIGINT Programs (DGP) of CSE for coordination.

[14] RFI#3, question 4.b, dated April 14, 2014 — response received from CSE July/August 2014.
[15] relating to the warrant were supplied by CSE on November 5, 2014.

In April 2011, an email from CSIS to CSE advised that it was preparing separate SLA requests for operations that related to the warrants CSE covers on behalf of CSIS. CSE's DGP SLA Coordinator consulted with the Director SIGINT Programs Requirements (SPR) as to whether

In June 2011, CSE and CSIS met to discuss the process for operations and an email from Director SPR reaffirmed and agreed that, in operations where CSE is already providing assistance to CSIS under a warrant for the specific target, CSIS does not need to submit separate requests to CSE for assistance.

In October 2011, CSE identified the need to further formalize process and therefore organized a meeting between CSE areas involved in these operations. The topics discussed during the meeting were:

- improved communication between agencies;
- clearly articulated priorities from CSIS;
- establishment of deadlines for non-urgent situations;
- limitations of support in some instances;
- creation of a checklist to implement some of the above; and
- better understanding of operations within CSE operational areas.

Since November 2011, the process was further refined by:

- improving communications from CSIS to provide advance warning when feasible;
- providing more background information by CSIS when feasible;
- establishing a that is respected by CSIS when feasible;
- limiting CSIS requests for support to urgent situations;
- focusing on
- increasing the internal vetting performed between operational areas to enable proper consideration of the implications of requests and resource limitations.

The target of a operation can range from

targets are conducted under part (c) of CSE's mandate in conjunction with a s. 16 warrant. CSOI-2-2[16] indicates that CSE, may submit

with CSE copied on the request to determine feasibility and customer interest.

Collection Methods Used

CSE advised that the bulk of comes from In addition, CSE provided support during the period of review using collection methods:

CSE assistance to CSIS during analytical and linguistic assistance when required.[19] CSIS may, in theory, use any collection method at its disposal to execute a warrant, subject to any limitations imposed by law in the performance of its duties. If CSIS chooses to request assistance from CSE it must do so under a valid warrant pursuant to s. 16 and s. 21 of the *CSIS Act*. CSE may provide assistance using any capability at its disposal, but the assistance provided is subject to any limitations imposed by law on CSIS.

CSE provided a chart of all operations that were requested during the period under review.[20] According to the chart, there were a total of

[16] CSOI-2-2, *Section 16* July 7, 2009.

[19] CSE analytic support may extend, when required, to CSIS collection methods

[20] *CSE Support to Operations – February 1, 2011 – October 31, 2013*, dated June 19, 2014.

operations during the period of review. cancelled, was received by CSE, and because of short notice. Under the warrant,

We requested and received examples of request forms and corresponding summary forms associated with undertaken for the warrant period February 13, 2012 to February 12, 2013.

The operations undertaken related to the warrant and resulted in CSE documentation provided during the period under review indicated that reporting for these was only provided to CSIS.

The request forms from CSIS detailed:

- warrant authority;
- date of request;
-
-
-
-
- DFATD intelligence requirements to be met;
- request for CSE assistance; and
- urgency of processing/reporting.

The summary forms detailed:

- general information related to the operation;
- the key targets;
- results of activities undertaken;
- list of reports resulting from the activities undertaken; and
- procedures, which CSE's OPS-4-3, section 3.5, indicates will be done for "each special operation (including operations)."

Section 16 Collection Programs

The CSE programs that may be used for s. 16 collection are:

operate under part (a) of CSE's mandate to acquire foreign signals intelligence; however, are specific to s. 16. During the period under review, CSE advised that only collection was used in reporting for s. 16 activities.

Collection

We asked whether was used as a collection program for operations undertaken during the period under review. The analysts and team leaders interviewed indicated CSE advised that although approval to operations was first granted in 2010, it was agreed in 2011 that it could continue to be used only upon request to support the broader s. 16 program. CSE advised that was not used for any of the activities undertaken during the period under review.

The Commissioner's office was advised that CSE legal services would have been consulted if new activities were being contemplated that did not clearly fall within the authorities granted. We were advised that, while no specific legal opinion was sought or

[21] See footnote 11, page 9.

given, CSE's legal counsel was involved in

In addition, in 2010, SIGINT senior management met with and briefed

VIII. FINDINGS

A) LEGAL REQUIREMENTS

Finding no. 1: Compliance with the Law

Based on the information reviewed and the interviews conducted, CSE's activities conducted under part (c) of its mandate in providing assistance to CSIS under ss. 16 and 21 of the *CSIS Act* complied with the law.

