DGI Familiarization Manual

Table of Contents

(This document is maintained in CERRID #841563.)

CHAPTER 1: INTRODUCTION TO CSE

1.1 General

CSE's mission

CSE is Canada's national cryptologic agency. Our mission is to provide the Government of Canada with two key services: foreign signals intelligence in support of defence and foreign policy, and the protection of electronic information and communication.

CSE's vision

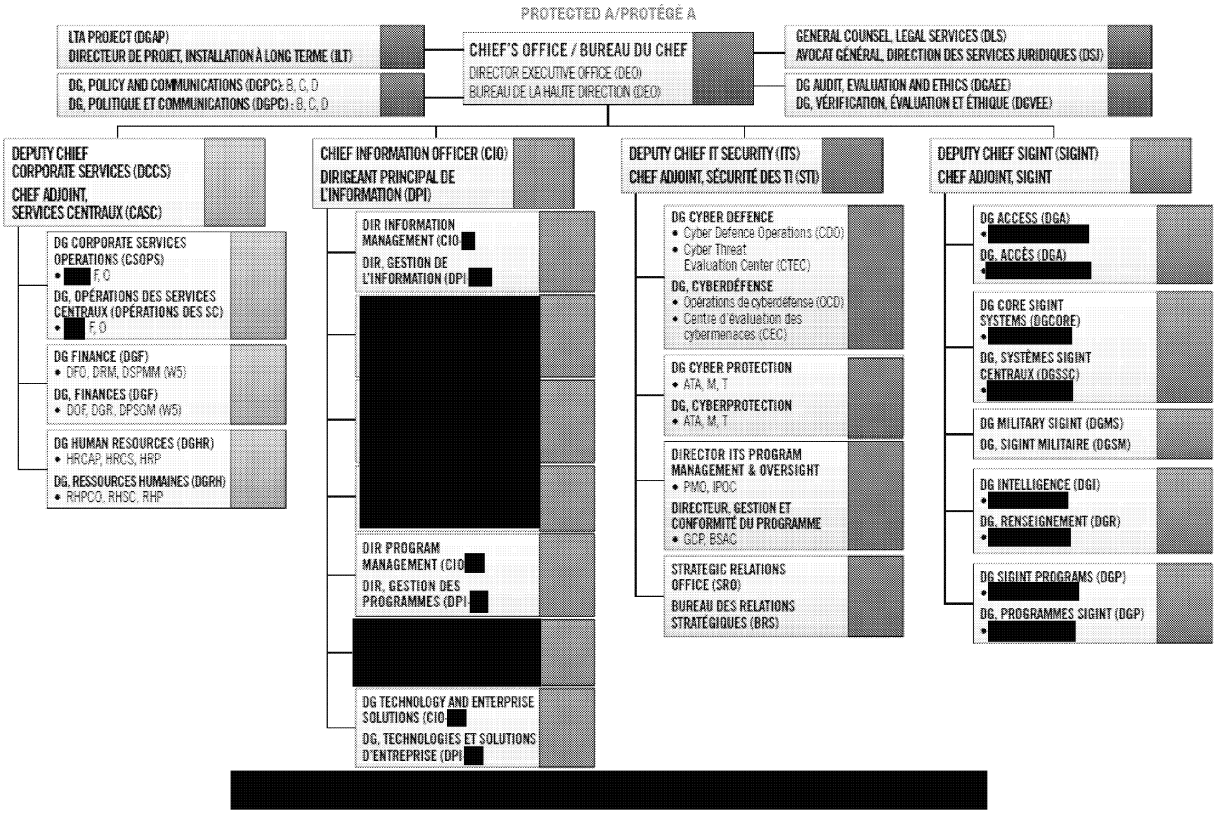
To be the national agency that masters the global information infrastructure to safeguard Canada's national security through information superiority.

CSE's crest

The CSE crest, or badge as it is officially described, was granted to CSE by the Chief Herald of Canada on October 19, 1994. The crest, CSE's corporate symbol, was designed by the Chief Herald, and the use of the Royal Crown was approved by the Queen.

The navy blue middle circle represents the world of information. The inner golden circle, together with the red maple leaf, symbolizes Canada. The lightning flashes denote communications, while the key represents the secure and sensitive nature of the information that CSE provides and protects. The outer blue and gold circle contains the motto *NUNTIUM COMPARAT ET CUSTODIT*, which is a Latin translation of the phrase "Providing and Protecting Information."

CSE's org chart



CSE's Chief

John Forster

Mr. Forster was appointed Deputy Minister and Chief of the CSE effective January 30, 2012.

Prior to his appointment, Mr. Forster served as the Associate Deputy Minister of Infrastructure from 2009 to 2012, where he oversaw the design and delivery of many of the Government's infrastructure stimulus programs under its Economic Action Plan. Previous to his tenure with Infrastructure Canada, he was the Associate Assistant Deputy Minister for Safety and Security at Transport Canada where he developed a transportation security strategy and focused on transportation security issues in aviation, rail, transit and marine modes.

Mr. Forster has a Bachelor of Science from the University of Toronto and a Master of Business Administration from York University. He has completed studies in environmental economics at Harvard.

CSE's mandate

According to the *National Defence Act* Part V.1, Section 273.64, CSE's mandate covers three parts:

Part A:
to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

Part B:
to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and

Part C:
to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

Questions to ask yourself as an analyst:	
1. **Nationality:** Is my activity directed at a foreign person or entity? 2. **Geography:** Is the foreign person or entity located outside of Canada? 3. **Foreign intelligence:** Does the expected information or intelligence relate to the capabilities, intentions or activities of the foreign person or entity? 4. **Priority:** Does the expected information or intelligence relate to an intelligence priority of the Government of Canada?	➢ If you answer **YES** to all questions, you can operate under **Part A**. Proceed in accordance with Operational Policy. ➢ If you answer **NO** to any question, this activity cannot be conducted under Part A. If the activity can be conducted under the authority of another Government of Canada federal law enforcement or security agency, CSE may be able to provide support under **Part C** if certain criteria are met. Consult your manager before any action is taken.

Analysts in the Intelligence Branch operate mostly under Parts A or C, very rarely under Part B.

1.2 CSE Values

Lawfulness

Operating scrupulously within the laws of Canada.

Every employee, observing this value:

- considers and follows relevant laws when taking action or making decisions;
- when in doubt, seeks advice and guidance from experts (e.g., their managers, CSE legal services, access to information and privacy) to identify the course of action that is consistent with the law; and
- respects the law and the obligation to maintain the oath of secrecy and high standards of security.

Respect

Believing in each other's ability to contribute to CSE's vision and mission and respecting the talents of all our employees. Treating all employees — regardless of level, occupation and location — with equal consideration and dignity.

Every employee, observing this value:

- recognizes and supports everyone's ability to contribute to CSE's vision, respecting the diversity of all employees' attributes and talents;
- creates a supportive environment, enabling others to feel confident about their contributions and encouraging them to be self-starting and innovative; and
- seeks to understand and balance the competing demands between work and personal life.

Integrity

Always acting ethically, reliably, and forthrightly. Assuming responsibility for actions taken and decisions made.

Every employee, observing this value:

- deals honestly and openly with people both inside and outside CSE;
- agrees on a desired outcome – through consultation with co-workers and clients – and works diligently to achieve it;
- respects the confidentiality and privacy of information; and
- accepts accountability for actions and outcomes without passing blame.

Teamwork

Everyone working together as partners to achieve our vision through an integrated process and clearly defined goals, roles and responsibilities.

Every employee, observing this value:

- provides clear communication and support to enable others to achieve higher common goals;
- puts team performance first by supporting a common vision and putting the desired outcome ahead of personal gain;
- realizes that the shared knowledge of individuals with different backgrounds is key to developing effective solutions and strategies;
- listens to others and willingly shares needed information, treating the opinions and concerns of others with respect; and
- builds partnerships both inside and outside of government, convincing others of the advantages of working together toward a common objective.

Professionalism

Consistently producing high quality work for all business activities while setting a standard for others to follow. Operating in a manner that complements the standards of specific professions and reinforces CSE's values.

Every employee, observing this value:

- applies or interprets rules and regulations responsibly by understanding their general intent and by bringing any that are in need of review/revision to the attention of the responsible parties;
- consistently takes a stand for the right thing to do – despite opposition from others – but knows when to compromise and set aside differences for the common good of CSE;
- produces quality work – as defined with the client – that is clear, accurate and precise, while, at the same time, continuously striving for improvement;
- identifies obstacles to the delivery of results, solving problems as they arise or making the appropriate persons aware when assistance is needed;
- accepts ultimate responsibility for his/her own continuing professional development and draws upon relevant learning opportunities and resources available through CSE;
- helps set performance standards and ensures their common understanding and consistent interpretation; and
- employs performance standards to make decisions objectively and openly, and to encourage consistency in dealings with others.

Service

Anticipating, understanding and responding appropriately to client needs. Striving to meet — if not exceed — CSE's quality service standards.

Every employee, observing this value:

- establishes and maintains strategic partnerships with other CSE employees to deliver quality products and services;
- knows when to say "no" to clients or co-workers in a manner consistent with CSE's values;
- focuses on the development of products and services that take advantage of diverse and changing technology; and
- anticipates client needs and responds appropriately.

Innovation

Developing new ways of understanding situations, solving problems and creating opportunities.

Every employee, observing this value:

- researches and develops new ideas and/or concepts, challenging assumptions and the *status quo* when necessary, to improve work methods and solve common problems;
- engages others in the thinking process (e.g., asking what if, undertaking option analysis, etc.) to encourage and assist them in finding solutions to problems or improving work methods;
- supports calculated risk-taking and applies best practices and lessons learned; and
- identifies and capitalizes on opportunities in new business segments to revitalize or abandon markets or programs as appropriate.

For more information

The "CSE Values and Ethics Code" can be found on the CSE intranet at:
[redacted]

1.3 Foreign Intelligence

What is intelligence?

