



# OPS-1-1

## Operational Procedures for the Release of Suppressed Information from SIGINT Reports

OPERATIONAL POLICY

Canada

---

## Table of Contents

---

1. Definitions.....	2
2. Introduction.....	4
3. Preparing Requests for Suppressed Information.....	8
4. Release of Suppressed Information Process .....	11
5. Silent Hour and Advance Release.....	13
6. Requests involving Second Parties .....	17
7. Retention and Storage of Suppressed Information .....	18
8. Request for Release of Suppressed Information Form .....	19
 ANNEX 1. Release Outside Canada of Canadian Identity Information Suppressed from SIGINT Reports .....	 21

---

## 1. Definitions

---

**1.1 Action-on** Action-on is any action, or decision to act, taken on the basis of COMINT information, which might jeopardize the COMINT source. Action-on usually involves a sanitization.

---

**1.2 Canadian** 'Canadian' refers to a

- a) Canadian citizen,
- b) A person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27, and who has not subsequently lost that status under that *Act*, or
- c) A corporation incorporated under an Act of Parliament or of the legislature of a province.

(*National Defence Act*, section 273.61).

For the purposes of this procedure, 'Canadian organizations' are also accorded the same protection as Canadian citizens and corporations.

A Canadian organization is an unincorporated association, such as a political party, a religious group, or an unincorporated business headquartered in Canada.

---

**1.3 Canadian Identity Information** Canadian identity information refers to information that may be used to identify a Canadian person, organization, or corporation, including, but not limited to, names, phone numbers, email addresses, IP addresses, and passport numbers.

---

**1.4 Second Party**

Second Party refers to CSEC's SIGINT counterparts and include: the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD), and New Zealand's Government Communications Security Bureau (GCSB).

---

**1.5 Suppressed Information**

Suppressed information is defined as information excluded from a SIGINT end-product report because it may reveal the identity of a Canadian or Allied entity. This information is stored in a limited-access database and is in most cases replaced in the report by a generic term.

Suppressed information includes, but is not limited to, personal identifiers such as names, passport information, [REDACTED] email addresses, phone numbers and IP addresses, [REDACTED]  
[REDACTED]

---

---

## 2. Introduction

---

- 2.1 Context** These procedures describe CSEC measures in place to protect the privacy of Canadians in the release of information suppressed from SIGINT reports in accordance with OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*.
- 
- 2.2 Objective** The objective of these procedures is to provide direction to CSEC and CFIOG staff involved in requesting, releasing and storing information suppressed from SIGINT reports to ensure compliance with:
- *National Defence Act*, Part V.1
  - *Ministerial Directive on Privacy of Canadians*
  - OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, and
  - Second Party policies.
- 
- 2.3 Application** These procedures apply to CSEC and CFIOG staff and any other parties who conduct activities under CSEC authorities, and who are involved in requesting, releasing and storing information suppressed from SIGINT reports.
- 
- 2.4 Authority for Release of Suppressed Information** CSEC's [REDACTED] is the authority for releasing information suppressed from SIGINT reports. This authority has been delegated in writing to the Operational Policy Section. Under certain circumstances as described in these procedures, this authority is delegated to OSOC or to Client Relations Officers (CROs).
- Note:** [REDACTED] remains the approval authority for requests to release suppressed information outside Canada, (see Annex 1 – *Release Outside Canada of Canadian Identity Information Suppressed from SIGINT reports*).
-

**2.5  
Audit/Review**

CSEC activities, including relevant policies and procedures, are subject to management monitoring (see OPS-1-8, *Operational Procedures for Policy Compliance Monitoring to Ensure Legal Compliance and the Protection of the Privacy of Canadians*), and to review by various government review bodies, including, but not limited to, the CSEC Commissioner and the Privacy Commissioner.

**2.6 Why do we  
Suppress  
Information  
from SIGINT  
Reports?**

Most information that may directly or indirectly identify a Canadian or a US, UK, Australian or New Zealand national is replaced in end product reporting with generic terms (for example, "a Canadian citizen" or "a US corporation"). Canadian identity information is suppressed in order to protect the privacy of Canadians as directed in CSEC legislation, the *Ministerial Directive on Privacy of Canadians* and *OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*. Such information may only be released according to these procedures.

