SIGINT PROGRAMS INSTRUCTION

FOREIGN ASSESSMENTS AND PROTECTED ENTITIES

Effective January 31, 2014

INTRODUCTION

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

(S//SI) Based on the authorities in the National Defence Act, Sections 273.64(1)(a) and 273.64 (2)(a), SIGINT activities must be directed at foreign entities located outside Canada. As such, an informed assessment of the foreign status must be performed against entities of intelligence interest prior to engaging in SIGINT activities such as targeting, reporting and metadata analysis. By definition, a foreign assessment is not definitive and requires regular monitoring and validation. CSOI-4-4, *Targeting Identifiers for Foreign Intelligence*, outlines the elements of information that must be considered in conducting a foreign assessment.

(S//SI) This SPI is intended to provide additional guidance in the form of principles. This instruction does not propose a specific process, nor negate any of the requirements outlined in CSOI-4-4. Each set of operational circumstances requires an appropriate course of action which cannot be captured ahead of time. Due to the complex nature of the SIGINT business, it is impossible to prevent all privacy incidents. However, policies and instructions, coupled with principles can help reduce the number, frequency and impact of privacy incidents.

(S) Individual operational areas are responsible for conducting and documenting foreign assessments. The Office of the CSE Commissioner (OCSEC), or other review bodies, may review the documentation associated with foreign assessments.

(S//SI) This SPI also provides guidance on assigning the "Protected Entity" status to known Canadian or allied entities in CSE's Target Knowledge Base (TKB).

(S//SI) This instruction complements guidance provided in:

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*,
- CSOI-4-1, *SIGINT Reporting*,
- CSOI-4-4, *Targeting Identifiers For SIGINT Reporting Under Part A Authorities*.

CONTEXT

(S//SI) While it is understood that a foreign assessment in a SIGINT context is not an absolute determination, nor is it always valid over time, enhanced guidance will address:

- recommendations from oversight bodies with respect to clarifying language related to the association between selection criteria (such as identifiers) and entities in operational records;
- policy questions from operational areas regarding "Protected Entities";
- principles to reduce privacy risks.

PRINCIPLES

(TS//SI) Establishing the location and nationality of an entity of intelligence interest is critical prior to initiating any SIGINT activity, but it is also increasingly challenging. In order to minimize privacy risks, four principles are proposed:

1. If there is no reason to believe that an entity may be Canadian or in Canada (or allied or in allied territory), consider it foreign.
2. If there is any uncertainty regarding the status of an entity, conduct research using the least intrusive methods first, progressing to more intrusive ones, only as required.
3. If it looks or is Canadian (or allied), and it is linked to an FI operation, protect it.
4. Use clear language to document the association between an identifier and an entity.

(S//SI) **PRINCIPLE 1**: Record the foreign assessment in CSE's TKB based on available information and reassess when new information comes to light, in accordance with CSOI-4-4. In many cases, noting the nationality and location of the foreign entity in the TKB along with the reasons for its suspected connection to an FI entity or issue of interest will be sufficient. This principle should cover the majority of activities for most operational teams.

(S//SI) **PRINCIPLE 2:** When in doubt about an entity's status, begin researching in the least intrusive data sources, such as CSE's TKB, the report dissemination tool (currently [redacted]) or non-SIGINT data sources, where feasible. This includes consultations with other agencies, such as DFATD and CBSA (via Corporate and Operational Policy -D2), open source queries using secure infrastructure ([redacted]), as appropriate. If non-SIGINT sources are inapplicable or inconclusive, then CSE SIGINT metadata repositories may be queried. The use of SIGINT data to perform a foreign assessment must be limited to just that, and when there is an indication that an identifier may be associated with a Canadian or allied entity, or an entity in Canada or allied territory, the activities **must stop** and the identity information must be documented as a "Protected Entity" in CSE's TKB in order to prevent other analysts from inadvertently directing their activities at this entity.

(TS//SI) Finally, if the research is conducted on a Canadian- or allied-looking identifier (e.g. with a Canadian area code or domain name), which an analyst believes is associated with a foreign person outside Canada and allied territory, the analyst's Team Leader must pre-authorize the use of SIGINT databases and tools to perform the assessment, given the increased risk to privacy. [redacted] repositories may be queried, provided the risks to privacy interests of Canadians have been considered. Any queries against auditable [redacted] repositories involving "friendly-looking" identifiers (e.g. mrjohnsmith@mail.ca or janet@yahoo.com) believed to be associated with foreign entities should be discussed with auditors in advance, to avoid compliance incidents.