Traditionally, intelligence has been subdivided into several categories. **Commercial intelligence** relates to the capabilities and intentions of one's commercial rivals and competitors, often to the acquisition of confidential or proprietary information about their strategies, e.g., bid information, processes, finances or markets. **Military intelligence** can be either tactical – relating to the disposition of the enemy's troops and equipment in the field – or strategic, relating to longer-term capabilities in the light of total military strength and the capacity to maintain it. **Security intelligence** applies to both domestic and foreign threats to the basic security of a state and to the integrity of the state system. **Criminal intelligence** applies to that which the police should know in order to counter and apprehend those engaged in organized crime, smuggling, extortion and the like. **Foreign intelligence** is probably the broadest category, in that it relates to the defence of a country and the conduct of its foreign affairs in the widest sense.

What is foreign intelligence?

As an employee of CSE's Intelligence Branch, you will soon be writing foreign intelligence reports for senior Government of Canada officials.

Foreign intelligence (FI) is defined as "information or intelligence about the **capabilities**, **intentions** or **activities** of a foreign **individual**, **state**, **organization** or **terrorist group**, as they relate to international affairs, defence or security" (*National Defence Act* Part V.1, Section 273.61). It includes data of a [redacted] and is obtained from a variety of sources. (To remember the key elements "capabilities, intentions, or activities", think CIA.)

What is SIGINT?

Signals intelligence (SIGINT) can be broken down into three categories:

- COMINT (Communications Intelligence)
- ELINT (Electronic Intelligence)
- FISINT (Foreign Instrumentation Signals Intelligence)

Most of the analysts in CSE's Intelligence Branch deal primarily with **COMINT**, or foreign communications intelligence. The intelligence is derived from several different sources, primarily [redacted] sources.

ELINT is [redacted] by the [redacted], a.k.a. [redacted] in the [redacted] to track electronic emissions, and [redacted]

[redacted]

How COMINT is collected

The communication modes that are used to provide COMINT include [redacted] Communications may be [redacted]

Signals are carried on electromagnetic waves that travel within and/or through the earth's atmosphere. These signals are communications between two entities: the transmitter and the recipient. Common examples of a transmitter are radio and television stations, while the receivers are the listeners and viewers.

Just as public broadcast communications are carried in the form of electromagnetic waves, so are private communications. Although private communications are not meant to be received en masse like public broadcasting signals, there is nothing to prevent unintended recipients from intercepting a private message if they have the proper equipment. When such a message is intercepted, it is still received undisturbed by the intended recipient; therefore the transmitter and recipient have no way of knowing whether the message was intercepted along the way. Some transmitting parties, aware that this form of intercepting communications exists, will send messages in a coded or encrypted form. The recipient, who has the key to the cipher, can decode the message and read it. Any unintended recipients who intercept the enciphered signal will not be able to read the actual message unless they can break the cipher.

CSE's international partners

Canada is one of five countries that have formed an alliance to cooperate in the [redacted] of foreign intelligence. The five members of the quinquepartite ("Five-Eyes") agreement are:

Acronym	Agency	Country
CSEC	Communications Security Establishment Canada	Canada
NSA	National Security Agency	USA
GCHQ	Government Communications Headquarters	UK
DSD	Defence Signals Directorate	Australia
GCSB	Government Communications Security Bureau	New Zealand

Second party operations

Not only do these five governments cooperate in the [redacted] of SIGINT, they have also agreed not to mount a SIGINT effort against one another. Thus, when we say that CSE [redacted] foreign intelligence signals, we mean signals from any country other than

the Five-Eyes. So, when we speak of Second Party operations (e.g. collection, requirements, reporting) we are referring to operations undertaken by one or more of the other four countries in the quinquepartite agreement.

[redacted] is located in room SLT A241 and has a [redacted] over which classified matters can be discussed [redacted] is in room SLT B256 and has a [redacted]

[redacted]

CHAPTER 2: INTELLIGENCE BRANCH (DGI)

2.1 Introduction

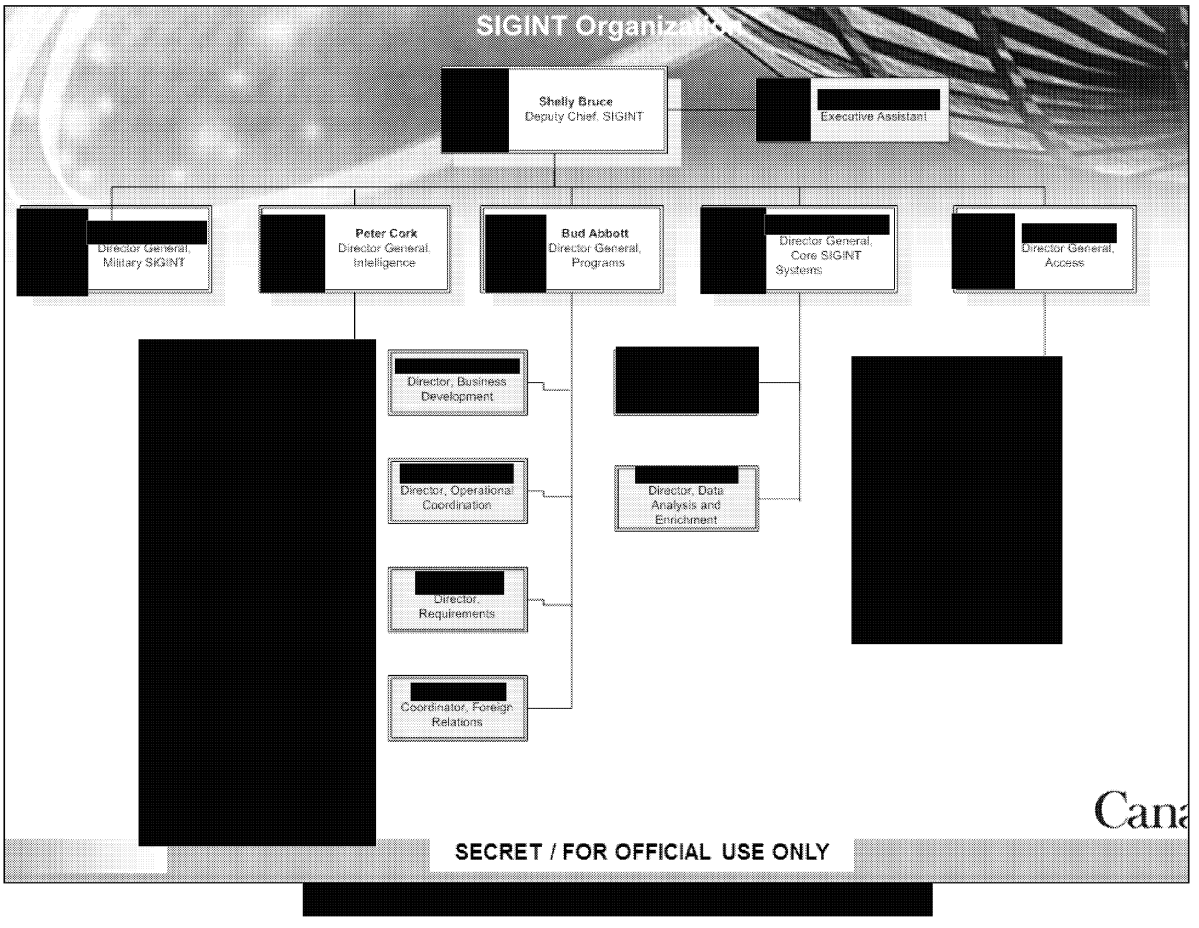
Intelligence Branch mandate

The Intelligence Branch, officially known as the Directorate General Intelligence or DGI, is responsible for the provision of foreign intelligence reports and activities in support of Government of Canada intelligence priorities.

Web location – DGI Homepage

Information from the Intelligence Branch is posted on the CSE Intranet under *Organization > SIGINT > Intelligence* at [redacted]

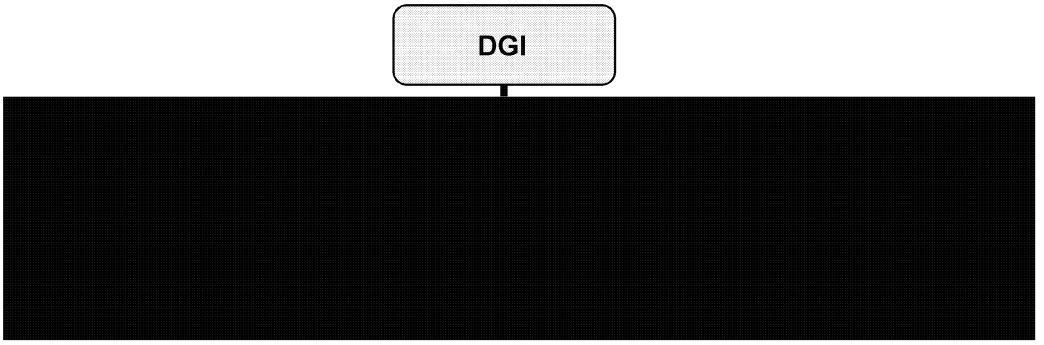
CSE SIGINT Organization



2.2 Organizational Structure of DGI

Overview

The Intelligence Branch is comprised of the following five groups:



The **group** Group)'s mandate is to produce SIGINT analysis, reporting, and services in support of the GC's requirements on and below are informally known as the Office of Counter-Terrorism (OCT), whereas is known as the Office of

The Group)'s mandate is to provide foreign intelligence supporting the as well as requirements, including

[redacted]

The [redacted] **group** [redacted] focuses on [redacted] concentrates on issues related to [redacted] This includes both traditional IRRELEVANT and [redacted] operations. Its primary targets are [redacted]

[redacted]	

[redacted]

The [redacted] **group** [redacted] Group) consists of the [redacted] the [redacted], and the [redacted] focuses on advanced techniques of [redacted] data and analysis throughout CSE. It provides support to [redacted] aims to be the first stop for new analytical tradecraft in DGI. Its staff supports DGI through [redacted] teaching and delivering [redacted] assists in developing, acquiring or promulgating techniques for advanced [redacted] information management, open source intelligence and [redacted] development. [redacted] focuses on [redacted] activities include:

- [redacted]
- [redacted]
- [redacted]

[redacted]	

Client and [redacted]

The Client and [redacted] Group [redacted] Group) supports the critical business functions of the Intelligence Branch through the activities of its three components, [redacted] Client Services (CRO and [redacted] support), and the [redacted] Program.