US, UK, Australian and New Zealand national information is suppressed in compliance with SIGINT partner policies. See OPS-1-7 *Operational Procedures for Naming in SIGINT Reports* for details on suppressing Canadian and allied information.

Effective date: 28 September 2012

## 2.7 Accountability

This table indicates responsibilities in relation to these procedures.

Who	Responsibility
DG Policy and Communications	<ul style="list-style-type: none"> <li>• Approving these procedures</li> <li>• Applying these procedures</li> </ul>
General Counsel Directorate, Legal Services	<ul style="list-style-type: none"> <li>• Providing legal advice, when requested</li> <li>• Reviewing these procedures to ensure they comply with the law</li> </ul>
Operational Policy staff	<ul style="list-style-type: none"> <li>• Revising these procedures</li> <li>• Understanding and complying with these procedures</li> <li>• Answering questions regarding these procedures</li> </ul>
All CSEC and CFIOG staff who are involved in the release of suppressed information	<ul style="list-style-type: none"> <li>• Reading, understanding and complying with these procedures and any amendments to these procedures</li> </ul>
All CSEC and CFIOG managers who are involved in the release of suppressed information	<ul style="list-style-type: none"> <li>• Ensuring their staff have read and understood these procedures and any amendments to these procedures</li> </ul>

## 2.8 Enquiries

All questions related to these procedures should be directed to operational Managers, who in turn will contact Operational Policy staff (e-mail [REDACTED] when necessary.

---

**2.9 References**

- *National Defence Act*
  - *Privacy Act*
  - *Access to Information Act*
  - *Canadian Charter of Rights and Freedoms*
  - the most recent *Ministerial Directive on Privacy of Canadians*
  - OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
  - OPS-1-7, *Operational Procedures for Naming in SIGINT Reports*
  - OPS-1-8, *Operational Procedures for Policy Compliance Monitoring to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
  - OPS-2-1, *End Product Sanitization/Action-on Procedures*
- 

**2.10  
Amendments**

Situations may arise where amendments to these procedures may be required because of changing or unforeseen circumstances. All approved amendments will be announced to staff and will be posted on the Operational Policy website at [REDACTED]

---



---

### 3. Preparing Requests for Suppressed Information

---

#### 3.1 Who May Request Suppressed Information

The following COMINT-indoctrinated persons having appropriate rationale may request suppressed information:

- Government of Canada clients
  - CSEC staff
  - Second Party government personnel via SIGINT policy offices, and
  - CSEC Client Relations Officers (on behalf of GC clients).
- 

#### 3.2 Processing Requests for Release of Suppressed Information

Requests for suppressed information are to be submitted to CSEC's Operational Policy Section via secure email or secure fax, using the "Request for Release of Suppressed Information" form. Operational Policy staff release the information to the requester if the specific criteria described in these procedures are met. See Section 4 of this document for more information on the process. See Section 8 of this document for a copy of the form.

---

#### 3.3 Conditions Governing the Release of Suppressed Information

Suppressed information is released by the Operational Policy Section on the understanding that:

- the requester requires the information in the exercise of the mandate of the organization or department
  - the released information will be under the control of that organization or department, and
  - the requesting organization or department (in Canada) will handle the information in accordance with the *Access to Information Act* and the *Privacy Act*.
-

Effective date: 28 September 2012

**3.4 Information Required for Release of Suppressed Information**

A "Request for Release of Suppressed Information" form must be submitted to the Operational Policy Section. The form must contain the following information:

- Name, title and 'organization' of the requester (Sections A and B of the form)
- Serial number of the SIGINT report (Section C)
- Date of request (Section D)
- Information requested (Section E)
- Rationale for the request (Section F), and
- An indication of any follow-on action contemplated by the requester (Section G).

**3.5 Rationale for the Request: Section F of the Form**

The requester must be explicit regarding the requirement for suppressed information.

First, the requester must indicate that the information relates to at least one of the following criteria :

- capabilities/intentions/activities of a foreign person, state, organization or terrorist group relating to international affairs, defence or security

- [REDACTED]

- use for prevention/identification/investigation of a potential threat to the life or safety of an individual in Canada or abroad
- terrorist activity or threats to the security of Canada

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

Second, if the request is related to a possible violation of a Canadian law, the requester must cite the appropriate law.