(TS//SI/CEO) A metadata query using an identifier that is associated [redacted] requires senior management approval under the authorities of OPS-1-10, *Operational Procedures for Metadata Analysis Using a* [redacted]

(S//SI) **PRINCIPLE 3**: For the sole purpose of preventing inadvertent targeting or naming, when an entity that has clear links to foreign entities of intelligence interest is assessed or known to be Canadian or allied, it is good practice to create a record in CSE's TKB for the entity and mark it "Protected". It should be noted that the OCSEC has made favorable comments about this practice in past reviews.

(S//SI) It may not be necessary or appropriate to include all available information about a Canadian or allied person in the TKB. Document the identifiers and any information that is required to understand the link to foreign intelligence entities, namely the entity's name, any aliases, the source of the information, the date of the information and the foreign targets with whom it is, or has been, in contact. Operational areas are responsible for determining how much additional information must be stored about a Canadian (or allied) entity in order to prevent privacy incidents, including (re)targeting, inadvertent naming, or unauthorized metadata analysis. Targeting or naming a "Protected Entity" constitutes a privacy incident that must be reported in accordance with instructions posted on the SPOC webpage. Please note that operational areas are discouraged from including information about Canadians in [redacted] repositories (e.g. [redacted]) as this would attract unwanted attention to Canadian entities.

(S//SI) **PRINCIPLE 4**: Use clear language to document the foreign assessment methodology and results (steps, data sources, date, etc.). In previous OCSEC reviews, the wording in targeting records was found to be unclear, particularly regarding attribution of an identifier to a specific entity. For example, stating that individual X is "associated with" phone number 512345678 may not be sufficiently explicit. It is preferable to indicate that individual X is the [redacted] of telephone number 512345678, or that he/she is [redacted] phone number 512345678, etc. If CSE's TKB is not suitable to document those details, consider creating a separate record that is accessible and retrievable by colleagues who have a need-to-know. For instance, [redacted] may be an appropriate mechanism to document the foreign assessment. Ideally, the TKB record should point to any other record that would be associated with the entity.

EXCEPTIONAL CIRCUMSTANCES – EMERGENCIES

(TS//SI) In exceptional circumstances[1], where available information does not allow a firm conclusion that an entity is or is not Canadian or in Canada (or allied or in allied territory), and there is an imminent threat to life or other emergency, an operational area may seek senior management guidance in weighing the risks of proceeding with targeting identifiers associated with this entity. Consultations with DGI, DGP and DGPC are recommended. DLS may also be consulted, as required. The facts supporting the decision to proceed with targeting the entity's identifiers must be thoroughly documented and retrievable to facilitate any future audit or review.

[1] Exceptional circumstances may be defined as threats to the security of Canada as defined in the CSIS Act, or as other circumstances described in OPS-1-10.

SIGINT PROGRAMS INSTRUCTION

(TS//SI) Below is an example of facts that could support a decision to make a foreign assessment in an emergency, where information is unclear or conflicting. Taken in isolation, none of these descriptors would be sufficient to make an informed assessment. These include information about [redacted]

[redacted]

PRIVACY INCIDENTS

(S//SI) Conducting research to make a foreign assessment and discovering that an entity is Canadian (or allied) or in Canada (or in allied territory) does not constitute a privacy incident, when the research did not touch on any unselected SIGINT content (such as might be held in certain auditable [redacted] repositories). Any results of queries leading to a "non-foreign" assessment must be destroyed.

(S//SI) When foreign assessment research involves unselected SIGINT content, and it is ultimately assessed that an entity is Canadian, at that point a privacy incident must be reported, in accordance with SPOC instructions posted on the Intranet. If the foreign assessment research within auditable [redacted] SIGINT content repositories reveal any 5-Eyes entities, these activities must also be reported to SPOC.

PROMULGATION

(C) I hereby approve SPI-1-14, Foreign Assessments and Protected Entities. This SIGINT Programs Instruction is effective immediately.

James Abbott
Director General, SIGINT Programs