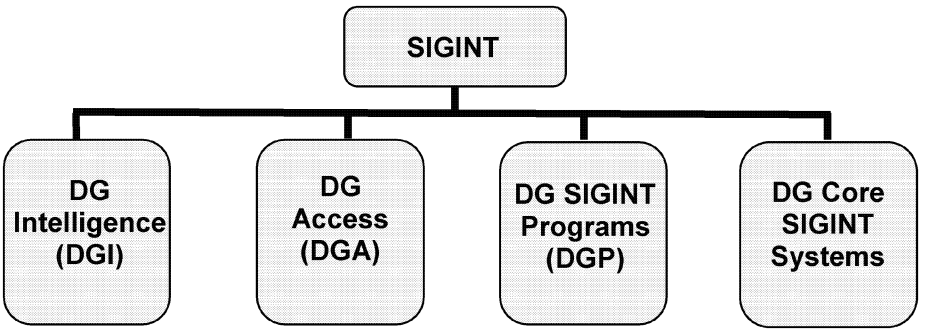
[redacted]	(budgeting, training, [redacted])
Client Services (CRO and [redacted]	support)
[redacted]	

2.3 Groups Contributing to the Work of DGI

Introduction

DGI operates together with virtually all other areas of SIGINT. This section describes the groups that comprise the SIGINT organization at CSE, and shows how their efforts contribute to the work that DGI performs.

The overall architecture within SIGINT is illustrated below:

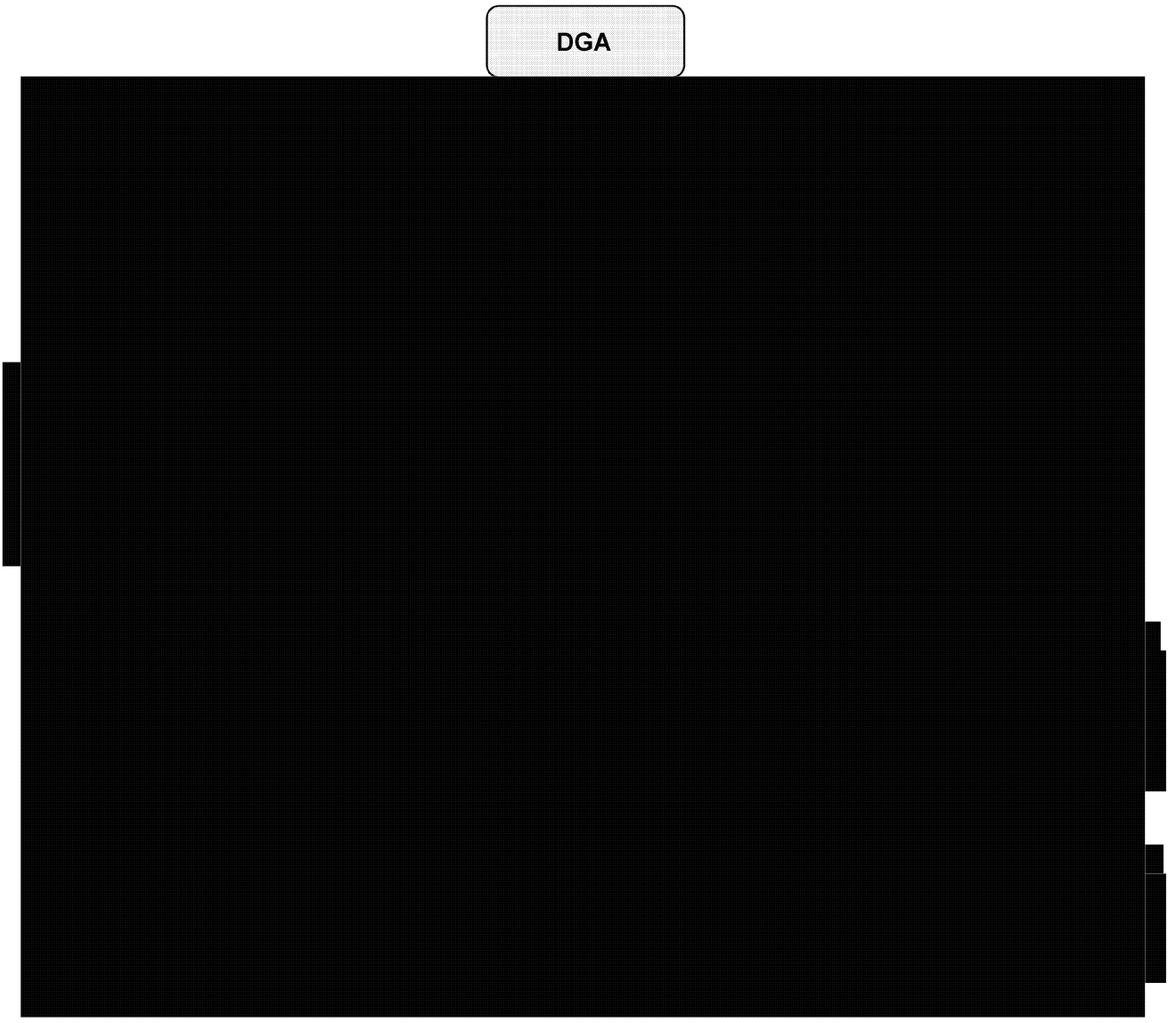


DG Access

DGA works to ensure CSE has the ability to [redacted]

[redacted]

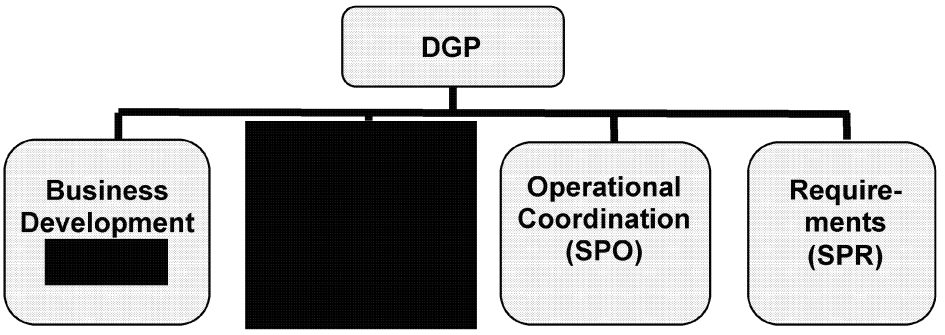
DGA is organized into the following [redacted] groups:



DG SIGINT Programs

DG SIGINT Programs (DGP, previously known as [redacted] Group) is responsible for a number of coordination functions. DGP maintains situational awareness of the strategic, operational and technical aspects of the end-to-end SIGINT mission.

DGP is made up of four groups:



Business Development [redacted]

[redacted] manages the [redacted] and [redacted]

The [redacted] manages SIGINT-related training and education at CSE, primarily through in-house developed learning events, but also by arrangement [redacted] through external course registration.

[redacted] two mandates are SIGINT Planning and SIGINT Performance Measurement. SIGINT Planning produces strategic operational plans, and the Metrics team produces data and analyses (metrics) illustrating SIGINT's performance against strategic or technical plans.

[redacted]

The [redacted] and staff facilitate the development of [redacted]

Operational Coordination (SPO)

SPO is responsible for maintaining the [redacted] and for managing the CSE Operational Production and Coordination Centre (COPCC).

[redacted] (also known as the Watch Office, formerly CANSOC, Canadian SIGINT Operations Centre), located in SLT C246, fulfills its role through two distinct areas. The Communications area is responsible for monitoring and troubleshooting CSE's internal and external communications and networks, and providing after-hours IT Service Desk support. The Watch Office is responsible for 24-hour monitoring of SIGINT and open sources for terrorism, outbreaks of hostilities and other threats to Canadian security. [redacted] also provides support to Client Relations Officers (CROs) and is the first responder in crisis situations.

COPCC, located in SLT C422, is a centralized operations structure that brings together critical staff from [redacted] to concentrate on urgent intelligence priorities. The COPCC, also known as "the floor", coordinates area specialists within a centralized operations structure that work together on the priority issues of the day.

Requirements (SPR)

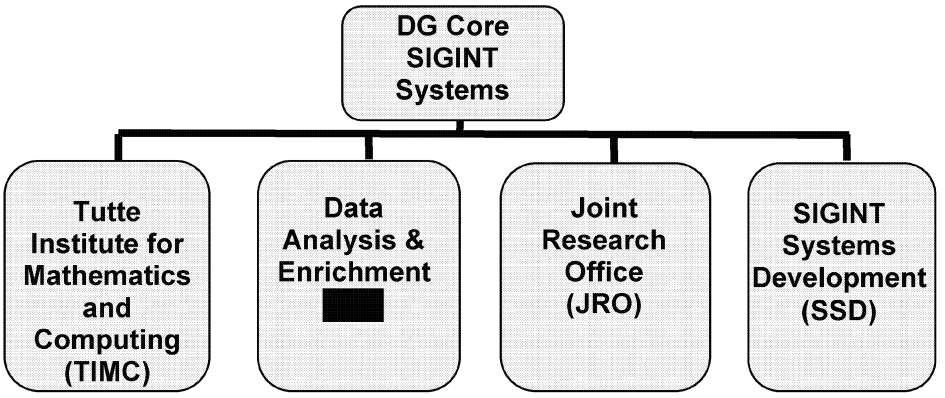
Two key components within the SIGINT Requirements group are SIGINT Programs Oversight and Compliance (SPOC) and SIGINT Programs Operational Requirements (SPOR).

