

Communications Security  
Establishment Commissioner

The Honourable Charles D. Gonthier, Q.C.



Commissaire du Centre de la  
sécurité des télécommunications

L'honorable Charles D. Gonthier, c.r.

CSE / CST  
Chief's Office / Bureau du chef  
AVR 03 2007  
File / Dossier CCM #07-00929

**TOP SECRET/COMINT/CEO**  
(with attachment)  
30 March 2007

The Honourable Gordon J. O'Connor, PC, MP  
Minister of National Defence  
101 Colonel By Drive  
Ottawa, Ontario  
K1A 0K2

Dear Mr. O'Connor:

The purpose of this letter is to advise you of the results of a review of the lawfulness of the activities of both the CSE client relations officers, called CROs, and the Operational Policy Section, known as D2, as they relate to the request for and release of Canadian identities suppressed in CSE foreign intelligence reports made available to Government of Canada clients. The review was undertaken under my general authority articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act (NDA)*.

In brief, the review concluded that the activities of the CROs and D2 in the release of Canadian identities were in compliance with the law and generally with CSE's related policies, although a number of inconsistencies were identified in the processes of requesting and releasing identities.

By way of background, the CRO programme was created by CSE in 1985 to facilitate the provision of foreign intelligence reports based on signals intelligence to officials in government departments. While there are several elements within the responsibilities of the CROs, this review focused on the role they play in the release

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

of Canadian identities (idents) in CSE foreign intelligence reports. It is CSE policy to suppress information that could identify a Canadian person or corporation (also referred to as Canadian identity information), or U.S./U.K./Australian/New Zealand persons and corporations in accordance with respective Second Party policies.<sup>1</sup> For example, where a Canadian is mentioned by name, the name is replaced by a generic reference such as "a Canadian businessman." If a client has both the authority and the need to know the name, he/she must make a formal request and provide justification. Since 1988, requests for release of idents have been centralized in D2. Over the past decade, the trend has been increasingly to direct secure electronic communication with D2, and access to the CSE report database known as [REDACTED]. However, CROs continue to be involved in ident requests, particularly from senior clients who do not have electronic access, notably in Foreign Affairs and International Trade Canada (DFAIT).

This review examined the roles of both the CROs and D2 in releasing Canadian identity information to Canadian clients and to Second Parties. Over a six month period, requests for suppressed information and the releases of that information were examined in detail to ensure compliance with law and policy. Interviews were also conducted with six CROs, two managers who co-ordinate the activities of the CROs reporting to them, and the manager of D2.

The review identified areas where I believe that both policy and practice can be improved to enhance the protection of privacy. In particular, I have made recommendations regarding: i) replacing a missing MOU between CSE and DFAIT; ii) where practical, expanding training of clients who make requests for the release of such information; iii) establish, where feasible, of more secure, electronic access by clients to D2 as a means of reducing inconsistencies and enhancing control over the ident release process; iv) re-examining its processes for releasing and accounting for multiple releases within a client department or agency; and v) examining the release of idents under the authority of the *Privacy Act* and amending the Request for Release of Suppressed Information form to include the appropriate section of the *Privacy Act* under which the release is authorized to be received by the requesting agency. With respect to recommendation i) above, I was pleased to learn that CSE has already begun the process to develop a new MOU.

The review also identified two areas that presented concerns during the period of review but that are currently being addressed by CSE. These areas are: i) training for personnel in the Operational Policy Section who are responsible for authorizing the release of suppressed information; and ii) records management, which has been a recurring theme of OCSEC recommendations.

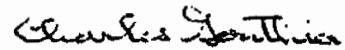
---

<sup>1</sup> Second Party refers to CSE's SIGINT partners in the U.S. (NSA), the U.K. (GCHQ), Australia (DSD) and New Zealand (GCSB).

As is my practice, I have provided officials at CSE an opportunity to review and comment on this report, prior to finalizing and forwarding it to you. I will continue to monitor the issues raised.

Please let me now if you have any questions or comments.

Yours sincerely,



Charles D. Gonthier

c.c. Mr. John Adams, Chief, CSE  
Ms. Margaret Bloodworth, National Security Advisor, PCO  
Mr. Ward Elcock, Deputy Minister, National Defence

**TOP SECRET/COMINT/CEO**

**Role of the CSE's Client Relations Officers  
and the Operational Policy Section (D2) in the  
Release of Canadian Identities**

**30 March 2007**

## **I. AUTHORITY**

This report was prepared on behalf of the Communications Security Establishment (CSE) Commissioner under his general authority articulated in paragraph 273.63(2)(a) of the *National Defence Act (NDA)*<sup>1</sup>.

## **II. PERIOD OF REVIEW**

The period of review is from 01 January to 30 June, 2005.

## **III. OBJECTIVES**

The purpose of this review, pursuant to paragraph 273.64(1)(a) of the *NDA*, is to assess the lawfulness of the activities of both the CSE Client Relations Officers (CROs) and the Operational Policy Section (D2), as they relate to the request and release of Canadian identities suppressed in CSE foreign intelligence reports made available to Government of Canada clients.