Third, the requester must explain how the information relates directly to an operating program of his/her organization or department.

SECRET//SI

OPS-1-1

Effective date: 28 September 2012

---

**3.6 Action-on:  
Section G of the  
Form**

The requester must indicate in Section G of the form if any follow-on action is contemplated upon receipt of the suppressed information. With few exceptions, any such action will require the prior approval of CSEC's Operational Policy Section. For action-on rules and approval authorities, refer to OPS-2-1, *End Product Sanitization/Action-on Procedures*.

---

## 4. Release of Suppressed Information Process

### 4.1 Release of Suppressed Information Process

The following table describes the process for requesting and releasing suppressed information to Canadian organizations or departments. The process for Second Party requests is described in Annex 1.

Step	Who Does It	What Happens
1	Requester	Reads a SIGINT report and determines there is a requirement for information suppressed from the report.
2	Requester	Completes a "Request for Release of Suppressed Information" form. Sections A-F are mandatory; Section G is to be completed when applicable.
3	Requester	Submits, via secure email [REDACTED]@cse-cst.gc.ca) or secure fax, a completed copy of the form to CSEC's Operational Policy Section.
4	Operational Policy staff	Review the request and determine whether it: - relates directly to an operating program of the requester's department, and - meets one of the approved release criteria.
5	Operational Policy staff	If the request relates to a suppressed identity in a Second Party report or a US, UK, Australian or New Zealand identity in a CSEC report, Operational Policy staff follow the procedures described in Section 6.1 of this document.
6	Operational Policy staff	Add the suppressed information to Section H of the form and forward the completed form back to the requester via secure email or fax.
7	Operational Policy Section	Retains a soft copy of the form in an on-line folder for [REDACTED] and purges all other copies of the form from email folders.

---

**4.2 Inadvertent Disclosure of Suppressed Information**

In the event that suppressed information is released inadvertently (for example, by an analyst who authors a report containing suppressed information), the incident should be reported to the Operational Policy Section for follow-on action and accounting purposes.

---

**4.3 Release of Suppressed Information to Government of Canada Departments**

Once suppressed information is released to an individual in a GC government department or agency, that information may be disseminated to other staff in the same department without the need to fill in an additional “Request for Release of Suppressed Information” form.

---

**4.4 Classification of Released Suppressed Information**

Released suppressed information without any association to SIGINT does not require COMINT protection.

---

---

## 5. Silent Hour and Advance Release

---

### 5.1 Silent Hour Requests, Crises and CRO support

Requests for release of suppressed information outside of core business hours should be directed to CSEC's [REDACTED]. In urgent cases, [REDACTED] will use the call-in list to contact Operational Policy staff.

During crisis periods or to support CROs working extended hours [REDACTED] the Manager of Operational Policy may authorize [REDACTED] to act as Release Authority for suppressed information. [REDACTED] will process requests during the silent hours, and must provide the Operational Policy Section with copies of any requests actioned during the period, including completed "Request for Release of Suppressed Information" forms.

---

### 5.2 Advance Release

Requests for release of information from GC clients are often handled via CSEC CROs who request the information on behalf of the client [REDACTED]. However, there are circumstances where a CRO can request suppressed information in advance of a meeting with a client in anticipation of a request for the information by the client:

- when providing service to senior GC clients (Ministers, Deputy Ministers, [REDACTED])
  - in urgent situations (emergencies), or
  - in cases where access to the client is difficult (for example: the client is located in another part of the city, or his/her schedule does not permit frequent meetings).
-

Effective date: 28 September 2012

---

**5.3 Advance  
Release: CRO  
Responsibility**

When the Operational Policy Section provides CROs with suppressed information without having the opportunity to vet the rationale as is the case with advance release, the CRO is delegated responsibility for release and is accountable for the release of the information.

Prior to releasing the suppressed information to the client, the CRO must ensure that:

- conditions governing the release of suppressed information are understood
  - the client provides all the information required to complete the form
  - the rationale meets criteria for release of information and is consistent with the operating program of the client's department or agency, and
  - any action-on contemplated by the client is noted (Note requirement to consult with the Operational Policy Section for action-on requests).
-

Effective date: 28 September 2012

**5.4 Advance  
Release Process**

The attached table outlines the process for advance release of suppressed information.