SPOC is responsible for ensuring that SIGINT's activities are conducted in compliance with CSE's legal and policy framework. SPOC also acts as internal oversight for SIGINT, including the implementation of compliance validation monitoring procedures. SPOC also produces the Canadian SIGINT Operations Instructions (CSOIs), which provide guidance to SIGINT personnel on how to conduct their work on a day-to-day basis. SPOC is the point of entry into SIGINT for external and internal audits and reviews (e.g., the Office of the CSE Commissioner (OCSEC)) and oversees the implementation of recommendations resulting from these reviews. In addition, SPOC coordinates the SIGINT response to the disclosure of SIGINT outside COMINT channels (e.g., Access to Information requests, government inquiries, criminal prosecutions and civil litigation suits).

SPOR IRRELEVANT maintains the National SIGINT Priorities List (NSPL).

DG Core SIGINT Systems

DG Core SIGINT Systems includes the following four groups:



Tutte Institute for Mathematics and Computing (TIMC)

The TIMC, formerly called the Cryptologic Research Institute (CRI), conducts classified research in the areas of cryptology and knowledge discovery. It is the first classified research institute of its kind in Canada, and works in partnership with a network of:

- distinguished mathematicians, computer scientists and engineers at the national and international level,
- leading researchers from Canadian and international universities and research institutes, and
- various Canadian governmental agencies.

Data Analysis and Enrichment [redacted]

[redacted]

Joint Research Office (JRO)

The JRO provides joint ITS and SIGINT oversight to ensure CSE's research program as a whole is responsive to the operational environment. The JRO monitors research requirements, provides advice and guidance on technology transfer, fosters research relationships, and aligns CSE's research programs through research management.

SIGINT Systems Development (SSD)

The mandate of SSD (formerly [redacted] Group) is to provide state-of-the-art IT solutions and support to SIGINT staff and clients in the government, while researching potential IT alternatives for the future. SSD is responsible for researching, developing, and maintaining many of the SIGINT tools which DGI analysts use, including:

- [redacted], the end-product report storage and authoring tool,
- [redacted]
- [redacted] the [redacted] and targeting tool, and
- [redacted] the metadata database for [redacted] collected traffic.

2.4 DGI Reporting

Overview

Previously, the Intelligence Branch focused primarily on [redacted] reporting. However, since the events of September 11 and Parliament's passing of the *Anti-Terrorism Act* in December 2001, greater emphasis has been put on [redacted] reporting. The emphasis on [redacted] was again reinforced in April 2004 with the introduction of Canada's National Security Policy, the first-ever policy of its kind in Canada (see [redacted]

While it is easy to divide SIGINT into broad reporting areas, there is much inherent ambiguity and overlap. [redacted] SIGINT has to contend with these blurred lines and alert complementary business lines to activity that may cross over into their areas.

GCRs

Government of Canada Requirements (GCRs) reflect the Canadian government's ongoing intelligence requirements.

GCRs are generated by SIGINT Programs Operational Requirements (SPOR), based on feedback from clients stating their areas of interest. A GCR is made up of a [redacted] A general statement of a requirement is used as the basis for a GCR. For example, [redacted] is the GCR for [redacted] For a complete list of GCRs, search for "GCR" in the [redacted] which contains a link to the list.

Currently, there are over [redacted] GCRs on the GCR list.

National SIGINT Priorities List

The National SIGINT Priorities List (NSPL) was developed in March 2004 to help CSE focus its work on those areas of highest overall concern to the Government of Canada in order to best leverage resources and optimize the SIGINT system.

The national requirements for SIGINT are presented and managed in 2 ways:

Standing Issues	The "Standing Issues" portion of the NSPL reflects the intelligence requirements of highest priority to the Government of Canada. These priorities are ranked 0-4, [redacted]

	[redacted]
Watching Briefs	The "Watching Briefs" of the NSPL are derived from [redacted]

The NSPL is updated and reviewed on a regular basis–in the case of the Standing Issues, at least quarterly; for Watching Briefs, at least weekly. The current NSPL can be found on the CSE website under *Organization > SIGINT > National SIGINT Priorities List.*

[redacted] Reporting

Most of the analysts who write [redacted] end-product reports (EPRs) work in [redacted] These analysts write [redacted] EPRs, [redacted] They work closely with our counterparts at CSIS and the RCMP in responding to requests. [redacted]

[redacted] Reporting

Analysts assigned to [redacted] belong to the [redacted] group, and generally work with intercepted communications (traffic) [redacted]

IRRELEVANT

IRRELEVANT

Rationale for [redacted] reporting

Reports based on [redacted] intelligence:

[redacted]

[redacted] reporting

DGI analysts also scan traffic [redacted]

Rationale for [redacted] reporting

Reports based on [redacted] intelligence can assist the Canadian government [redacted]

DGI reports and client feedback

Once a report has been approved for release within DGI, it is retained in an end-product report database, accessible via CSE Client Relations Officers (CROs) scan the report file on a daily basis and choose reports to show their clients, and then the CROs provide the feedback to the reporting units via

This process of client feedback via the CROs not only helps the analysts fine-tune what the clients' requirements are (and are not), but also contributes to the analysts' sense of work satisfaction, since this is evidence that their work has served a specific purpose. In some cases the CROs provide comments that the client made about the report, such as "the report was timely, useful", "the client was not aware of ...", "the client recommended that this report be shown to X", etc. The next section on CSE clients and Client Relations Officers explains the role of the CROs in more detail.

2.5 Clients and Client Relations Officers (CROs)

CSE's clients

CSE provides SIGINT to Canadian government officials in some departments in Ottawa. These clients are served from five client service centres located in:

- Foreign Affairs, Trade and Development Canada (DFATD)
- Privy Council Office (PCO)
- Canadian Security Intelligence Service (CSIS)
- Industry Canada (IC)
- Department of National Defence (DND)

Each client service centre is led by a Level V supervisor who supervises the work of the Client Relations Officers (CROs), monitors client satisfaction and plans future service to the client departments. The individual CROs are responsible for providing tailored, personalized service to up to clients.

Client Relations Officers (CROs)

SIGINT reports are either sent directly to clients through electronic delivery services or delivered to clients personally by a CRO. Except for limited hard-copy series reports, SIGINT reports are stored in the end-product database.

CSE CROs are employees of the [redacted] They work in one of the five client service centres and provide SIGINT to over [redacted] clients, from director to ministerial level. When a new client is indoctrinated for SIGINT, the CRO conducts an introductory interview, explaining the SIGINT program and soliciting requirements for personalized service. After the interview, the CRO writes a [redacted] This allows SIGINT analysts to consider this client's requirements in their acquisition and reporting efforts. The CRO then queries [redacted] on a regular basis for end-product reports that meet the client's requirements.

The frequency of client service visits varies according to the urgency of the intelligence and the stated needs of the client for service. Clients read SIGINT for the purpose of acquiring greater information on the [redacted] They also seek insight on threats and tactics of hostile international entities of interest to the Government of Canada.

Client feedback

During a client service interview, the CRO presents the reports to the client in priority order (based on pertinence and urgency) and monitors the reactions of the client. These reactions and any information volunteered by the client are called *feedback*. The CRO may also ask specific questions concerning reporting, designed either to elicit more feedback and new requirements or to provide background information to analysts at CSE to steer further reporting and acquisition.

Feedback also monitors CSE's success in answering client requirements, the quality of service and reporting, and how SIGINT was used by the government.

RFIs

Requests for Information (RFIs) are requests from clients for SIGINT support on a specific issue or target. They can come from any of CSE's Government of Canada clients. RFIs, submitted and reviewed in [redacted], facilitate direct contact between CSE and the client and help analysts focus their targeting to assist with client operations. All RFIs are prioritized and actioned according to the NSPL. The response can be in the form of an end-product report or a [redacted] sent only to the requesting agency/department.

Info Needs

Information Needs (Info Needs) are a means for a client to communicate foreign lead information to DGI for use by CSE analysts. Info Needs are disclosures of particularly sensitive operational information from law enforcement and security agencies (LESAs), typically CSIS, the RCMP and

CBSA. As the information often contains Canadian identity information (CII), Info Needs are communicated by e-mail to DGI, and not as an RFI.

CRO services

CROs offer a range of services to the client including:

- indoctrinations and de-indoctrinations to special compartmented information
- advice in using information from SIGINT
- sanitizations
- requests for suppressed information
- referrals of reports to other clients
- correct interpretation of SIGINT

[redacted]

CHAPTER 3: SECURITY

3.1 Introduction

IRRELEVANT

Group Security Officers (GSOs)

IRRELEVANT

3.2 CSE Telephones

IRRELEVANT

Telephone security

IRRELEVANT

Telephone greetings

IRRELEVANT

Dialing out of CSE

IRRELEVANT

Dialing NSA

IRRELEVANT

3.3 Handling classified material

Clearances and indoctrinations

Most employees in the Intelligence Branch hold a Top Secret Special Access (TSSA) clearance, but some employees work with material that requires an additional clearance and is protected under the Exceptionally Controlled Information (ECI) program. Access to ECI material is on a NEED-TO-KNOW basis, and is COMPARTMENTED; in other words, only those individuals who require the knowledge and clearance to work on a specific task receive the particular ECI indoctrination.

If you receive ECI indoctrinations, please remember that ECI material is very sensitive and should not be the subject of idle chat. You may discuss ECI information only with people who have the required ECI indoctrination.

As a new employee in the Intelligence Branch, you will need to ask many questions on a regular basis in order to acquire a clear picture of what we do and of what is expected of you, and you should not let any apprehension about treading into ECI-related matters deter you from asking questions. In the unlikely event that you do ask a question that touches on an ECI area, the respondent will simply tell you that he/she is not permitted to give you that type of information. Fortunately for everyone, you are already indoctrinated for the vast majority of information related to the daily workings of the Intelligence Branch.