The initial objectives of this review were to:

1. identify and describe the origin, mandate and the scope of activities of the CROs;
2. identify and examine authorities that govern CROs' activities;
3. examine the CROs' role in releasing Canadian identities or information about Canadians to CSE clients;
4. examine a sample of releases to clients, including second parties<sup>2</sup> to ensure compliance with the law and with CSE policy; and
5. examine, review and report on any other issue that may arise during the course of this review and that may impact on CSE's ability to conduct its activities lawfully and safeguard the privacy of Canadians. We will inform CSE of our intention to examine "any other issue that may arise"; and

Subsequently, as described in our letter to Director, Corporate and Operational Policy dated 14 February, 2006, the scope of this review, in particular objective 3, was broadened to incorporate the role of the Operational Policy Section (D2) and include requests for Canadian identities from second parties.

---

<sup>1</sup> R.S.C. 1985, c. N-5.

<sup>2</sup> Second party countries are the CSE's partner SIGINT agencies in the United Kingdom (GCHQ), the United States (NSA), Australia (DSD) and New Zealand (GCSB).

#### IV. METHODOLOGY

Applicable documentation was examined, as noted above, as well as any records and files deemed relevant to the activities of the CROs. A sample of requests for suppressed information (Canadian identities) and the releases of that information were examined in detail to ensure compliance with law and policy. Interviews were conducted with six CROs and two managers who co-ordinate the activities of the CROs reporting to them. Toward the end of the review process and prior to forwarding the draft report to CSE for comment as to factual accuracy, a meeting was held at CSE, to present a summary of findings.

#### V. REVIEW FINDINGS

##### **Origin, Mandate and Scope of Activities of the Client Relations Officers (CROs) and the Operational Policy Section (D2)**

CSE has provided foreign intelligence reports based on signals intelligence (SIGINT) to officials in government departments since its formal establishment in 1946. Reports were delivered by hand. In 1985, the client relations officer (CRO) programme was created and the CROs began providing reports to clients, though reports continued to be delivered by hand from CSE to some clients. At that time, there were three primary clients: the Department of External Affairs (now called Foreign Affairs and International Trade Canada - DFAIT), the Privy Council Office (PCO) and the Department of National Defence (DND). CSE negotiated space in the client departments for the CROs who moved "on-site". Throughout the 1990s, the client base expanded to include many other departments and agencies such as CSIS, RCMP, Industry Canada, Agriculture, Fisheries & Oceans, and Finance.

In addition to providing intelligence reports and explaining to individual clients and potential clients the role of CSE and SIGINT, CROs receive feedback from clients about CSE reporting and assist in determining client needs based on Government of Canada intelligence priorities.

The CROs play a role in the release of Canadian identities (idents) that have been suppressed but referenced in generic terms in CSE's foreign intelligence reports. CSE's Operational Policy section, D2, is the authority for releasing idents (OPS-1-1, 2.4).

As a result of the increase in the number of both clients and CROs, a small staff was required to provide administrative support. Early in 2002, there was a minor re-organization that resulted in supervision of the CROs being transferred to three SIGINT managers, each becoming responsible for certain CROs.

In mid-1990s, the CROs were also becoming involved in what are referred to as "action-on" cases, for example, where information from CSE reports is worked into a client's departmental note or report. The requester, with the help of the CRO and D2 would consult to "sanitize" the CSE information, that is, ensure that the source(s) and method(s) used to obtain the information

was not exposed (OPS-5-9, "End Product Sanitization/Action-on Procedures"). The resulting note or report might still be classified but would no longer have to be handled through COMINT channels, thus allowing a broader distribution and facilitating the action a client was contemplating taking on the basis of the information. D2 was, and remains, the responsibility centre for the "sanitization" of reports. If a client wishes to use CSE information in a departmental note, the CROs will work with clients and then submit the "sanitized" information to D2 for approval. If a report involves Second Party information, D2 will seek appropriate approval, i.e. from the relevant Second Party.

During the period of review, there were 31 client departments/agencies of the federal government receiving CSE reports. These clients were served by 15 CROs with the largest concentration being at DFAIT where there are four CSE CROs as well as six DFAIT CROs. The unique situation at DFAIT results from the large number of individual clients within the department and from the fact that the vast majority of those clients do not have direct, secure electronic access to CSE, as compared to the individual clients at CSIS for example, who do have electronic access. Some of the CROs serve multiple departments, especially for departments where the demand for CSE reporting is not as great or as constant.

There has been a notable trend over the past decade. The role of the CROs has become more focused on key senior clients (e.g. Ministers, Deputy Ministers and Assistant Deputy Ministers), with lower-level clients increasingly using secure computer communication with CSE and access to its foreign intelligence reporting. CSE places its reports in a database known as [REDACTED] which can be accessed by a broad but select number of CSE clients who have been cleared for access to the secure government computer network called MANDRAKE. [REDACTED] is used primarily by policy and intelligence analysts in key security and intelligence departments and agencies.

The majority of ident requests are now made via email directly to D2. This is largely because of the development of the secure electronic computer system (MANDRAKE) and CSE's drive to provide improved service to its clients<sup>3</sup>; CSIS is the primary example, as briefly noted above. However, DFAIT and PCO still largely work with the CROs. At DFAIT, the CROs have a prominent role in serving the large number of individual clients, many of whom hold more senior positions. There are some cases where [REDACTED] (OPS-1-1, 4.2, 5.2 – 5.4). CROs receiving idents from D2 via [REDACTED] (i.e. not MANDRAKE) delete all related e-mails after the ident has been provided to the client. As per policy prevailing during the period of review, hardcopy forms were kept (see below, subsection on "Retention and Storage").