Step	Who does it	Action											
1	CRO	In anticipation of a request from a client under the circumstances described in section 5.2 above, contacts the Operational Policy Section via phone or email, asking for advance release of suppressed information  <b>Note:</b> The CRO does not fill in a Request for Suppressed Information form at this time.											
2	Operational Policy staff	Provide the suppressed information to the CRO											
3	CRO	<ul style="list-style-type: none"> <li>Acts as Release Authority for the information</li> <li>Meets with the client</li> </ul>											
4	<table> <tr> <th>If the client...</th><th>And provides a rationale that...</th><th>Then the CRO...</th></tr> <tr> <td rowspan="2">Requests the suppressed information</td><td>Meets the approved criteria</td><td>Will release the suppressed information and will forward a completed form to the Operational Policy Section following the meeting.</td></tr> <tr> <td>Does <u>not</u> meet approved criteria</td><td>Will deny the request, inform the Operational Policy Section of the details via email following the meeting and will destroy the information.</td></tr> <tr> <td>Does not request the suppressed information</td><td>-</td><td>Notifies the Operational Policy Section and destroys the information.</td></tr> </table>		If the client...	And provides a rationale that...	Then the CRO...	Requests the suppressed information	Meets the approved criteria	Will release the suppressed information and will forward a completed form to the Operational Policy Section following the meeting.	Does <u>not</u> meet approved criteria	Will deny the request, inform the Operational Policy Section of the details via email following the meeting and will destroy the information.	Does not request the suppressed information	-	Notifies the Operational Policy Section and destroys the information.
If the client...	And provides a rationale that...	Then the CRO...											
Requests the suppressed information	Meets the approved criteria	Will release the suppressed information and will forward a completed form to the Operational Policy Section following the meeting.											
	Does <u>not</u> meet approved criteria	Will deny the request, inform the Operational Policy Section of the details via email following the meeting and will destroy the information.											
Does not request the suppressed information	-	Notifies the Operational Policy Section and destroys the information.											



SECRET//SI

OPS-1-1

Effective date: 28 September 2012

---

**5.5 Review of  
Advance  
Release forms**

Operational Policy staff will review all forms submitted under the Advance Release process after the fact. The Operational Policy Section reserves the right to refuse requests for advance release of suppressed information, such as in cases where previous rationales were weak, incomplete or lacking in detail.

---

## 6. Requests involving Second Parties

### 6.1 Requests Involving Second Party Reports or Allied Identities

This table describes the process the Operational Policy Section follows when requests involve Second Party reports or allied identities.

If a Canadian client requests...	Then...
a US, UK, Australian or New Zealand identity suppressed from a CSEC report	Operational Policy staff review the rationale and release the information if appropriate.
Canadian identity information suppressed from a Second Party report	Operational Policy staff: <ul style="list-style-type: none"> <li>review the rationale and, if appropriate, ask the Second Party counterpart for the information (A rationale need not be provided to the Second Party.)</li> <li>input the information into the database holding suppressed information, and</li> <li>release the information to the client.</li> </ul>

### 6.2 Second Party Requests

This table describes how the Operational Policy Section handles Second Party partner requests for suppressed information.

If a Second Party requests...	Then the Operational Policy Section...
Canadian identity information suppressed from a CSEC or a Second Party report	Follows procedures described in Annex 1
An identity of their own national suppressed from a CSEC report	Provides the suppressed information.
An identity of another SIGINT allied national suppressed from a CSEC report	Contacts the other Second Party for authorization prior to releasing the information.

## 7. Retention and Storage of Suppressed Information

### 7.1 Storage of Suppressed Information

CSEC analysts who author reports containing suppressed Canadian and/or Allied identities enter the information into the suppressed information repository upon completion of the report.

When obtained from counterparts, the Operational Policy Section inserts information suppressed from Second Party reports into the repository.

### 7.2 Retention

For CSEC reports, suppressed information is retained in the following locations as outlined in the table below. In the case of Second Party reports, suppressed information, when available, is retained only in the repository.

**Note:** Completed "Request for Suppressed Information" forms exchanged via secure email must be purged from CSEC email systems once requesters have retained a hard copy, and the Operational Policy Section has retained a soft copy in a separate folder.