Printing of classified material

IRRELEVANT

Removal of classified material

IRRELEVANT

IRRELEVANT

Destruction of classified material

IRRELEVANT

3.4 Office Security

Uncleared personnel

IRRELEVANT

Covering up

IRRELEVANT

Visits

IRRELEVANT

Disarming the office

IRRELEVANT

Arming the office

IRRELEVANT

IRRELEVANT

Safes

IRRELEVANT

Walk-through

IRRELEVANT

Foreign travel

IRRELEVANT

Building pass

IRRELEVANT

Cameras

IRRELEVANT

Radios

IRRELEVANT

Portable and wireless devices (PIDs)

IRRELEVANT

IRRELEVANT

CDs and multimedia files

IRRELEVANT

Fire alarm

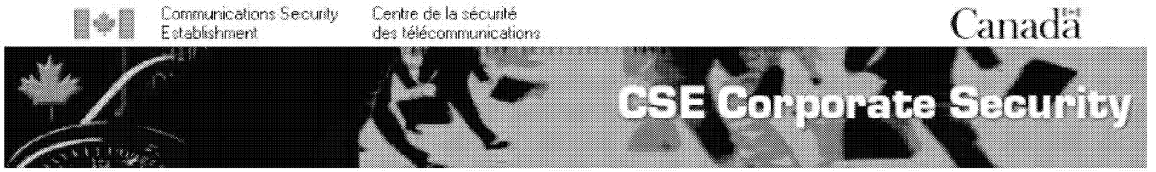
IRRELEVANT

Health and safety

IRRELEVANT

Security communiqués

IRRELEVANT



April 2004

Security is your business!

IRRELEVANT

17 February 2004

PUBLIC STATEMENTS ABOUT CSE

IRRELEVANT

CSE Communications CST

Communications Security Establishment | Centre de la sécurité des télécommunications

Corporate Security Directorate

UNCLASSIFIED
For Internal CSE Use Only

June 12, 2007

BBQ Season & "Conversational Security"

IRRELEVANT

UNCLASSIFIED
For Internal CSE Use Only

Canada

IRRELEVANT

IRRELEVANT

August 2004

IRRELEVANT

IRRELEVANT

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Corporate Security Directorate

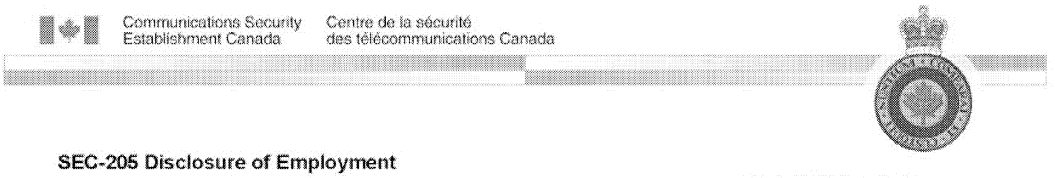
UNCLASSIFIED

1 Dec 2008

What to Say About Working at CSEC

IRRELEVANT

Security is your business, too—make it a priority!



SEC-205 Disclosure of Employment
Effective date: December 1, 2008

CONFIDENTIAL

SEC-205 DISCLOSURE OF EMPLOYMENT

IRRELEVANT

Corporate Security Directorate

Canada

SEC-205 DISCLOSURE OF EMPLOYMENT *continued*

IRRELEVANT

Continued on next page

Basic Principles about Disclosing Your Employment *continued*

IRRELEVANT

Continued on next page

Basic Principles about Disclosing Your Employment *continued*

IRRELEVANT

Disclosing Your Employment – General Scenarios

IRRELEVANT

Continued on next page

Disclosing Your Employment – General Scenarios *continued*

IRRELEVANT

Disclosing Your Employment – Specific Scenarios

IRRELEVANT

Continued on next page

Disclosing Your Employment – Specific Scenarios *continued*

IRRELEVANT

Disclosing Your Employment – Specific Scenarios *continued*

IRRELEVANT

Disclosing Your Employment – Specific Scenarios *continued*

IRRELEVANT

Reference

IRRELEVANT

Security Committee Policy Promulgation

IRRELEVANT

UNCLASSIFIED

TEST YOUR SPY - Q

IRRELEVANT

1 of 2

UNCLASSIFIED

IRRELEVANT

2 of 2

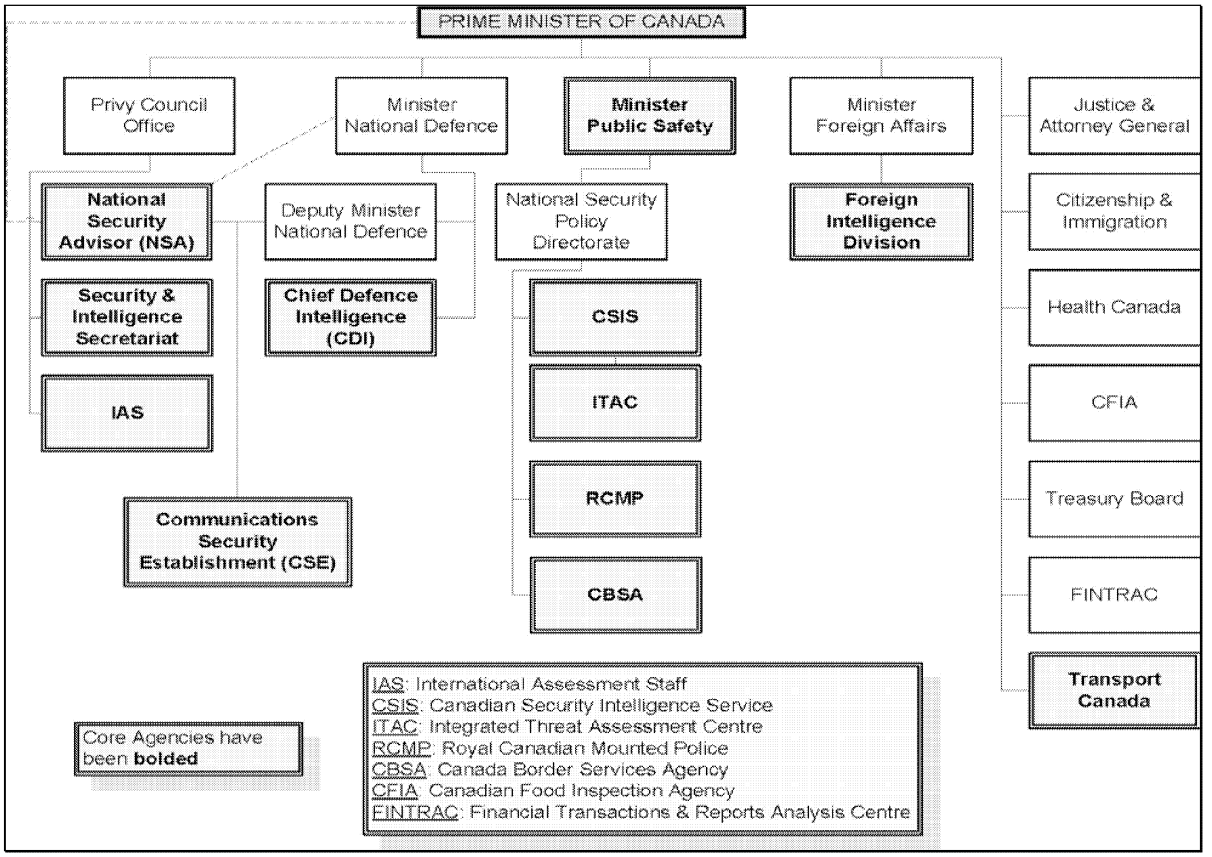
CHAPTER 4: CSE IN THE INTELLIGENCE COMMUNITY

4.1 GENERAL

The core of the Canadian intelligence community comprises those departments and agencies having responsibilities for foreign affairs, defence and national security:

- Privy Council Office (PCO)
- Foreign Affairs, Trade and Development Canada (DFATD)
- Department of National Defence (DND)
- Canadian Security Intelligence Service (CSIS)
- Royal Canadian Mounted Police (RCMP)
- Public Safety and Emergency Preparedness Canada (PSEPC)
- Canada Border Services Agency (CBSA), formerly a part of Citizenship and Immigration Canada (CIC)
- Integrated Threat Assessment Centre (ITAC)

Other departments such as Transport Canada also play an important role in the process; see the structural diagram below:



The CSE Commissioner

The Office of the CSE Commissioner (OCSEC) was established in 1996 under the *Inquiries Act*, and the duties of the Commissioner were codified in the *National Defence Act* in December 2001. The mandate of the CSE Commissioner, a supernumerary or retired judge, is to review the operations of CSE and attest to their compliance with the laws and Constitution of Canada. The Commissioner will undertake any investigation in response to a complaint, and inform the Minister of National Defence and the Attorney General of any activity not in compliance with the law. The Commissioner submits an annual report to the Minister of National Defence, which is then tabled in Parliament. The Commissioner has full access to all documents related to the agency, and to the personnel of CSE.

The OCSEC website at CSE contains a record of the Commissioner's Annual Reports.

The Chief of CSE

The Minister of National Defence is accountable to Cabinet and Parliament for all CSE activities, while providing direction on how CSE carries out its mandate. The Chief of CSE is a Deputy Minister of National Defence reporting directly to the Minister. (Before 16 November 2011, the Chief, as Associate Deputy Minister, reported indirectly to the Minister through two Deputy Ministers: the National Security Advisor to the Prime Minister, who was responsible for CSE's policies and operations, and the Deputy Minister of National Defence, who oversaw financial and administrative matters.) The Chief also participates in a committee of Deputy Ministers supporting the Cabinet Committee on Security, Public Health and Emergencies, chaired by the Deputy Prime Minister, and the Ad Hoc Cabinet Committee on Security and Intelligence Priorities, chaired by the Prime Minister. An Intelligence committee of Assistant Deputy Ministers meets more frequently throughout the year to assist the various departments and agencies to function as a community.

