OPS-1-1: Policy on Releasing Suppressed Information

Effective Date: 14 November 2014

1. Introduction

1.1 Objectives

This policy outlines when CSE may release suppressed information to authorized recipients. Adhering to this policy will ensure that CSE protects the privacy of Canadians and persons in Canada and is compliant with the:

- *Canadian Charter of Rights and Freedoms* (the Charter);
- *Privacy Act;*
- *National Defence Act* (NDA), Part V.1;
- *Ministerial Directive on the Privacy of Canadians;* and
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*.

This policy supersedes Amendment 2 of OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports* (28 September 2012), and Section 2 of OPS-1-6, *Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports* (11 March 2010).

1.2 Context

The NDA mandates CSE to:

- Acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada (GC) intelligence priorities (part (a) of the mandate);
- Provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the GC (part (b) of the mandate); and
- Provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties (part (c) of the mandate).

Continued on next page

Introduction, Continued

Context (continued)

CSE's activities must be subject to measures to protect the privacy of Canadians and persons in Canada in the use and retention of intercepted information. In addition, where CSE has a privacy protection agreement with a foreign cryptologic agency (such as with Second Parties), CSE protects the identity information of their nationals.

Accordingly, CSE and its Second Party partners suppress privacy-sensitive information in their reporting by replacing specific identifying information (such as a name or email address) with a generic term (such as "a named Canadian" or "a Canadian email address"), thereby making it impossible for the reader to identify the individual.

Authorized recipients of these reports may request and receive suppressed information if they have both the legal authority and operational justification to receive it.

1.3 Authority to Release Suppressed Information

CSE's authority to release suppressed information about Canadians and persons in Canada stems from its authority to acquire, use, retain and disclose the information under subsection 273.64(1) of the NDA (and subsection 8(2) of the *Privacy Act*). The authority to release identity information related to Second Party entities originates in CSE's agreements with its partner agencies.

Any release of suppressed information must be in accordance with the NDA and the *Privacy Act*, as well as any relevant Ministerial Directives and Authorizations, and any applicable agreements.

The Chief, CSE has delegated the authority to release suppressed information to the [redacted] Under certain circumstances, this authority has been further delegated (see PCI-3, *Releasing Suppressed Information* for more information).

Continued on next page

Introduction, Continued

1.4 Application

This policy applies to CSE and CFIOG staff and any other parties acting under CSE authorities who are involved in requesting, releasing, and storing suppressed information from foreign intelligence (FI) or cyber defence reports.

1.5 Accountability

The following table outlines key responsibilities related to this policy:

Who	Responsibility
Chief, CSE	• Approves this policy
General Counsel Directorate, Legal Services (DLS)	• Reviews this policy to ensure compliance with the law • Provides legal advice, as required
Director General, Policy and Communications (DG PC)	• Recommends this policy for approval • Ensures the appropriate application of this policy
Policy Management	• Revises this policy • Answers questions regarding this policy
All CSE and CFIOG staff involved in requesting, releasing, and storing suppressed information	• Read, understand and comply with this policy and any amendments

1.6 Consequences of Non-Compliance

Failure to abide by this policy jeopardizes CSE's ability to fulfill its mandate in a manner that is compliant with its legal, Ministerial, and policy obligations. Non-compliance with this policy may lead to a finding of unlawfulness by the CSE Commissioner or a loss of trust by the Canadian public and/or Second Party partners.

Personnel who do not comply with this policy will face management disciplinary sanctions up to and including termination of employment.

1.7 Definitions

For definitions of key terms in this policy, see the *OPS Policy Glossary.*

2. Assessing Release Requests

2.1 Overview

Any authorized recipient of CSE reports can request suppressed information, including GC clients, client relations officer (CROs), Second Party government officials (via their national cryptologic policy centre), [redacted] and CSE staff.

Foreign entities may not submit requests for suppressed information directly to CSE. However, GC and Second Party partners may submit a request for suppressed information with the intent of sharing the information with a foreign entity. Any release of suppressed information where the final recipient is a foreign entity requires a Mistreatment Risk Assessment (MRA). See OPS-6, *Policy on Mistreatment Risk Management* and section 4.3 of this policy for more information.

Note: For the purposes of this policy, [redacted]

All requests must be submitted to CSE's Privacy and Interests Protection team via an appropriate classified system.

2.2 Providing a Rationale

Requesters must provide a robust justification for their request that:

- Outlines their requirement for the suppressed information;
- Identifies how it relates to their mandate and operational program; and
- Confirms that the information will remain under the control of the requester.

