SIGINT PROGRAMS INSTRUCTION

SPI-2-14

SIGINT ███████████████ DATA

Effective March 20, 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.).

(TS//SI) Under Section 273.64(1)(a) of the *National Defence Act (Part a) of CSE's Mandate*), in order to enable the acquisition of foreign intelligence from the Global Information Infrastructure[1] (GII), SIGINT engages in Network Analysis and Prioritization activities. These activities seek to ███████████████████ ████████████████████ of most value to meet GC foreign intelligence priorities. Network Analysis and Prioritization activities include:

- ● ███
- ● ███
- ● ███
- ● ███
- ● ███

(TS//SI) ███████████ data" is that information which details the ██████████████████ ███████████████████████████████████ Information becomes ███████████ data' once it has been recognized and evaluated as such, and therefore is distinct from "metadata", as outlined in SPI-2-13, *Metadata in a SIGINT Context*. ███████████ data is recognized and evaluated within the 5-Eyes SIGINT Production Chain ███████████████████████

(S//SI) SPI-2-14 complements existing policy instruments, including:
- ● OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities;
- ● OPS-1-11, Retention Schedules for SIGINT Data; and
- ● SPI-2-13, Metadata in a SIGINT Context.

---

[1] Global information infrastructure (GII) includes electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in, or relating to those emissions systems and networks. (National Defence Act, section 273.61)

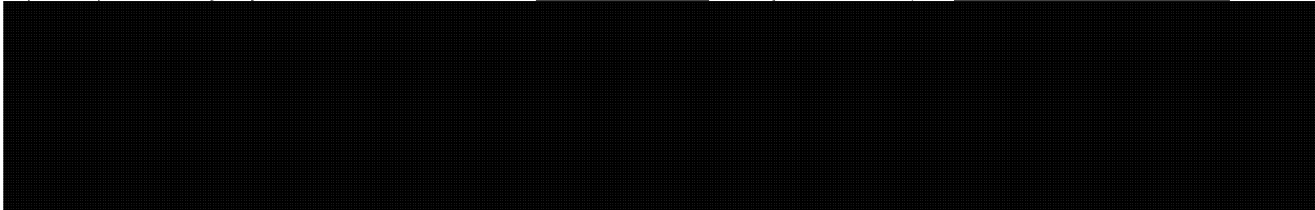Communications Security Establishment Canada   Centre de la sécurité des télécommunications Canada

Canadä

SIGINT PROGRAMS INSTRUCTION

SPI-2-14

CONTEXT

(TS//SI) The expression █████████ data" applies to information relating to any █████████████ ██ It can pertain to ██ such as:

████████████████████████████
████████████████████████████
████████████████████████████
████████████████████████████

(TS//SI) For the purposes of this instruction, █████████ data pertains only to ████████████ ██ ██ ██ ██

(TS//SI) ████████ data can be derived from many sources, including SIGINT, HUMINT and Open Source. The following are examples of sources of ███████ data:

- SIGINT ████████
- SIGINT traffic content,
- SIGINT metadata,
- SIGINT ████████████████████████████
- HUMINT-acquired data, and
- publically available information such as ████████████████

AUTHORITIES AND PRIVACY

(TS//SI) Under Part a) of CSE's mandate, CSE is permitted to derive and retain ████████ data █████ ██ because this data is necessary to enable ████████████████████████████████████ enhances SIGINT's ability to █████████████████████████ offer the best potential FI value, i.e. ██████ ████████████████████████████ and also supports CSE's ability to provide assistance under Section 273.64(1)(c) of the *National Defence Act* (Part c) of CSE's mandate), should a domestic partner agency request it.

██
██

SIGINT PROGRAMS INSTRUCTION

SPI-2-14

(TS//SI) Given that ████████ data pertains to ███████████████████████████ ███ Should ███████ Information[4]" associated with a Canadian ███████████ be discovered and retained while deriving ███████ data, measures to protect Canadian privacy interests must be applied, in accordance with OPS-1.

HANDLING, RETENTION, USE AND DISSEMINATION

(S) The source of ████████ data will determine associated policy requirements. Source information must be stored with all ███████ data records[5]. Multiple sources of ███████ data can be combined or merged to produce the most accurate and complete representation ███████

(S) HUMINT-derived ███████ data does not constitute SIGINT data, and will, at a minimum, be afforded the protection that is requested by the originating agency.

(S//SI) ████████ data derived from Open Source does not constitute SIGINT data. Requests for ███████ data made through ████ will follow SPOC guidance posted on the ████████

(TS//SI) Given that ███████ data is evaluated, it may be retained for as long as operationally required or as long as the information remains relevant. Recognizing the complexity of the GII, ███████ data is shared across the 5-Eyes SIGINT Production Chain on a daily basis, ██

(TS//SI) ████████ data may be released ███████████████████████████████ in the form of a serialized product. ████████ data derived from SIGINT data may be sanitized for release outside COMINT channels, in accordance with published sanitization procedures. Requests to share ████████ data ████████ ███████████ will be assessed on a case-by-case basis, through consultations with appropriate stakeholders.

---

[3] ██

[4] ████████ information is information of, from, or about a Canadian ████████████████████████ ████████████████████████████████████ See OPS-1 for details.

[5] ████████ data included in serialized product does not require source information.

[6] Link: ████████████████████████████████████

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Canada

2016 03 17

AGC0273

3 of 4

A-2017-00017--03962

PROMULGATION

(C//SI) I hereby approve SPI-2-14, SIGINT ███████████ Data. This SIGINT Programs Instruction is effective immediately.

James Abbott
Director General, SIGINT Programs

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Canada