Since CSE's inception, the Chiefs have been:

1946-1971	**Edward Drake**
1971-1980	**Kevin O'Neill**
1980-1989	**Peter Hunt**
1989-1998	**Stew Woolner**
1999-2001	**Ian Glen**
2001-2005	**Keith Coulter**
2005-2012	**John Adams**
2012-	**John Forster**

4.2 The Privy Council Office (PCO)

Role of the PCO

The Privy Council Office (PCO) provides public service support to the Prime Minister across the entire spectrum of policy questions and operational issues facing the Government, including matters relating to the management of the federation and constitutional development. Under the direction of the Clerk of the Privy Council and Secretary to the Cabinet, the PCO is the general public service department of the Prime Minister and the Cabinet's secretariat.

Structure of the PCO

The clerk of the Privy Council and Secretary to the Cabinet provides direct support to the Prime Minister from the perspective of the values, traditions and expertise of the public service. This position encompasses three inter-related roles:

- the Prime Minister's Deputy Minister
- the head of the Public Service of Canada
- the Secretary to the Cabinet

As head of the public service department of the Prime Minister, the Clerk of the Privy Council serves as the principal link between the Prime Minister and the public service, and is responsible to the Prime Minister for its overall effectiveness. In providing support to the Cabinet, he or she provides support and advice to the Ministry as a whole to ensure that the Cabinet decision-making system operates according to the design of the Prime Minister.

Under the direction of the Clerk of the Privy Council and the Secretary to the Cabinet, the function of the PCO is to assist the Prime Minister in maintaining the cohesion of the Ministry and giving direction to it. The Prime Minister looks to the PCO for advice and support, therefore, in appointing senior office holders and organizing the government, in operating the Cabinet decision-making system, in setting overall policy directions, in advising on particular initiatives, and in managing specific issues that are of special concern to the head of government.

Clerk of the Privy Council and Secretary to the Cabinet

As the senior public servant supporting the Prime Minister, the Clerk of the Privy Council and Secretary to the Cabinet has three primary responsibilities:

- He/She is the Prime Minister's Deputy Minister, providing advice and support to the Prime Minister on his or her full range of responsibilities as head of government, including management of the federation.

- As the Secretary to the Cabinet, he/she provides support and advice to the Ministry as a whole and oversees the provision of policy and secretariat support to Cabinet and Cabinet Committees.

- He/She is the Head of the Public Service, responsible for the quality of expert, professional and non-partisan advice and service provided by the Public Service to the Prime Minister and the Ministry.

National Security Advisor to the Prime Minister

The National Security Advisor to the Prime Minister provides information, advice and recommendations on national security and emergency policy matters, and coordinates integrated threat assessments and inter-agency cooperation among security organizations. The National Security Advisor also oversees two groups within the PCO: the Security and Intelligence Secretariat, responsible for supporting the Cabinet in formulating intelligence policies, and the International Assessment Staff (IAS), which produces intelligence assessments on a wide range of subjects for Cabinet and senior officials.

Assistant Secretary to the Cabinet (Security and Intelligence)

Under the direction of the Assistant Secretary to the Cabinet (Security and Intelligence), this secretariat is responsible for overall coordination and policy direction for the security and intelligence sector. It also provides secretariat support to a deputy head level committee, the Interdepartmental Committee on Security and Intelligence (ICSI). The Clerk of the Privy Council and Secretary to the Cabinet is the chair of ICSI, and the Deputy Clerk of the Privy Council (the Coordinator) is the vice-chair. The secretariat provides general supervision of the overall management of intelligence organizations and general policy guidance and priorities to the intelligence community.

The Assistant Secretary to the Cabinet is also responsible for the physical and personnel security of the Prime Minister's Office (PMO) and the PCO.

Assistant Secretary to the Cabinet (Global Affairs)

The Assistant Secretary to the Cabinet (Global Affairs) has two major functions. The first derives from the Prime Minister's responsibility as head of government to be actively involved in the formulation and execution of foreign and defence policy. The Assistant Secretary provides the Prime Minister with advice on all major foreign and defence policy issues, and support in dealings with other heads of government and heads of state (e.g., correspondence, visits to Canada, and foreign travel). In addition, he/she deals directly, on behalf of the Prime Minister, with foreign government representatives in Canada and with senior officials of foreign leaders' offices.

Assistant Secretary to the Cabinet (Economic and Regional Development Policy)

The Assistant Secretary to the Cabinet (Economic and Regional Development Policy) is accountable for monitoring, coordinating and advising on specific issues in economic and regional development policy and trade policy and priorities, and their implications for federal-provincial relations.

The policy sector includes the following areas: energy, mines, agriculture, fisheries and oceans, forestry, science and technology, industrial and regional development, transport, communications, trade investment, competition policy, and labour. It also includes, in a broader sense, micro-economic policy issues of interest to the Government. The Assistant Secretary is accountable for the effective functioning of the Cabinet Committee on Economic and Environmental Policy and various ad hoc committees as required.

International Assessment Staff (IAS)

The International Assessment Staff (IAS) within the PCO provides government departments and agencies with original, policy-neutral assessments of foreign developments and trends that may affect Canadian interests.

4.3 Canada's role in the international intelligence community

Sharing of intelligence

Since the end of the Second World War, the Canadian intelligence community has entered into a number of bilateral and multilateral agreements related to the sharing of foreign or security intelligence with intelligence agencies in the quinquepartite ("5-eyes") intelligence community [redacted] One key element involves the agreement of members of the 5-eyes community (Canada, US, UK, Australia and New Zealand) to cooperate in the conduct of their separate SIGINT programs, including the sharing of the bulk of the collected intelligence. In addition, there is a regular exchange of assessed intelligence among the allies, including close consultation in the production of such assessments.

Collaboration

Collaboration and task sharing are of basic benefit to Canadian intelligence activities. Canada's bilateral and multilateral agreements allow access to a vast and costly process that Canada could not and would not duplicate. In addition, collaboration in the intelligence domain contributes to Canada's overall relations with the countries concerned.

Constraints

The Canadian intelligence community is faced with a number of constraints in its efforts to satisfy the needs and concerns of the Canadian government. In some areas, Canada's intelligence collection is based on the interests of Canada as a member of the Alliance, a part of "burden sharing", but recent reorientation and additional resources have focused on specifically Canadian requirements. Intelligence exchange with the Allies is constrained by national interest and availability. Policy constraints and international agreements prevent covert collection against close allies. [redacted]

4.4 History of CSE

World War II and the Examination Unit (XU)

During the Second World War, at the request of the Department of External Affairs, the National Research Council established an Examination Unit (XU) to spy on the Vichy French legation because Vichy "was suspected of propaganda activities in Quebec." The XU, created on 9 June 1941 on Montreal Road, formed a cryptographic bureau in Ottawa, primarily to work against intercepted diplomatic cipher traffic out of Ottawa.

Edward Drake and the Joint Discrimination Unit (JDU)

As the XU grew during the war, it was moved to the LaSalle Academy on the corner of Guigues Street and Sussex Drive. In 1945, it merged with DND's Y unit and became known as the Joint Discrimination Unit (JDU), headed by Lieutenant-Colonel Edward Drake. At its peak, the intercept and processing staff amounted to 1,671 military and civilian personnel.

Communications Branch of the National Research Council (CBNRC)

In September 1945, the Under-Secretary of State for External Affairs and the Chiefs of Staff decided to recommend that a national SIGINT organization be maintained in Canada in peacetime. A target was established at the beginning of 1946 for an intercept organization consisting of 100 manned positions (40 Royal Canadian Navy, 40 Army, 20 Royal Canadian Air Force) and later a proposal was made for a national SIGINT centre which became known as the Communications Branch of the National Research Council (CBNRC) with an original establishment of 179 civilians.

In May 1946, Prime Minister Mackenzie King approved the proposal which was in the form of an Order in Council over the signatures of the Ministers of National Defence, External Affairs, and

Trade and Commerce (for NRC). At the same time, the Communications Research Committee (CRC) was established to provide guidance to the national SIGINT effort. In 1948, a senior committee, the Communication Security Board (CSB), was also established to handle high-level policy matters.

In 1950, the CBNRC moved its headquarters from the LaSalle Academy to its new building, the Rideau Annex, on Alta Vista Drive. However, in 1961, it outgrew the premises and moved into its specially built facility, the Sir Leonard Tilley Building on Heron Road.

Division of SIGINT tasks

When CBNRC started in 1946, the SIGINT tasks undertaken, by arrangement with UK and US authorities, were [redacted] The basic purpose of these tasks was to provide initial training in producing intelligence from a variety of foreign communications and cipher systems.

In 1947, arrangements were made with the UK and US to take over certain aspects of the work on a [redacted]

By 1950, the main focus had shifted to work on Canadian intercepted traffic, and the [redacted]

Creation of CSE

On 1 April 1975, CBNRC was transferred to the Department of National Defence and became the Communications Security Establishment, or CSE. This came about as a result of a January 1974 CBC TV program called "The Fifth Estate: The Espionage Establishment", which revealed CBNRC's involvement with security and intelligence matters and its association with NSA and GCHQ.

CSE was established within DND as the national agency responsible for Canadian communications security (COMSEC) and SIGINT programs. While the Minister of National Defence was designated the minister responsible for CSE, CSE was established as a distinct entity within DND. CSE's "separate employer" status has made it less dependent on DND in the administrative area than CBNRC was on the NRC: for example, CSE could now do its own collective bargaining, job classification, hiring and other such administrative functions.

In early 2008, CSE changed its name to CSEC, in line with the Federal Identity Program of the Government of Canada, which requires all federal agencies to have the word *Canada* in their name.