What	Who	Location	Retention Period
Hard copy of the traffic containing the identities attached to the resultant end product	Issuing Analyst	In a locked safe or filing cabinet with limited access	
Suppressed information from reports entered into the suppressed information repository by analysts and Operational Policy staff	<ul style="list-style-type: none"> <li>Issuing Analyst</li> <li>Operational Policy staff</li> </ul>	In the annotation field in the suppressed information repository, accessible only by Operational Policy staff, system administration staff, and report actors	
Completed "Request for Suppressed Information" forms	Operational Policy Section	Retains soft copy in a separate folder accessible only by Operational Policy staff	
	Requesters	May retain hard/soft copy according to: <ul style="list-style-type: none"> <li>Classification markings</li> <li>Departmental procedures related to the handling of information about Canadians</li> </ul>	

## 8. Request for Release of Suppressed Information Form

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 ( <i>mark an 'X' in the appropriate space(s)</i> ): ----- a) capabilities/intentions/activities of a foreign person, state, organization or terrorist group relating to international affairs, defence or security <div style="background-color: black; height: 20px; width: 100%;"></div> ----- c) use for prevention/identification/investigation of a potential threat to the life or safety of an individual in Canada or abroad ----- d) terrorist activity or threats to the security of Canada <div style="background-color: black; height: 100px; 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  <i>Released by:</i>  <i>Comments:</i>  This information is provided on the understanding that the requesting department requires the 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> .	

---

## **ANNEX 1 - Release Outside Canada of Canadian Identity Information Suppressed from SIGINT Reports**

---

### **A1.1 Introduction**

These procedures describe CSEC measures in place to protect the privacy of Canadians in the release outside Canada of Canadian identity information suppressed from SIGINT reports (including Canadian reports that are based on private communications collected by CSEC under the authority of a Ministerial Authorization).

---

### **A1.2 Context**

Second Parties occasionally request the release outside Canada of Canadian identity information that is suppressed from a Canadian SIGINT report or from a SIGINT report issued by another Second Party. GC clients may also request the release outside Canada of Canadian identity information suppressed from a Canadian or Second Party SIGINT report.

Because of the potential for serious repercussions to Canadian interests, all requests for the release of Canadian identity information outside Canada must be given careful consideration.

---

Effective date: 28 September 2012

### A1.3 Description of Release Process

The following table describes the stages involved in the processing of a request to release Canadian identity information (suppressed from SIGINT reports) outside Canada.

Stage	Who does it	Action	
1	Second Party, or GC client	Forwards a detailed request to CSEC’s Operational Policy Section. (See A1.4 for content of request.)	
2	Operational Policy staff	Review the request; and	
		<b>If the request is</b>	<b>Then Staff will</b>
		Incomplete	Ask Second Party or GC client for additional information.
		Complete	<ul style="list-style-type: none"><li>• Research/gather information related to the request(see A1.5); and</li><li>• Forward a request assessment to the Manager, Operational Policy (see A1.6)</li></ul>
3	Manager, Operational Policy	Provides to Director, Corporate and Operational Policy (Dir COP), recommendation that the request be approved or denied.	
4	Dir COP	<ul style="list-style-type: none"><li>• Reviews recommendation;</li><li>• Provides to ██████████ recommendation to approve or deny the request.</li></ul> <p>Note: When the request is extremely time sensitive (e.g., an imminent threat-to-life situation), Dir COP may approve or deny the request if ██████████ is unable to review the request within a reasonable time. Dir COP will brief ██████████ as soon as operationally feasible on the authorized release.</p>	
5	██████████	<ul style="list-style-type: none"><li>• Reviews recommendation;</li><li>• Consults with the CCSEC only as necessary. (The CCSEC may consult with counterparts at Canadian partner agencies including the National Security Advisor); and</li><li>• Approves or denies the request.</li></ul>	

Continued on next page

Effective date: 28 September 2012

**A1.3 Description of Release Process (continued)**

Stage	Who does it	Action
6	Operational Policy staff	<ul style="list-style-type: none"> <li>Provides reply (which is vetted by the Operational Policy Manager) to Second Party or GC client, which includes a caveat that the information is for research and lead purposes only (see A1.7).</li> <li>Retain request and all related documentation; and</li> <li>Update Metrics table.</li> </ul>

**A1.4 Content of Request**

The request for release of suppressed Canadian identity information must include:

- A detailed rationale which includes:
  - a justification of why the release of the Canadian identity information is in the interest of the requesting allied recipient country;
  - an explanation of how the requested information relates directly to an operating program or activity of the allied recipient; and
- A description of how the recipient will use the information, and any possible action-on activity taken against a Canadian.