Although the approval process changed, CSE still acts as an agent of CSIS in the processing of intercepts obtained from s. 16 warrants authorized by the Federal Court and as an agent of the requesting minister in the dissemination of the FI/EPR obtained from the interception of communications under warrant. CSE indicated that its internal processes did not change substantively, as it participated in the warrant renewal process in the same manner as before and received copies of the warrants from CSIS when they were issued by the Federal Court. CSE also indicated that Justice Canada lawyers working in CSE's Legal Services Unit are not consulted on a regular basis but all CSE employees involved in the process are aware that legal consultative services are available should a legal question arise.

The Commissioner's office asked whether CSE had requested or received any legal advice concerning the new approval process for s. 16 activities. We were advised that there was not.

CSE can also provide assistance concurrently under s. 12 of the *CSIS Act* for any of the s. 16 targets that may also be the subject of s. 12 warrants. For the period under review, we were provided with a list of s. 12 warrants that correspond to the s. 16 warrants being reviewed and were advised that this service is generally provided for targets that carry significant security concerns.

Finding no. 2: Protection of the Privacy of Canadians

Based on the information reviewed and the interviews conducted, CSE's activities conducted under part (c) of its mandate in providing assistance to CSIS under ss. 16 and 21 of the *CSIS Act* are conducted in a manner that includes measures to protect the privacy of Canadians.

Private Communications

A private communication is defined at s. 183 of the *Criminal Code*:

> any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.

The Commissioner's office asked CSE to provide information with respect to the number of EPRs generated under each warrant that contained or were based on private communications. We were advised that by their very nature, all reports based on s. 16 collection contain information derived from private communications. However, the s. 16 program falls under part (c) of CSE's mandate, not part (a), and therefore the assistance is conducted only pursuant to a warrant obtained by CSIS from the Federal Court. CSE's OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities,* states that:

> Warranted activities, such as the interception of private communications, may only be conducted against those persons or class of persons specified in each warrant.[22]

CSE's OPS-4-3,[23] provides the following definition for *information about Canadians:*

> In the context of s. 16 of the *CSIS Act*, "information about Canadians" is defined in warrants as information contained in any communication intercepted pursuant to a warrant, or information obtained that relates to a person who is a Canadian citizen, a permanent resident within the meaning of the *Immigration and Refugee Protection Act*, or a corporation incorporated by or under an Act of Parliament or of the legislature of a province.

---

[22] OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, December 1, 2012 at page 9.
[23] OPS-4-3, *Procedures Related to the Section 16 Program*, February 11, 2009, section 9.18.

One of the conditions contained in s. 16 warrants is that the privacy of Canadians must be protected when OPS-4-3 indicates that all information about Canadians must be destroyed unless the information:

- relates to activities that would constitute a threat to the security of Canada as defined in the *CSIS Act*;
- could be used in the prevention, investigation or prosecution of an alleged indictable offence; or
- relates to those foreign states, persons or corporations for which the requesting minister has personally requested assistance, in writing, pursuant to s. 16 of the Act.

CSE indicated that it is not possible to determine what percentage of the traffic received would include information about Canadians because although traffic may have been received, it may not have been accessed by an analyst and that additionally:

-
- s. 16 reporting is not subject to the same kinds of annotation requirements as CSE collection under part (a). This is set out in OPS-1, section 2.11: "Warranted activities, such as the interception of private communications, may only be conducted against those persons or class of persons specified in each warrant…There is no requirement to apply SIGINT privacy annotations to s. 16 traffic"; and
- s. 16 traffic that is not marked for retention by analysts Data that is acquired pursuant to part (c) of CSE's mandate is retained in accordance with OPS-1-11, section 2.9.[24]

It is not uncommon that the subjects of s. 16 warrants

CSE indicated that any person, including who met the definition of Canadian found at ss. 16(1)(b)(i) and (ii) of the *CSIS Act*, could not be targeted under a s. 16 warrant.

[24] OPS 1-11, *Retention Schedule for SIGINT Data*, dated October 31, 2007.

CSE advised that individuals targeted as a result of s. 16 general intercept and search warrants

Subsequent to the Mactavish decision, CSIS (which generally targets the s. 16 entities and forwards the information to CSE must now be satisfied that the named targets are not Canadians.