Many senior clients such as ministers, deputy ministers and directors-general do not use or do not have access to electronic foreign intelligence reports. Not all client departments or agencies

<sup>3</sup> The CSE 2005 Vision document, issued in 2000, sets out direct access by clients to CSE databases as a priority. As analysis of the vision proceeded, we were informed that unforeseen difficulties arose that did not make achieving the objectives possible. Pursuant to a request for the document, an initial search of the CSE intranet failed to retrieve a copy, however, a hardcopy version was subsequently obtained from CSE records and provided to OCSEC following the OCSEC briefing of the findings and recommendations of this review.

are served by the MANDRAKE network. Therefore, much of the CRO's activity focuses on these particular senior clients. Reports will be individually provided to senior clients.

A feedback system was developed to help guide report production for servicing clients. A significant part of the success of the CRO programme is attributed by CSE officials to the direct and tailored access to CSE intelligence that is provided to individual senior clients.

#### **Authorities and Guiding Documents for CROs and the Operational Policy Section (D2)**

CROs and staff of D2 who deal with requests for the identity of a Canadian in CSE reporting are guided by the following policies, all of which flow from the *National Defence Act* which states that CSE's foreign intelligence collection and information technology security (ITS) activities "shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information" (273.64(2) of the *NDA*):

- OPS-1 ("Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities" dated 20 June 2002);
- OPS-1-1 ("Procedures for the Release of Suppressed Information from SIGINT Reports" dated 11 February 2003);
- OPS-1-7 ("SIGINT Naming Procedures" dated 15 September 2004); and

The above-noted policies were those in effect during the period of review. They have since been updated.

In addition, the Ministerial Directive on Privacy of Canadians, dated June 19, 2001, sets out ministerial expectations for CSE in protecting privacy while carrying out its mandate.

#### **The Role of the CROs and D2 in the Request and Release of Suppressed Information**

CSE foreign intelligence reports that are distributed to client departments and agencies and that contain personal information about Canadians or citizens of Second Party countries, have the identifying information suppressed. For example, where a Canadian was mentioned by name, the name would be replaced by a generic reference such as "a Canadian businessman". If a client has both the authority and the need to know the name, they must make a formal request and provide justification (explained in detail below). Since 1988, requests for release of Canadian identities (idents) have been centralized in the Operational Policy section (D2). In recent years, the nature of idents has also changed. For example, since September 11, 2001, the value of analyzing metadata (data about data) has increased, with certain metadata identifying Canadians, for example telephone numbers and IP addresses.



CROs provide advice to their clients with respect to idents suppressed in CSE reporting. When an individual client requests the release of suppressed information about a Canadian that was contained in a CSE-generated report, the CRO may, when the client does not have direct communication to CSE/D2, "request the information on behalf of the client following a meeting" (OPS-1-1, 5.2). The "Request for Release of Suppressed Information" form (see appendix "A") must be completed, which includes providing the justification for the request. It is then forwarded to D2. In certain cases, a CRO may request the information in advance of a meeting with a client (OPS-1-1, 5.2 to 5.5 "Advance Release"), anticipating such a request because of the CRO's familiarity with that particular client. Most often, advance releases involve senior clients, for example Deputy Ministers. Advance release may also be prompted by emergency situations or situations where prior access to the client is difficult, for example located in another part of the city or because the client's schedule does not permit frequent meetings (OPS-1-1, 5.2).

As previously stated, the largest number of CROs serving one client department is situated within the Department of Foreign Affairs and International Trade (DFAIT). The reason for this unique situation is that the Department decided it preferred to use the CROs rather than electronic service. Therefore, only 15 of approximately 300 individual clients in DFAIT have direct electronic access to CSE via the MANDRAKE system and therefore most requests for the release of suppressed information are made through the CROs. Of the ten CROs, six are DFAIT employees and the remaining four are from CSE. This includes the CRO Unit Head who is a DFAIT employee but was formerly an employee of CSE. We were informed that an MOU exists specifically to address this special arrangement. However, when we requested to see the MOU, despite a concerted effort over time, the document could not be located, either within CSE or DFAIT. This is a concern to us.

**Recommendation #1:** If the Memorandum of Understanding between DFAIT and CSE cannot be located, it is recommended that a replacement MOU be prepared.

The importance of a comprehensive and efficient information management system is difficult to overstate. Information management has been a recurring theme in OCSEC recommendations for the past six years.<sup>4</sup> CSE responded most recently to OCSEC that a hard copy file retention system for operations and tracking is in place within SIGINT, and that implementation of an electronic IM system is set for completion in fiscal year 2007-2008 (see CSE response to OCSEC recommendation 1 in the report "CSE Support to Law Enforcement: RCMP – Phase II" dated 16 June, 2006). Among other purposes, proper information management is essential for ensuring CSE's own accountability and compliance with its authorities.

<sup>4</sup> See: "A Study of the EPR Process – Phase II: Handling Information About Canadians" dated 6 April, 2001; IRRELEVANT dated 13 November, 2002; "ITS Activities Pursuant to MAs" dated 20 May, 2003; "Review" dated 1 June, 2004; "A Study of the Collection Program" dated 15 March, 2005; "External Review of CSE Information Technology Security Activities Conducted Under MA" dated 29 March, 2006; "CSE Support to Law Enforcement: RCMP (Phase II)" dated 16 June, 2006; "Review of CSE's Activities Conducted Under the Industry Canada MA" dated 18 December, 2006.

