SIGINT PROGRAMS INSTRUCTION

INADVERTENT COLLECTION OF NON-TARGETED TRAFFIC

Effective: February 25, 2014.

INTRODUCTION

(C) SIGINT Programs Instructions (SPIs) are working aids intended to address gaps and grey areas that are only partially addressed by, or scattered over several, existing policy instruments. They represent a consolidated and/or expansion of information contained within other policy instruments (e.g., CSOIs, OPS documents, etc.)

(S//SI) SPI-3-14 complements policy instruments regarding the protection of the privacy of Canadians, including:

- OPS-1, *Protecting the Privacy of Canadians & Ensuring Legal Compliance in the Conduct of CSE Activities*;
- OPS-1-11, *Retention Schedules for SIGINT Data*;
- OPS-1-13, *Operational Procedures Related to Canadian* [redacted] *Collection Activities*; and
- CSOI-4-4, *Targeting Identifiers For Foreign Intelligence Under Part (a) of CSE's Mandate*.

(U) CSE must always act lawfully in delivering its mission. Protecting the privacy of Canadians is a fundamental tenant of our mission. CSE must apply reasonable measures to safeguard the privacy of Canadians while striving for the most effective[1] collection operations to produce foreign signals intelligence of value to GC clients.

CONTEXT

(TS//SI) CSE's operating environment is complex. Unlike private sector service providers or commercial carriers, CSE cannot call upon informed network administrators to locate and acquire traffic of interest. [redacted]

[redacted]

[1] 'Effective' here is primarily intended to refer to the degree to which its collection programs collect data, metadata, and communications associated with government of Canada intelligence requirements. The more collection is in line with these requirements, the more effective it can be said to be.

(TS//SI) Given these factors, it is understood that CSE is likely to encounter occasional system issues that result in the inadvertent collection of non-targeted traffic, in spite of having taken all reasonable measures to prevent it. To mitigate the risk to the privacy of Canadians resulting from such issues, and to maintain compliance with its legal requirements, CSE has policies and procedures in place to handle situations when inadvertent collection occurs. These procedures include:

- The mandatory annotation of any recognized Private Communication (PC) or viewed traffic that contains information about Canadians for selected data. (OPS-1 - Reporting is provided to the Minister of National Defence on annotated PCs and non-essential annotated PCs are destroyed.);
- The prohibition from searching traffic repositories for anything other than traffic matching an appropriately targeted entity (OPS-1, CSOI-4-4);
- The automatic purging of collected traffic after a certain time (OPS-1-11); and
- The requirements to report, evaluate and resolve, and document any instance of inadvertent collection of non-targeted traffic once identified (OPS-1-13 and SPOC procedures).

(S//SI) Due to the variety and complexity of CSE selection, collection and processing systems, each identified instance of inadvertent collection is likely to be different in scope and consequence from others. Thus, each must be independently assessed.

REQUIRED ACTIONS IN THE EVENT OF INADVERTENT COLLECTION OF NON-TARGETED TRAFFIC

(TS//SI) Guidelines for incident evaluation and assessment are included below. Existing procedures established by DGP/SPOC will be used during the evaluation, and begin with submission of the Inadvertent Collection of Non-Targeted Traffic web form. The web form will capture details of the event for tracking and compliance purposes, to include:

- Determining the scope of overall inadvertent collection:
  - *How long has the inadvertent collection been occurring?*
  - *Which collection, processing, and viewing systems are implicated?*
  - *Does the incident involve the inadvertent collection of metadata or content or both?*
  - *What percentage of overall collection from the collection source is inadvertent?* (e.g. as a percentage of overall collection from the [redacted] system)
  - *What percentage of collection of the specific type in question is inadvertent?* (e.g. as a percentage of [redacted]
- Based on the results of the above analysis, determine whether any inadvertently collected traffic items have been annotated by analysts as private communications or as containing information about Canadians.

- Assess the legal and policy implications of the inadvertent collection.
  - *Has CSE inadvertently violated any policies, any Canadian law?*

- Assess whether there exists a requirement to take immediate action, based on significant, unmitigated risks, and consider:
  - immediate suspension or alteration of implicated collection systems
  - options for purging already collected inadvertent traffic
  - whether communications or instructions are required for staff who may have been exposed to inadvertently collected traffic
  - completion of privacy incident notification (if required)
  - consultation with legal services and/or DGPC and, as required, proactive notification of OCSEC, MND

- If risks can be mitigated effectively in the near term, consider:
  - ongoing monitoring of the implicated collection system(s) to determine if inadvertent collection reoccurs
  - communications or interim instructions to staff and management
  - interim policy direction to mitigate any immediate privacy concerns
  - reasonable longer-term actions, such as altering technical systems, policies or procedures, etc. to provide reasonable privacy protections and ensure that CSE collecting only data that it is authorized to acquire

(S//SI) All decisions related to the management of inadvertent collection will be justified and documented by SPR for oversight, compliance, and planning purposes. Appropriately classified documentation on handling of these cases will be published, in an effort to ensure wide understanding of relevant policy considerations, and to help set expectations in handling of future situations.

(S//SI) All actions identified as required to incident handling will be assigned to individual points of contact with clear timelines for follow up and resolution. Policy and oversight areas must be kept advised of actions and progress to ensure compliance and incident tracking.

ROLES AND RESPONSIBILITIES

Director SPR	Director SPR oversees and coordinates the overall SIGINT response to inadvertent collection events and ensures that DGP, DC SIGINT and SIGINT Round Table (RT) are informed about any event and responses taken.
Individual or Group within SIGINT who recognized the event	Immediately upon discovery of inadvertent collect, reports the incident to SPOC and fills out the inadvertent collection web form at Inadvertent Collection of Non-Targeted Traffic web form.
SPOC	The SPOC Compliance Management Team coordinates response in the event of inadvertent collection for SIGINT, prepares a report for Director, SPR, and publishes associated context and resolution.
Associated SIGINT Collection Area(s)	Provides contextual information on relevant collection systems and, as appropriate, options to mitigate future events. Adjusts collection systems as a result of decisions taken, if required.
[redacted] Group	Provides contextual information on relevant processing systems, and adjusts processing infrastructure as a result of decisions taken, if required.
[redacted]	Provides contextual information on collected traffic and related targeting. Works with SSD and requests purging of traffic items from CSE [redacted] traffic repositories as a result of decisions taken, if required.
SSD	Provides contextual information on processing systems related to the incident. Adjusts processing infrastructure or purges data identified by [redacted] as a result of decisions taken, if required.
DC SIGINT & SIGINT Roundtable	Provides executive direction and decision-making in response to inadvertent collection incidents, as appropriate.

PROMULGATION

(S//SI) I hereby approve SPI-3-14, *Inadvertent Collection of Non-Targeted Traffic.* This SIGINT Programs Instruction is effective immediately.

James Abbott

SIGINT PROGRAMS INSTRUCTION

Director General, SIGINT Programs