Late Cold-War Period

[redacted]

Throughout the 1990s, as CSE moved further away from its Cold War focus, the pace of change in the telecommunications world shifted from evolutionary to revolutionary. New technologies proliferated. The volume, variety and velocity of communications increased exponentially. The routing of messages became unpredictable – "anything could be anywhere" in the new communications landscape. At the same time, budget and human resources cutbacks impaired CSE's ability to keep up with the changing world.

9-11 and the *Anti-terrorism Act*

The terrorist attacks of 11 September 2001 fundamentally changed the way security issues are dealt with in North America. These events were a wake-up call for Canada and a turning point for CSE. Up to this time, CSE was legally prevented from targeting any communication where there might be a possibility of intercepting a Canadian "private communication," which is defined in Canada's Criminal Code as any communication that originates or terminates in Canada, where there is an expectation of privacy. When the target was the Soviet Union, there was little risk of intercepting private communications. But with globalization and the Internet, CSE had no way of ensuring that its foreign targets' communications did not originate or terminate in Canada. Although CSE had the technical capability to collect foreign intelligence, it legally had some constraints.

The Chief of CSE at the time, Keith Coulter, was informed by his General Counsel Solicitor-Clien

Solicitor-Client Privilege

CSE and Department of Justice drafters worked through a three-week-long session, developing new concepts in Canadian law – including the regime of Ministerial Authorization – to resolve the matter of the interception of private communications so that CSE could be empowered to carry out its mandate.

Cabinet Confidence

CSE's new legislation was included into the *Anti-terrorism Act*, which was tabled in Parliament on October 15, 2001. It was passed in record time and came into force on December 24, after making its way through committee hearings in the House of Commons and the Senate.

The *Anti-terrorism Act* impacted CSE in two important ways: it provided CSE with a legislated mandate, and it filled an authority gap that enabled CSE to engage in the war on terrorism. Under its legislated mandate, CSE engages in three broad areas of activity: collection of foreign intelligence ("Part A"), protection of electronic information ("Part B"), and assistance to federal law enforcement and security agencies ("Part C"). Under Ministerial authority, when directing its activities at foreign entities abroad, CSE could now conduct operations even if doing so risked acquiring private communications of Canadians as well. When this occurs, the Act allows CSE, in cases where a strict set of conditions is met, to use and retain these communications. Otherwise, upon recognition, they are deleted. Similarly, CSE may now obtain a Ministerial Authorization to carry out essential IT Security activities that run the risk of intercepting private communications. In support of the commitments outlined in the *National Security Policy*, CSE has greatly increased its focus on security issues. CSE now devotes the majority of its foreign intelligence efforts to gathering and reporting intelligence on issues such as [redacted] CSE also supports deployed Canadian Forces operations abroad. Consistent with the objectives of the *National Security Policy*, CSE is focusing ever more sharply on helping the Government protect its most critical information and networks.

Intelligence provided by CSE has been directly responsible for helping to protect Canadian troops in Afghanistan from terrorist attack. CSE has also provided intelligence on foreign terrorist targets used to protect the safety and interests of Canadians and our closest allies. This was intelligence that CSE would not have been able to acquire without the *Anti-terrorism Act*. Similarly, CSE's IT Security program has used Ministerial Authorizations to ensure that Government of Canada computer systems and networks are better protected from cyber attack.

CSE Historical Society

More about CSE's history can be found on the CSE Historical Society's webpage. This is a volunteer organization, which anyone can join and contribute to. See [redacted]

4.5 A History of Intelligence Agreements

1940

The Ogdensburg Treaty formalized the means and methods to coordinate North American security and information sharing. United States/Canadian intelligence cooperation began in October 1941 when the Canadians offered the US Federal Communications Commission free access to the product

of Canadian wireless monitoring activities. In return, the US gave Canada technical direction-finding (DF) data that subsequently made significant contributions to the Allied North Atlantic Ocean surveillance network. This was the beginning of Canada's SIGINT capability.

1945

Britain and the US agree on a SIGINT accord known as **BRUSA** (later known as UKUSA). The BRUSA bilateral agreement provided for sharing material with other Commonwealth countries, and for a special Canada/US link and task-sharing. The agreement was signed 5 March 1946.

1946

Commonwealth Signals Intelligence Conference, February 22 to March 8

After the end of World War II, the US and the four "old commonwealth" countries (UK, Canada, Australia and New Zealand) decided that signals intelligence provided material of such value that it should not be abandoned. The effort required was so great that wartime cooperation in allocating targets had to be continued. The agreement resulting from this conference achieved that objective and provided for future cooperation. One of the recommendations of the conference was:

> "SIGINT centres and intercept stations, existing or established, will not be regarded solely as part of the intelligence organization of the country or command in which they are situated, but will also form part of a SIGINT scheme in the interests of the Commonwealth as a whole."

Authority: In consultation with other Canadian authorities, the Under-Secretary of State for External Affairs (USSEA) approved the negotiation of the arrangements set out in the conference recommendations. He presumably kept the Prime Minister informed, but there is no record of this.

1948

Formal 5-eyes SIGINT agreement reached; minor changes from the BRUSA agreement.

1949

Canada/US Signals Intelligence Agreement (CANUS)

This agreement formalized the arrangements under which Canada and the US had been cooperating. The agreement was to govern COMINT relations between the two countries on behalf of the existing and any successor COMINT authorities. Exchange of material and information was to be adequate to meet national requirements, and in particular the intelligence product was to be exchanged to meet the intelligence requirements of the agencies represented by each authority.

Authority: With the approval of the USSEA, the Chairman of the Communications Research Committee exchanged letters with the Chairman, United States Communications Intelligence Board. Appendices covering security principles and technical implementation were agreed later in 1949.

1957

Tripartite Alerts Agreement

Formalized existing arrangements among Canada, the US and the UK for automatic and rapid exchange of intelligence indicating the intention on the part of any Communist country to initiate hostilities in the NATO area, with a provision for channels of communication on a continuous 24-hour basis.

Authority: With the agreement of the Prime Minister, SSEA and Minister of National Defence, an exchange of letters took place in Washington between the Canadian and UK Ambassadors and the Secretary of State. This was confirmed in London and Ottawa, and constitutes a formal international agreement.

Agreements with US and UK intelligence authorities were made whereby Canada undertook to bear the main responsibility for the collection and analysis of SIGINT on [redacted] The original trilateral CANUKUS agreement has been extended to include Australia and New Zealand and involves not only the exchange and exploitation of intelligence on Communist countries, but also on the most important strategic areas of the world.

1960

Tripartite Alerts Agreement Extension

Amendment to the 1957 agreement to cover exchange of intelligence in the event of any "Sino-Soviet Bloc" aggressive action, whether or not such action seemed likely to affect the area (i.e., provided for consultations on threats to world peace).

Authority: Prime Minister approved, with agreement of SSEA and Minister of Defence, an exchange of letters between Canadian and UK Ambassadors in Washington and the US Secretary of State, constituting a further formal international agreement.

1965

Bilateral Canada-US agreement on consultation in relation to situations which might lead to the outbreak of hostilities involving North America and concerning procedures relating to the authorization of the Commander-in-Chief of NORAD for the operational use of nuclear weapons.

CHAPTER 5: ANALYST APPLICATIONS

Most analyst applications are used for traffic scanning, reporting, research and target development.

The repertoire of analyst applications is in a constant state of flux, with new tools emerging, old tools being decommissioned, and revisions and upgrades occurring constantly. The list of tools presented in this section is a current snapshot of some of the more important and frequently used tools. A fuller list with more complete descriptions can be found on the [redacted] search "Tools".

In addition to the tools listed below, the CSE Intranet and Extranets are valuable research resources for personal, professional, and organizational reasons. The CSE **Intranet** offers analysts access to [redacted]

The CSE homepage [redacted] Analysts have access to the [redacted] the homepages of [redacted] education, as well as virtually all of CSE's policies, directives, manuals, and other traditionally "paper" products.

Through the CSE Intranet homepage, analysts are also able to access the various [redacted] Government of Canada **Extranets**. These include the [redacted] and CTSN, the Canadian Top Secret Network.

5.1 Catalogue of Tools

[redacted]

[redacted]

[redacted]

CTSN

The Canadian Top Secret Network (CTSN, previously called MANDRAKE) is CSE's secure online link with its Government of Canada partners in the security and intelligence community. Available only in the National Capital Region at the TS//SI//TK level, CTSN provides e-mail connectivity and provides an electronic intelligence dissemination network using web technology.

[redacted]

CTSN also includes a powerful search function from the main CTSN page, where users are able to search for [redacted] in each of the five member departments, as well as in other related GC departments like the RCMP, the Department of Justice, Citizenship and Immigration Canada (CIC), and the Canada Revenue Agency (CRA).

[redacted]

[redacted]

[redacted]

[redacted]

IRRELEVANT

[redacted]

[redacted]

[redacted]

[redacted]

MANDRAKE

See CTSN.

[redacted]

[redacted]

[redacted]

[redacted] is CSE's end-product report (EPR) database and report creating tool, and contains the EPRs that CSE produces and that CSE receives from Second Parties. Using [redacted], analysts can search and scan reports, draft and release new reports, create intelligence items, and review feedback on reports.

[redacted] It is the first-line resource for gathering information and for assessing reportability of potentially new intelligence.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

See [redacted]

For more information on analyst applications, see the [redacted] entry **SIGINT Tools**.

CHAPTER 6: ANALYST DUTIES

6.1 Overview

Reporting

One of the main responsibilities of the DGI analyst, particularly of those in [redacted] is to produce foreign intelligence reports on [redacted] issues pertaining to [redacted] that are of interest to the Canadian government. To accomplish this, the analyst must be able to analyze, interpret and assess the intelligence value of collected traffic, and to maintain a good background knowledge of various global issues. In addition, a majority of [redacted] require the analyst to develop and maintain language skills through self-study, courses, and/or reading magazines and other foreign language material.