---

**Observation #1:** We encourage CSE to continue on a priority basis the implementation of these records management systems for both hardcopy and electronic documents.

We were informed that CROs are generally selected for their experience and knowledge of SIGINT processes and reporting, as well as for knowledge of policy. There may not be a competition, particularly if an individual is judged suitable for such a position and is willing to become a CRO. One of the managers indicated that individuals who are selected are still interviewed by a board. CROs are assigned standard goals to achieve and are evaluated by their respective CRO manager, based on meeting client needs and adherence to policy. A statement of qualifications for CRO Unit Heads which lists formal requirements, experience and personal suitability requirements was provided at the time of the interviews but a statement of qualifications for CROs was not, though one was subsequently provided, following the briefing to CSE on the findings and recommendations of this review.

Part of the examination of the role of the CROs involved inquiring what training was received, especially as regards the release of Canadian identities suppressed from CSE reporting. Interviews were conducted with two CRO managers and five CROs whose experience ranged from 6 to 20 years.

Subsequent to being selected, a new CRO receives training from Operational Policy (D2), the section that manages requests for and releases of suppressed information (i.e. Canadian identities) in CSE reporting. Training consists of familiarization with all relevant policies regarding identities, suppression, request requirements, sanitization and "action-on". We were also informed that training occurs on the [REDACTED] database, client requirements and the SIGINT production areas (i.e. the writing of the foreign intelligence reports that are entered into [REDACTED]).

Training is also provided by D2 to the principal clients who have direct access to CSE for email and [REDACTED] (CSE reports), via MANDRAKE, as stated above. CSIS and PCO analysts receive a half-day presentation by a D2 staff member. We were provided the PowerPoint presentation and attended one of the sessions given at PCO.

#### **Examination of Releases of Suppressed Information**

Under paragraph 273.64(2)(b) of the *NDA*, CSE's foreign intelligence collection activities "shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information." Three CSE policies provide guidance in this area (as cited above in the section on "Authorities and Guiding Documents"). Dates are given for the version of the policy in effect for the period of review:

- OPS-1, "Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities", dated 20 June, 2002: this policy sets out basic principles and provides overall guidance on how CSE is to protect the privacy of Canadians in the use and retention of intercepted information;
- OPS-1-1, "Procedures for the Release of Suppressed Information from SIGINT Reports", dated 11 February, 2003: this policy provides direction to the staffs of CSE and the Canadian Forces Information Operations Group (CFIOG) involved in requesting, releasing and storing information suppressed from SIGINT reports to ensure compliance with the *NDA*, the Ministerial Directive on Privacy of Canadians, OPS-1 and second party policies; and
- OPS-1-7, "SIGINT Naming Procedures", dated 15 September, 2004: this policy sets out specific procedures for protecting the privacy of Canadian persons, corporations and organizations in SIGINT reports.

When reviewing the "Request for Release of Suppressed Information" forms, we expected that:

- requests would comply with three sections of OPS-1: 6.9 (setting out the requirements of the requester to provide justifying information, and requiring the release authority to ensure the request is consistent with the criteria set out); 6.10 (appropriate authorizations to release the suppressed information); and 7 (retention and storage of private communications or information about Canadians);
- the conditions specified in OPS-1-1, 3.3 (conditions governing the release of suppressed information) would be met and also that the information specified in sections 3.4, 3.5 and 3.6 would be provided (information required for the release, rationale for the request, and any action to be taken on the basis of the information);
- the process for release of suppressed information, as per section 4.1 of OPS-1-1 would be followed (process for releasing suppressed information).

We asked to see the total number of requests for releases of suppressed information during the period under review (January to June, 2005). We were informed that there were 203 requests from Government of Canada clients, involving the release of [REDACTED] Canadian identities (some requests involve more than one identity).<sup>5</sup> [RELEVANT]

[RELEVANT]

[RELEVANT]

These exemptions must be approved by the Director General Intelligence or the Deputy Chief SIGINT and the Director General, Policy and Communications. An additional eight requests came from Second Parties (also described

<sup>5</sup> A total figure of [REDACTED] was provided initially, but subsequent to another verification by CSE a revised total was provided.

below, in subsection on "Requests Involving Second Parties"). More than half the requests of 203) were from CSIS while 20% (43 of 203) were from DFAIT. [REDACTED]

In examining the release request forms we found that the majority met our expectations and fulfilled the requirements set out in CSE policies. There were, however, inconsistencies identified regarding some requests and releases.

There were instances where the same, or similar, inconsistencies appeared. We pursued these with the Manager of D2 and have included them in our analysis, accompanied by a recommendation, where appropriate. The following paragraphs describe the nature of the inconsistencies, and any implications for compliance or for the protection of the privacy of Canadians.

#### Request for Release of Suppressed Information Form

The Request for Release form requires, apart from the basic client information and CSE report reference number, a response from the requester to four questions:

- i) section F.1 - why the information is required (checking off one or more of 13 categories);
- ii) section F.2 - if there is an actual or potential violation of a Canadian law, cite the law;
- iii) section F.3 - how the information requested relates to the client's operating program or to the activity of the department or agency;
- iv) section G - is any action anticipated, based on the information.

The requirements for client information and the form itself were amended subsequent to recommendations from a 2000/2001 OCSEC review of CSE End Product Reports (EPRs) production and process.<sup>6</sup> The requirements as they are set out in the release request forms we examined, and as currently stated in policy, remain valid.