In the course of s. 16 activities, CSE may become aware that is a Canadian, as per s.16 of the *CSIS Act*. This is based on CSE's target knowledge and incidental information, including with Canadian status will fall into two categories:

1. those that are of FI interest, who will be identified as *Vanweenans*[26]

2. those that are not of FI interest, who will not be identified as *Vanweenans* and incidental collection on these targets will not be monitored

The interviews conducted with analysts who worked on the warrants under review indicated that most

[26] At para. 29 of the Mactavish decision, Mactavish J. explained "*Vanweenans*": "The practice of this court has been to require the Service to include in warrant applications a list of all those [...] known to the Service whose communications may be incidentally intercepted in the exercise of the powers granted by the warrant. These [...] are known colloquially as "*Vanweenans*", from the decision of the Supreme Court of Canada in *R. v. Vanweenan*, (1988) 2 S.C.R. 148."

The analysts interviewed also advised us that if a piece of traffic appears to be that of (which analysts can determine because of their familiarity with the target) and the information is of FI value, the CSE report will parse the information only from the foreign subject matter perspective

B) MINISTERIAL REQUIREMENTS

Finding no. 3: Ministerial Requirements

Based on the information reviewed and the interviews conducted, CSE's activities conducted under part (c) of its mandate in providing assistance to CSIS under s. 16 of the *CSIS Act* complied with ministerial requirements.

The 1987 Tri-Ministerial MoU

While the Tri-Ministerial MoU has been superseded by the 2008 process change letter, CSE advised that much of its policy content relies on the MoU, and that the content of the MoU has not been widely affected by the process change letter. CSE's policies and procedures related to s. 16 assistance still reflect the requirement under section 22(1) of the 1987 MoU that states, "Prior to disclosure to the requesting Minister, and/or his designee, information or intelligence, the nature of which falls within the mandate of the Communications Security Establishment, shall not be disseminated beyond Canada except by the Establishment" (this would include cryptologic information).

Since the process letter does not contain the same detailed content, processes, roles and responsibilities as was contained in the Tri-Ministerial MoU, the Commissioner's office was advised that continues to look to the Tri-Ministerial MoU as an important document to understand the intent and foundational principles of the s. 16 program. CSE deems that its role in the s. 16 process has not fundamentally changed as a result of the new s.16 process adopted in 2008, as CSE still acts as the agent of CSIS in the processing of intercepts obtained from warrants authorized by the Federal Court, and as the requesting minister's agent in the dissemination of intelligence obtained from these intercepts. In doing so, CSE is acting under part (c) of its mandate and is guided, not only by the conditions of the warrant, but also by its own policies such as OPS-4-1, *Operational Procedures for Assistance to Law Enforcement and Security Agencies under Part (c) of CSE's Mandate* and OPS-4-3, *Procedures Related to the Section 16 Program.*

Recommendation no. 1: Discussions to Formalize New Process

As a result of the elimination of the Tri-Ministerial MoU of 1987 and its replacement with the new process adopted in 2008 for the s.16 program, CSE should initiate discussions with CSIS and any other related parties in order 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, and then ensure that all references to the 1987 Tri-Ministerial Memorandum of Understanding in existing CSE policies and procedures be removed.

Recommendation no.2: CSE approval process

CSE should ensure all policies related to the section 16 program and the assistance it provides CSIS are consistent with and reflect the new approval process.

CSE-CSIS s. 16 MoU

Section 3, paragraph 3.3 of the CSIS-CSE MoU of 1990 indicates that

> Each party shall comply with any policies, procedures or guidelines that the other may make for the handling of intelligence provided by it. The parties are free to propose alternative procedures pursuant to their own policies and approvals to suit the circumstances of a particular case. If agreed to by both parties, such alternative procedures will be implemented as specified.

CSE advised that CSIS has provided specific guidance to CSE on three issues:

1. Handling of solicitor-client material: The CSE Director SPR issued an email July 19, 2010, which indicated that if CSE wished to retain or report on solicitor-client communications containing FI, CSIS must be advised first. CSIS must then seek the permission of the Federal Court to use this information. The Director noted that the reporting of FI was to be delayed until such time as CSIS obtained the permission from the Court. However, as the volume of reports from any solicitor-client communications was low, any delays would be insignificant. These guidelines have been incorporated into CSE's OPS-1 policy, section 3.8.

   In addition, CSE posts information about the reporting and retention of information received from solicitor-client communications