If a request relates to a possible violation of a Canadian or international law or agreement, the requester must identify the relevant law or agreement.

Second Parties must also identify how the information relates to their national intelligence requirements.

Continued on next page

Assessing Release Requests, Continued

2.3 Assessing the impact of a release

Before releasing suppressed information, the Privacy and Interests Protection team must assess the validity of the request and whether the release could impact the operational interests of the GC or pose a risk to the privacy of a Canadian or person in Canada. This may include:

Considerations	Examples
Type of information requested	• Full vs. partial name • Email address
Relevance of request to Canada's national interests (including any impact on international affairs, defence or security)	• Links to Canada's intelligence priorities • Safety and security of Canada and its allies
Possible positive impact on a Canadian or person in Canada	• Rescue/release of a Canadian hostage • Removal from a no-fly list
Possible negative impact on a Canadian or person in Canada	• Public release or further sharing of the information • Imposition of travel restrictions • Detention • Potential financial loss • Reputational damage • Civil litigation

3. Releasing Suppressed Information

3.1 Release Authorities

[redacted] is the approval authority to release suppressed information. Within the Privacy and Interests Protection team is responsible for releasing information.

See *PCI-3, Releasing Suppressed Information* for more information on the delegated authorities to release suppressed information within [redacted]

3.2 Releasing CII for Cyber Defence

Provided it will be used to help protect information infrastructures of importance to the Government of Canada, SIGINT may share unsuppressed Canadian identity information (CII) with IT Security. All SIGINT teams sharing unsuppressed CII with ITS are responsible for appropriately tracking and recording each occurrence. A periodic record of this sharing must be provided to the Privacy and Interests Protection team (D2A) for final record keeping.

3.3 Releasing CII Outside Canada

The release of CII outside of Canada must be managed through more rigorous approval process due to the potential impact on Canada's national interests. All requests must be carefully assessed to ensure compliance with legislation, Ministerial direction, and CSE policy.

3.4 Repetitive Releases

A repetitive release occurs when a GC or Second Party partner requests information pertaining to a Canadian entity about which it has previously received information. Because the potential impact on the operational interests of the GC and the risks to the privacy of a Canadian or person in Canada have already been assessed, the approval authorities for repetitive releases follow a modified process.

See PCI-3: *Releasing Suppressed Information* for more information.

Continued on next page

Releasing Suppressed Information, Continued

3.5 Releasing Information about Second Party Entities

The Five Eyes are responsible for managing the privacy rights of their own nationals. Each agency has the authority to receive information about its national entities and CSE must provide suppressed information related to a Second Party entity from a CSE report to its respective national cryptologic agency upon request.

CSE may release suppressed information about a Second Party entity from its own reporting to a GC recipient [redacted]

3.6 Requesting Second Party Information

While the Five Eyes are the approval authority for releasing the identity information of their own nationals, requests for suppressed information are submitted to the agency that authored the report containing the information. For example:

If ...	Then ...
CSIS requests suppressed information pertaining to a UK national contained in a GCHQ report	CSE submits the request and justification to GCHQ and GCHQ approves or denies the release.
CSIS requests suppressed information pertaining to a US national contained in a GCHQ report	CSE would submit the request and justification to GCHQ and GCHQ consults the NSA on the request.

CSE must submit a new request to the originating Second Party agency if a separate GC department requests suppressed information pertaining to a Second Party entity. For example, CSE must submit a new request if CSIS requests suppressed information that has previously been released to the RCMP.

3.7 Advance Release

To streamline support during a high-level meeting, crisis or other emergency or time-sensitive situation, a CRO may request the advance release of suppressed information if they anticipate their client will require the information on an urgent basis.

Continued on next page

Releasing Suppressed Information, Continued

Advance Release (continued)

The Privacy and Interests Protection team assesses the CRO's request. If an Advance Release is approved, the CRO is delegated responsibility for assessing a client's request and may only release the suppressed information in accordance with this policy and *PCI-3, Releasing Suppressed Information.*

The CRO must note any action-on being contemplated by the client and consult with the Privacy and Interests Protection Team, as appropriate. If the client does not request the Advance Release information, the CRO must not use or retain the information.

3.8 Exceptional Circumstances

In exceptional circumstances, [redacted] may approve, in writing, procedures that deviate from this policy and its associated instructions. [redacted] may also delegate alternate authorities for releasing suppressed information.

Any exceptional authorizations must be limited in scope and duration as appropriate to the circumstances. All entities acting under delegated release authorities must comply with Canadian law, Ministerial direction and CSE policies and procedures.