We noted that several requests, mostly from DFAIT or involving a diplomatic advisor to the Prime Minister, had inappropriate rationales checked off in section F.1 of the form. When an explanation is provided of how the information being requested relates to an operating program or activity of the requester's department (section F.3 of the form), it should be reconcilable with

<sup>6</sup> "A Study of the EPR Process – Phase III: An Analysis of EPR Production and Safeguards", 6 April, 2001. Recommendations included: i) CSE must update its release criteria used to support requests for the release of Canadian names/identities; ii) CSE must ensure that ... a client must provide a clear and independent rationale to justify each request – one which can be linked to the operating program of the client department ...; iii) CSE should require clients to provide a clear indication of the intended use of the released Canadian information...

the rationale checked off in section F.1. In a number of cases, this could not be done. We discussed these examples with the Manager of D2, who agreed with us in most instances. In those instances where the Manager did not agree, we generally accepted the explanations. In one example, the explanation in F.3 stated that a senior advisor at PCO required the Canadian identities for a briefing about [REDACTED]

[REDACTED] The rationale checked off in F.1 was [REDACTED]

[REDACTED] which is more for technical purposes and cannot be reconciled with the explanation. In another example, three individual clients in DFAIT were making the same request but the two rationales checked off (in F.1) were not appropriate for the explanation provided in F.3. The Manager of D2 agreed with this observation.

Section F.2 of the Release form states that "(i)f the request relates to a potential or actual violation of a Canadian law, please cite the law." There were two inconsistencies of note with this section. The first concerns [REDACTED] ident release request forms (almost 10% of the total), all from within CSE ([REDACTED] Group; three individuals, though the majority of requests were from one person in particular). Section 273.64 of the *NDA* (CSE mandate) was cited in response to this question, which is inappropriate in this context. The manager of D2 agreed. The CSE mandate provisions cannot be violated in the context of a request for a Canadian identity. The analysts may have been thinking of their authority to make the request, as opposed to what law may be violated by the subject of the report which contained suppressed Canadian identity information. This situation suggests a lack either of a careful reading of the form and what it is asking for, or a lack of understanding of the *NDA*. In either case, it leads to questions about the training and guidance provided to the CSE analysts making the release requests. While there is no issue of non-compliance or lack of protection of the privacy of Canadians in this situation per se, the concern is in the confusion about what is required.

The second inconsistency in this section relates to what would be an expected link between question F.1 ("Rationale for Request") and F.2 (cite which law if there is any potential or actual violation of a law). [REDACTED] forms (approximately 5% of the total) indicated that the rationale in F.1 concerned [REDACTED], or [REDACTED]

[REDACTED] but did not cite any law in F.2 which would be expected for these particular rationales. The issue here relates directly to the protection of the privacy of Canadians and that the release of a Canadian identity should only occur in those instances where the client demonstrates a justifiable need to know that information. The policy in this case is adequate and clear. Section 3.5 of OPS-1-1 states that the client "must be explicit regarding the requirement for suppressed information." This situation suggests that either the clients require more familiarization or training on the requirements to request the release of suppressed information, or the CSE officials (CROs or in D2) processing the requests should return to the client to require the additional information.

Inconsistency also arises in section F.3 which requires the client to "(e)xplain how this information relates directly to an operating program or activity of your department." Most clients in the Release forms we reviewed cite the law governing their department or agency. However,

for certain clients from within CSE (e.g. [REDACTED] Group), the activity described includes a specific, foreign country target while other clients within the same group, where the described activity of the client is virtually the same, a specific target is not cited. Citing a specific target for an internal CSE request may confirm two things. First, that it is indeed a foreign target, consistent with CSE's foreign intelligence collection mandate, and second, that it could be linked back to the Foreign Intelligence Priorities and the Government of Canada Intelligence Requirements. Without the specific target named, the description of the activity still does demonstrate the use to which the information is being applied and that it falls within CSE's mandated activities. Nonetheless, the inconsistency about naming, or not, a specific, foreign target raises the questions "Why?" and "Is it required?"

In a request from an individual client at CSIS, the explanation provided in F.3 [REDACTED] Accepting this as an oversight, since a [REDACTED] we nonetheless verified in the original report and found that [REDACTED] and that therefore there was no need for the information to have been suppressed in the first place. This should have been evident to the release authority in D2. This same official in D2, however, in another request by the same client at CSIS, but involving several Canadian identities, appropriately advised the client that each requested identity must be linked to the client's authority to have the information and a justifiable need to know it.

We observed an additional inconsistency with respect to a comment in section H of the Release Request form, to the effect that the information may only be used for the purposes described in Section G of the form "AND must be treated as TOP SECRET//COMINT//CEO." Other requests that were similar, signed off by different release authorities, did not have such caveats. This point addresses the protection of CSE information, which is especially important when it involves information about Canadians. It also raises the question why a caveat is needed in one case and not in another similar one. Again, the inconsistency raised for us the question of training and awareness regarding the processing of requests for the release of suppressed information.

One of the requests noted that it was for [REDACTED]. It was not clear from the form whether the request [REDACTED] was providing telephone numbers to CSIS who then inquired as to the identities. We sought clarification from CSE/D2 and were informed that this was indeed an unusual request made in this way. Normally [REDACTED] the information (telephone numbers) [REDACTED] but, we were informed, possibly because the telephone numbers [REDACTED] and that therefore there was a SIGINT connection [REDACTED]. A CSE manager noted to the CSIS liaison officer at CSE that: "We haven't had this kind of request before, so we want you to know about it and when CSIS receives this information you'll know what the path was." The CSE manager also noted that they had filled in the Request for Release of Suppressed Information form so they could track the release of the [REDACTED] phone numbers; this, even though there was no indication the telephone numbers originated from a CSE end-product report.