**A1.5 D2 Research**

As part of the release process, Operational Policy staff must research and gather information related to the request.

**Questions to ask include but are not limited to:**

- Q1. For Canadian SIGINT reports, what is the collection source and type of communication (e.g. a private communication, or a communication of a Canadian located outside Canada)? In particular, is the report based on a private communication collected by CSEC under the authority of an MA?
- Q2. Is there any indication that the Canadian is involved in an unlawful activity?
- Q3. Are relevant GC departments [REDACTED] concerned about the release of the suppressed information to allied recipients?
- Q4. What are possible implications for Canadians and/or Canadian interests if the suppressed information is released to allied recipients.

*Continued on next page*

Effective date: 28 September 2012

**A1.5 D2  
Research  
(continued)****Whom to ask/ where to look:**

- [REDACTED] (Q1);
- Subject matter experts including the originator of the SIGINT report, CSEC specialists, CSEC Executives, and partner intelligence agencies (Q1, Q2, Q3, Q4); and
- GC clients (directly or via CSEC CRO) who have requested and received the suppressed Canadian identity information (Q2, Q3, Q4).

**Note:** If no GC client has requested the suppressed information, Operational Policy staff will consult the CROs and/or the CSEC PM (for a CSEC report) and ask that the report be shown to a GC client who may be able to provide the required feedback. The suppressed information will then be provided to the CRO as an advance release (see OPS-1-1 Section 5.2-5.3)

**A1.6 Request  
Assessment  
Criteria**

Operational Policy staff must research and gather information related to request, and provide an assessment of the request to the Manager, Operational Policy. Based on this assessment, the Manager will provide to [REDACTED] (via Director, Corporate and Operational Policy) a recommendation to approve or deny the request. The request assessment must:

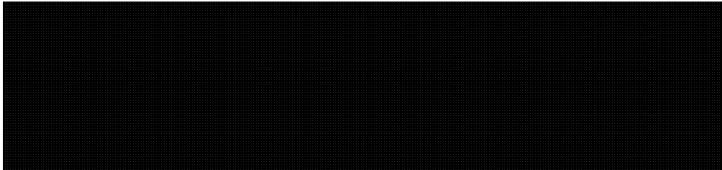
- A. Include the complete request from the Second Party or GC client (see A1.4), which describes:
  - The rationale, and
  - Any possible action-on taken against a Canadian.
- B. Show that the requested information relates to one of the following:
  - capabilities/intentions/activities of a foreign person, state, organization or terrorist group relating to international affairs, defence or security
  - [REDACTED]
  - prevention/identification/investigation of a potential threat to the life or safety of an individual
  - terrorist activity or threats to the security of the requesting country
  - [REDACTED]

*Continued on next page*




Effective date: 28 September 2012

**A1.6 Request  
Assessment  
Criteria**  
(continued)

- 
- 
- C) Indicate if the release of the Canadian identity information is essential to understanding the foreign intelligence in the SIGINT report.
  - D) Provide any indication that the Canadian (whose information is being suppressed) IS or IS NOT involved in one of the activities listed above (at A1.6-B).
  - E) Discuss any concerns or sensitivities that relevant GC departments may have regarding the release of the Canadian information outside Canada.
  - F) Identify possible implications for Canadians and/or Canadian interests if the suppressed information is released to allied recipients.
- Identify (for Canadian reports) the source of the collection and the type of communication (in particular, if it is a private communication collected by CSEC under the authority of an MA).
- 

**A1.7 Caveat to  
be Included on  
Reply**

The following caveat must appear on all replies to Second Party or GC clients that include Canadian identity information to be released outside Canada:

No further action may be taken with regards to this information without the prior approval of CSEC/Operational Policy. CSEC requests that the Canadian identity information be protected in accordance with the SIGINT community's procedures for handling allied national identities. Furthermore, this information may not be used in affidavits, court proceedings, or for any other legal or judicial purposes without the prior approval of the Chief, CSEC. Questions should be directed to CSEC/Operational Policy @cse-cst.gc.ca).

---