3.9 Automated Release

[redacted] may approve technical means that automate manual processes, so long as [redacted] is reasonably satisified that there are appropriate measure(s) to protect privacy.

3.10 Unauthorized Release

Any release of suppressed information that is not in accordance with this policy and its associated instructions must be reported to the Privacy and Interests Protection team [redacted]@cse-cst.gc.ca) for follow-on action and accounting purposes.

4. Handling Released Suppressed Information

4.1 Classification of Released Suppressed Information

After its release, suppressed information retains the security classification of the FI or cyber defence report from which it originated and is subject to the same handling and use restrictions as the original report.

For information on sanitizations of Special Intelligence (SI) information, see PCI-2, *Sanitizations and Actions-On.*

4.2 CSE Caveats

When releasing suppressed information, CSE must include measures to remind recipients of their responsibilities regarding its use and retention. The use of accredited systems and caveats is generally considered effective. CSE uses different caveats depending on whether the recipient is a Canadian or Second Party entity, for example:

> No further action may be taken with this information without the prior approval of CSE/Corporate and Operational Policy. CSE 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, CSE. Questions should be directed to CSE, Corporate and Operational Policy ([redacted]@cse-cst.gc.ca).

A list of caveats can be found on CSE's [redacted]

4.3 Further Dissemination of Released Information

GC and Second Party partners may request suppressed information with the intent of using it internally or sharing it with another national agency, or a foreign [redacted] The rules related to the further dissemination of released information vary according to the recipient.

GC Partners: GC partners do not require CSE approval to further disseminate suppressed information within their own organization at the original classification and on a need-to-know basis. GC recipients require CSE approval before disseminating suppressed information to [redacted]

Continued on next page

Handling Released Suppressed Information, Continued

Further Dissemination of Released Information (continued)

[redacted] may not disseminate supressed information to an external client without approval from CSE.

Second Parties: A Second Party must specify the intended recipients of the suppressed information at the time of the request and require CSE approval prior to further disseminating suppressed information. If a Second Party intends to share suppressed information with a foreign entity, CSE is responsible for conducting the MRA.

4.4 Action-on

Recipients of suppressed information may not take any follow-on action as a result of the information without prior approval from CSE's Privacy and Interests Protection team. For more information on action-on requests, see PCI-2, *Sanitizations and Actions-On.*

4.5 Storing Suppressed Information

CSE reporting standards require CSE analysts who author reports containing suppressed information to store the information in an appropriate suppressed information repository (e.g. [redacted]). Suppressed information obtained from Second Party reports is also retained in this repository. Access to the repository is limited to designated personnel.

GC and Second Party partners that receive suppressed information from CSE must ensure that their policies and procedures comply with the requirements of the *Privacy Act* and the *Canadian SIGINT Security Standards* (CSSS-100), where applicable.

4.6 Retaining and Destroying Suppressed Information

CSE's operational policies provide detailed guidance on the retention and destruction of FI and cyber defence reports. For further information, consult:

- OPS-1-11, *Retention Schedules for SIGINT Data*;
- OPS-1-14, *Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization*; and
- OPS-1-15, *Operational Procedures for Cyber Defence Activities Using System Owner Data.*

5. Additional Information

5.1 References

- *Canadian Charter of Rights and Freedoms*
- *National Defence Act*
- *Privacy Act*
- *Access to Information Act*
- *Personal Information Protection and Electronic Documents Act*
- *Ministerial Directive – Framework for Addressing Risks in Sharing Information with Foreign Entities*
- *Ministerial Directive on the Privacy of Canadians*
- *CSE Ethics Charter*
- OPS 1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
- OPS 1-8, *Operational Procedures for Policy Compliance Monitoring to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
- OPS 1-11, *Retention Schedules for SIGINT Data*
- OPS 1-14, *Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization*
- OPS 1-15, *Operational Procedures for Cyber Defence Activities Using System Owner Data*
- OPS 6, *Policy on Mistreatment Risk Management*
- *OPS Policy Glossary*
- PCI 2, *Sanitizations and Actions-On*
- PCI 3, *Releasing Suppressed Information*
- CSSS-100, *Canadian SIGINT Security Standards*

5.2 Amendments

Situations may arise where amendments to this policy are required because of changing or unforeseen events. Significant changes require Chief, CSE approval, though this approval may be delegated. Minor amendments may be approved by DG PC.

5.3 Audit and Review

The implementation of this policy is subject to management monitoring, internal audit, and external review by various government review bodies, including the CSE Commissioner and the Privacy Commissioner.

5.4 Questions

Questions related to this policy and its associated procedures should be submitted to [redacted]@cse-cst.gc.ca.