During a meeting with the Manager of D2 to discuss questions we had about the client Request for Release of Suppressed Information forms, we appreciated the manager's frankness and the seriousness with which she approached the issues we raised. She acknowledged those areas that were not consistent with policy, indicating that she would look into them and if similar situations were still occurring how they might be corrected. The manager also pointed out certain steps that have been taken since the period of review to strengthen compliance with policy. For example, a new procedure has been implemented in which a release of a Canadian ident, authorized by a newer member of D2, will be reviewed by a more senior individual in the section. In certain instances that we raised, the manager's explanations clarified points and alleviated our concerns. In addition, since July, 2005 – that is, subsequent to the period of review – the D2 Manager conducts a once-monthly review of a random sample of ident releases to examine them for compliance with policy.

During the course of our review of these Release Request forms, a number of positive elements were also observed. In certain instances, the CSE release authority would go back to the requesting client who had made a very general statement in the form. The releasing official in D2 advised the client of the requirements for making a request.<sup>7</sup> We understand from the D2 manager that they do refuse requests or may advise that insufficient information has been provided. She noted that clients will often re-submit the request with additional information and the release is then authorized. D2 does not record these instances, and we do not see a need to do so.

We also observed that the direct link from CSIS analysts to D2 at CSE appears to facilitate more accurate and complete release request forms. The requests from CSIS that we reviewed were almost always complete and complied with CSE policy. We noted two instances where the CSE release authority advised the individual client on how to improve their requests. We examined these and noted that the basic information required from the client was supplied but that the additional advice offered by D2 was useful.

During a meeting with the Manager of D2 to review and discuss the inconsistencies that we had noted in the Release Request forms, it was observed that of the two major clients requesting ident releases (CSIS and DFAIT) inconsistencies were more likely to involve DFAIT. Looking at what may help to explain this, we examined factors that distinguish these two major clients from each other. One distinction, as already noted, is that CSIS analysts have direct, secure electronic access to CSE for making requests whereas most individual clients in DFAIT are served by CROs (though the one CRO at DFAIT who was interviewed had not received any requests for release of Canadian identities during the past year). Another distinction is that CSIS analysts are provided with a half-day training session from CSE/D2. DFAIT personnel do not receive this formal training, and it would be impractical for senior clients (e.g. ADMs, DMs) who are unlikely in any case to access reports electronically. There is also the point that clients who do have direct electronic access, including the Request for Release of Suppressed Information form, are reminded each time of the requirements for requesting a release. These distinctions suggest that where clients are given training by CSE/D2 and have direct, secure electronic access to CSE

<sup>7</sup> For example, report numbers [REDACTED] and [REDACTED]



to make requests, there appears to be a higher probability that the requests will fulfill the requirements of policy more consistently and comprehensively. This is positive for both compliance and protecting privacy. We suggest CSE examine this further.

**Observation #2:** Recognizing that steps have been taken since the period of review to strengthen compliance with policy for authorizing release of Idents, we encourage CSE to conduct more comprehensive training for those who are authorized to release Canadian identity information in D2, to ensure policy is consistently applied.

**Recommendation #2:** That, where practical, more comprehensive and frequent training for clients be conducted, referring to the model of what is done for CSIS and PCO analysts.

**Recommendation #3:** That, where feasible for other clients, CSE follow the model it has established for direct, secure electronic communication between CSIS analysts and CSE/D2 to make requests.

IRRELEVANT

#### **Direct Access Between Clients and CSE/D2**

As previously noted, certain clients have direct access to CSE, most notably CSIS. This includes direct access to the CSE end-product report database known as [REDACTED] as well as secure e-mail access to D2 for requesting the release of suppressed information contained in reports found on [REDACTED]. The secure email includes attachments such as the form for Request for Release of Suppressed Information. Both [REDACTED] and the secure email are accessed by clients through a secure Government of Canada communication system known as MANDRAKE that links various departments and agencies within the security and intelligence community. The CROs play a role in assisting clients to gain access to MANDRAKE and to determining information that is relevant to client needs that is available through the system.



### Multiple Releases of the Same Ident

One area of concern we identified relates to two individual clients in the same department requesting the release of the same suppressed information from a CSE report. Based on answers we received in interviews with the CROs and in responses from the manager of D2, there appear to be potential gaps with respect to consistency in applying the release criteria.

Once one individual client in a department or agency has requested an ident and it has been released, CSE policy (OPS-1-1, section 4.3) states that "that information may be disseminated to other staff in the same department as necessary, without the need to fill in an additional Request for Release of Suppressed Information form." The released information is then under the control of the client department or agency (OPS-1-1, 3.3) which is subject to the *Security of Information Act (SOIA)*<sup>8</sup>, the *Access to Information Act*<sup>9</sup> and the *Privacy Act*<sup>10</sup>. Therefore, client departments must ensure that if released suppressed information is provided to another individual, that individual must have a need to know it.

We were informed that in certain instances where a report and ident are particularly sensitive, not all individual clients within the department or agency who request the same suppressed information may receive it. For example, if a Director General in the Department of Foreign Affairs requests an ident that was already provided to an Assistant Deputy Minister, it does not hold that the DG will automatically receive it. If, however, they did receive it and a release request form is not required to be filled out, there is no hardcopy record of the request or justification; there would only be a verbal request, most likely involving a CRO. We were informed by the manager of D2 that if multiple forms requesting the same suppressed information are received, D2 accepts them and does not necessarily spend the time looking to see whether they were from the same department and that therefore, according to OPS-1-1, 4.3, the request forms subsequent to the first one were not necessary. This inconsistency in whether each request is or is not submitted on a request release form raises questions about the accuracy of the statistics. As stated, the released information is under the control of the requesting client department, where it is beyond the scope of the CSE Commissioner's mandate. Nonetheless, we believe this is an area that could be addressed at the CSE end, in the interests of being able to account for all clients who receive ident information.

**Recommendation #4:** That CSE re-examine its processes with respect to the release of the same ident to individual clients within the same department or agency, with the objectives of i) ensuring consistency of application; and ii) of accounting for each release, including multiple releases of the same ident, within a client department or agency and thus ensuring more accurate statistics.

<sup>8</sup> R.S.C. 1985, c. O-5.

<sup>9</sup> R.S.C. 1985, c. A-1.

<sup>10</sup> R.S.C. 1985, c. P-21.

---

### Requests Involving Second Parties

Also during the period of review, there were a total of eight requests from second parties, guided by OPS-1-1, sections 6.1 and 6.2 (involving the process for and handling of requests from second parties). There were [REDACTED] identities released and [REDACTED] denied ([REDACTED] to NSA and [REDACTED] to GCHQ). No issues of concern arose with respect to these requests and their conformance with policy.

### Advance Releases

Advance release of a Canadian identity, that is releasing the ident prior to the receipt of a formal request from a client, invariably involves a Client Relations Officer. Procedures are set out in CSE policy OPS-1-1, 5.2-5.5. In certain circumstances, a CRO may request suppressed information from D2 in advance of a meeting with a client, in anticipation that the client will request the release of suppressed information in a CSE report. Based on experience, the CRO is familiar with the needs of individual clients and is in a position to anticipate such a request. This occurs primarily when servicing senior clients such as Assistant Deputy Ministers, Deputy Ministers or Ministers, or when access to the client is difficult. It can also occur for emergencies or urgent situations. The CRO is accountable for the release of the information. If the client does make the request for the release and the rationale satisfies the CRO, then it will be released. Subsequent to releasing the ident, the CRO will complete a form for Request for Release of Suppressed Information and forward it to D2.

During the period of review, there were [REDACTED] requests for advance releases, all originating from CROs at the Department of Foreign Affairs. We requested, and received, all related information and explanations with respect to these advance requests, including the follow-up forms which had been filled out and submitted, as required by policy. There were no issues of concern.

### Inadvertent Disclosure

Inadvertent disclosure of Canadian identity information, dealt with in section 4.2 of OPS-1-1, occurs when identifying information about a Canadian or person from a second party country is included in a report when it should have been suppressed and replaced by a generic description, according to policy (OPS-1-7 "SIGINT Naming Procedures"). We were informed by several interviewees that inadvertent disclosure is most likely to occur in second party reports. There are very few incidents like this that occur. Two of the CROs were interviewed independent of each other, and each noted that Canadian identities had appeared in a second party report. The CROs told us that they informed the originator and D2 as required by policy (OPS-1-1, section 4.2). The reports were withdrawn and then re-issued with the identity information suppressed.

---

Retention and Storage of Suppressed Information

CROs, who are involved in advising and releasing ident to clients, demonstrated during the interviews that they were fully aware of retention policy (OPS-1-1, 7.2 "Retention and Storage of Suppressed Information", dated 11 February, 2003) and practice. All the CROs interviewed informed us that e-mails from D2 containing the suppressed information requested by the client is deleted immediately after it has been provided to the client. D2 retains, for a minimum of [REDACTED] a soft copy (i.e. electronic) in the suppressed information repository to which only D2 staff, system administration staff and the original report writer have access. The CROs informed us that hardcopies of the Request form are kept for up to [REDACTED] subsequent to which they are destroyed (put in "burn bags" which are collected and burned). The manager of D2 explained and demonstrated how the suppressed information repository was used and maintained. We were satisfied that it performs as required; it remains the responsibility of the individuals using it and the managers to ensure that policy is applied appropriately.

Client retention of Canadian identities is also set out in CSE policy OPS-1-1, section 7.2. The version in effect at the time stated that a requester could retain a hard copy of the ident information in an approved container for a maximum of [REDACTED]

A previous recommendation by OCSEC ("Report on the Activities of CSE's [REDACTED] dated 22 June, 2005) stated that "CSE establish a mechanism to track and verify adherence to its policy requiring that clients retain hard copy forms with Canadian identities for a maximum of [REDACTED] and that soft copies be deleted from all e-mails." CSE accepted the recommendation, with modification, responding that the involvement of the CROs has been reduced and the responsibility of the clients to properly store the information has been re-inforced, "in accordance with Government of Canada policy on the protection of private information". CSE also noted that OPS-1-1 would be clarified to this effect. We note that the policy has since been amended and that the maximum [REDACTED] retention period has been dropped in favour of emphasizing that requesters "may retain hard/soft copy according to: classification markings and departmental procedures related to the handling of information about Canadians".

Disclosure and the Privacy Act

OPS-1-1 makes general reference to the *Privacy Act*. It is not, however, referred to in the Request for Release of Suppressed Information form. A previous OCSEC review<sup>11</sup> raised the issue of disclosure of Canadian identities and what section of the *Privacy Act* would apply. Reviewers at the time were advised that in most instances, disclosure of ident was made under the authority of 8(2)(a) as foreign intelligence (FI) and as a consistent use. As the report observed, 8(2)(a) may be appropriate for disclosing to DFAIT which has a foreign intelligence mandate and therefore is consistent in requesting personal information retained and used by CSE as essential to foreign intelligence. However, in the case of a law enforcement or security

---

<sup>11</sup> "CSE Support to Law Enforcement: Royal Canadian Mounted Police, Phase II" dated 16 June, 2007.

agency, 8(2)(e) may be the more appropriate section under which to disclose the ident ("the request for information must come from an investigative body listed in the regulations of the *Privacy Act*").

IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT
IRRELEVANT	IRRELEVANT	IRRELEVANT	

**Recommendation #5:** That CSE examine the disclosure of idents under the *Privacy Act* with a view to amending the Request for Release of Suppressed Information form to include the section of the *Privacy Act* that is the appropriate authority.

## VI. CONCLUSIONS

The review of the activities of the CSE client relations officers (CROs) and the Operational Policy Section (D2) in the release of Canadian identities (suppressed information) to requesting clients found the activities to be in compliance with the law and generally with CSE's related policies. The expectations that we established in reviewing the Request for Release of Suppressed Information forms were generally met, though there were a number of inconsistencies identified with respect to client requests and CSE authorizations to release the suppressed information. These inconsistencies exposed areas where we believe that both policy and practice can be improved to enhance the protection of privacy. In particular, we have made recommendations regarding: i) the training of clients who make requests for the release of such information; ii) the establishment of more secure, electronic access by clients to CSE Operational Policy Section as a means of reducing errors and enhancing control over the ident release process; iii) the re-examination of its processes for releasing and accounting for multiple releases within a client department or agency; and iv) the examination of release of idents under the authority of the *Privacy Act* and amending the Request for Release of Suppressed Information form to include the appropriate section of the *Privacy Act* under which the release is authorized to be received by the requesting agency.

We also made observations in two areas that are currently being addressed by CSE but which for the period of review raised concerns. These areas were: training for personnel in the Operational Policy Section who are responsible for authorizing the release of suppressed information; and ii) records management, which has been a recurring theme of OCSEC recommendations.

---

<sup>12</sup> R.S.C. 1985, c. C-23.

---

### Summary of Recommendations

**Recommendation #1:** If the Memorandum of Understanding between DFAIT and CSE cannot be located, it is recommended that a replacement MOU be prepared.

**Recommendation #2:** That, where practical, more comprehensive and frequent training for clients be conducted, referring to the model of what is done for CSIS and PCO analysts.

**Recommendation #3:** That, where feasible for other clients, CSE follow the model it has established for direct, secure electronic communication between CSIS analysts and CSE/D2 to make requests.

**Recommendation #4:** That CSE re-examine its processes with respect to the release of the same ident to individual clients within the same department or agency, with the objectives of i) ensuring consistency of application; and ii) of accounting for each release, including multiple releases of the same ident, within a client department or agency and thus ensuring more accurate statistics.

**Recommendation #5:** That CSE examine the disclosure of ids under the *Privacy Act* with a view to amending the Request for Release of Suppressed Information form to include the section of the *Privacy Act* that is the appropriate authority.

**Appendix "A"**  
**Request for Release of Suppressed Information Form**

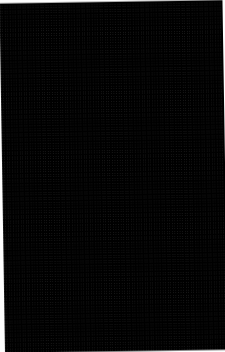
(when completed)

**TOP SECRET//COMINT//Canadian Eyes Only**

A. Requesting Client's Name	B. Client Title and Department
C. Report Serial Number	D. Date of Request
E. Information Requested	
F. Rationale for Request ( <i>please complete all three questions</i> )	
This information is required because it relates to (mark an 'X' in the appropriate space(s)):	
<div style="background-color: black; height: 150px; width: 100%;"></div>	
If the request relates to a potential or actual violation of a Canadian law, please cite the law.	
Explain how this information relates directly to an operating program or activity of your department.	
G. Please indicate what action, if any, is being contemplated based on this information. ( <i>Note that some actions require prior CSE approval.</i> )	
H. Suppressed Information	
Released by:	
Comments:	
This information is provided on the understanding that the requesting department requires this information to perform its lawful duties, and that this information will be handled in accordance with the <i>Access to Information Act</i> and the <i>Privacy Act</i> .	

---

**Appendix "B"**  
**CSE Personnel Interviewed**



Director, Corporate and Operational Policy  
Manager, Operational Policy Section  
Manager, External Review and Policy Compliance  
CRO Manager  
CRO Manager  
CRO for CSIS and the RCMP  
CRO for PCO and Special Events  
CRO for Foreign Affairs and International Trade Canada  
CRO for the Department of National Defence  
CRO for Agriculture Canada, PSEPC, Canadian Food Inspection Agency;  
formerly at Industry Canada