Once the research and analysis has been completed, the analyst writes an EPR (=end-product report) using [redacted], CSE's SIGINT reporting tool. These reports may be limited to Canadian clients, such as CSIS, the PCO or DFATD, or may be disseminated throughout the 5-Eyes community.

Targeting

Analysts are assigned [redacted] In some cases these [redacted] in other cases, the [redacted]

Within a [redacted] identified as entities of interest, i.e., targets. Selectors (e.g., phone numbers, e-mail addresses, IP addresses) are associated with these entities and targeted in [redacted] Analysts will often seek out these selectors and target (and detarget) them as necessary, in order to collect (intercept) communications to and from these entities.

Analysts are responsible for reporting on these targets on the basis of intercepted communications. They must eventually develop a sound knowledge of related current events, Government of Canada requirements (GCRs), volume and type of traffic received, and the reportability of the intercepted communications.

Scanning

Once a selector is targeted, the analyst scans the traffic database (CTR, or Consolidated Traffic Repository, accessed through [redacted] for reportable intelligence. In addition, classified and open-source publications are scanned for content that may provide background information and augment the intelligence. Scanning, therefore, plays a major role in much of the analyst's activities.

SIGINT Development

Another aspect of an analyst's duties is SIGINT Development (SD). SD is the set of activities and processes that enable access to foreign intelligence in the global network. The analyst is responsible for knowing as much information as possible about the target to help the SIGINT system [redacted] collect data for the analyst to provide intelligence to clients. Any information indicating [redacted] is essential for the end-to-end SIGINT system to find [redacted] the target. An analyst's SD activities may include, but are not limited to:

- [redacted]
- [redacted]
- [redacted]

Other duties

In addition to scanning, reporting, and SD duties, analysts are required to always be on the lookout for keywords and new selectors that could be submitted for targeting. Such information can be obtained by having CROs request that their clients provide them with [redacted]

When time allows, DGI analysts also update existing working aids and develop new ones that pertain to their tasks. An example of a working aid that analysts can and should continually consult and update is the [redacted] Analysts are encouraged to develop any working aids that may help them or others with their tasks.

6.2 Scanning

Scanning EPRs

The analyst scans end-product reports (EPRs) in [redacted] on a daily basis in order to:

- be informed of recent developments in current issues and specifically in matters relating to his/her targets,
- see what CSE's [redacted] especially on his/her targets,
- see what other areas in DGI are reporting to maintain a general knowledge of all DGI reporting, and
- verify that a report he/she issued the previous day is in the database with no errors; if there is an error a correction or cancellation may be required.

The analyst also scans for clients' feedback on the analyst's reporting line, which may provide valuable information that influences future reporting. Feedback often reveals the areas of heightened interest or concerns about timeliness, relevance, or other factors.

Scanning open-source material

Analysts are expected to stay abreast of developments in their area of responsibility through newspapers, journals and other non-classified sources. Such research is essential to their understanding of a topic and their ability to follow developments, including changes in terminology. Keeping up with open-source reporting also enables the analyst to determine the urgency of reporting on a given subject, and to eliminate or use effectively material already in the public domain.

CSE subscribes to a variety of English and foreign language newspapers and journals, and analysts are expected to read these regularly. They can have their names added to distribution lists for these publications by contacting Library Information Services. Analysts are also encouraged to suggest additional publications to which CSE could subscribe.

Most units have shared laptop computers with [redacted] available for [redacted] research. The CSE Library can also conduct searches on request, through access to outside libraries and online databases. Analysts usually get the required [redacted] briefing and indoctrination soon after joining DGI.

[redacted] is the office that [redacted]

Scanning traffic

Analysts use [redacted] application, [redacted] fax, [redacted] The traffic is stored in [redacted] Consolidated Traffic Repository (CTR).

[redacted]

[redacted]

The Office of Cryptologic Studies (OCS) provides several modules of online training for [redacted] Consult the OCS web page for more information, or contact [redacted]

Annotating traffic

In order to protect the identity of Canadians and their communications while scanning traffic, analysts must annotate any traffic where:

- one communicant (whether Canadian or not) is physically located in Canada,
- one communicant is Canadian and physically located outside Canada, or
- both communicants are foreign, located outside Canada, and the communication contains information about a Canadian person, organization or company, but that information does not constitute foreign intelligence.

Guidelines on annotating traffic can be found in OPS-1, Annex 2. More information on annotations can be found in the [redacted] under "Privacy Annotations", as well as on the DGI homepage under "Privacy of Canadians". The OCS also offers the mandatory course S286 Privacy Annotations and Sign-Off Procedures, usually scheduled twice each year.

6.3 Reporting

Reportability

The analyst's first priority (and CSE's main responsibility) is to provide foreign intelligence that supports the development and conduct of the Canadian government's foreign, defence, economic and security policies.

When deciding on the reportability of an item, the analyst must take into consideration such things as:

- Government of Canada Requirements (GCRs)
- the National SIGINT Priorities List (NSPL)
- previous reporting on the topic, either by CSE or a partner agency
- whether the information would be available through open sources
- the current reporting threshold; e.g., if the message has less intelligence value but the unit is not busy, the message can be reported; however, if everyone is very busy, the analyst may decide not to report it.

Frequently, a single piece of traffic will not provide sufficient information on which to report – it may provide only one piece of the puzzle. In such cases, the analyst must continue searching for

traffic over a period of time until there is sufficient information to put all the pieces of the puzzle together.

In the case of [redacted] reporting, CSE's first priority and main responsibility is [redacted] material, then by issues of interest to Canada. If a piece of traffic is reportable but is not CSE's main reporting responsibility, second-party agencies, e.g. NSA, should be consulted by [redacted] phone or e-mail to [redacted] However, if the material is particularly sensitive for Canada, the analyst will forego contacting the second-party agency and issue the report as Canadian Eyes Only (CEO).

Translation

SIGINT traffic in a foreign language must be translated into English before it is reported. The act of translating obliges the translator/reporter to clarify points in the original language which may be vague and therefore open to interpretation. The role of the translation quality controller, another analyst competent in the language, is to ensure that the correct interpretation of the original text has been rendered into proper English. As a result, the translator should produce a polished, accurate translation to demonstrate that the concepts and nuances of the original text have been properly understood and idiomatically reformulated. (In some cases, analysts may be granted an exemption and draft the report without first doing a translation.)

[redacted]

Besides dictionaries and linguistic working aids, there are various political reference books, end-product databases, and human resources (e.g., linguists, CROs, the CSE librarian) that the analyst can turn to for help to ensure that he/she has a good understanding of the subject at hand and produces an accurate translation.

If a translation specialist is not available, analysts can also use machine translation applications for producing a rough gist of [redacted] which ideally will provide a good enough English rendition to determine if the traffic is potentially useful. A fuller translation can then be requested from a linguist analyst if warranted. CSE currently uses [redacted]

[redacted] into English, as well as identifying an unknown language. (For sensitive translations that should remain CEO, a [redacted] version is also available; see the [redacted] entry under [redacted] for access information.)

Analysts may also provide translations to other SIGINT groups (particularly [redacted] Data Analysis and Enrichment [redacted] for Cryptologic Intelligence Reports (CIRs). Analysts are also asked to bring any reportable CIR items that they come across in their scanning to the attention of the respective groups. CIR material includes information such [redacted]
Although CIR translations are usually short and seem straightforward, they are often difficult to do because they can be quite technical.

Reporting

The analyst reports the intelligence in the traffic according to the reporting guidelines (see in particular CSOI-4-1 *SIGINT Reporting*). It is the analyst's responsibility to write an objective and accurate report, and verify the accuracy or meaning of anything in the original text that may be ambiguous (e.g., the accuracy of a title, the expansion of an abbreviation, [redacted]

Once the report has been written, it is (1) reviewed by one or more editors who verify and confirm that it conforms to all legal and policy guidelines, (2) returned for corrections, and (3) approved for release by the appropriate authority. Once released, the report will appear in [redacted] and can be accessed by all valid recipients, including Client Relations Officers (CROs) who can select it to show to interested clients within the Government of Canada.

APPENDIX: Commonly Used Acronyms at CSE

[redacted]	
ADCS	Associate Deputy Chief SIGINT
ADM	Assistant Deputy Minister
[redacted]	
[redacted]	
ATIP	Access to Information and Privacy
ATK	Analyst Tool Kit
[redacted]	
[redacted]	
BRLO	British Liaison Office
[redacted]	
CAG	Collective Address Group
CANSLO	Canadian Special Liaison Office
[redacted]	
CAP	Counseling Advisory Program
CAPIA	Canadian Association of Professional Intelligence Analysts
[redacted]	
CBSA	Canada Border Services Agency
[redacted]	
CCSE	Chief CSE
CDI	Chief of Defence Intelligence (DND) (formerly DGINT)
[redacted]	
CEO	Canadian Eyes Only
CFEWC	Canadian Forces Electronic Warfare Centre
CFIOG	Canadian Forces Information Operations Group
CFJIC	Canadian Forces Joint Imagery Centre
CFSOC	Canadian Forces SIGINT Operations Centre
[redacted]	
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIR	Cryptologic/Communications Information Report
CM	Collection Management
[redacted]	
COI	Community of Interest
COMINT	Communications Intelligence
COMPUSEC	Computer Security
[redacted]	
COMSEC	Communications Security
CONOP	Concept of Operations
COPCC	CSE Operational Production and Coordination Centre
[redacted]	
CRM	Client Relations Management
CRO	Client Relations Officer
[redacted]	
CSIS	Canadian Security Intelligence Service
CSOI	Canadian SIGINT Operations Instruction
CT	Counter Terrorism
CVAN	CSE Visitor Access Notification
[redacted]	
[redacted]	
CWW	Compressed Work Week
DDI	Delivery Distribution Indicator
DFAIT	Department of Foreign Affairs and International Trade (formerly FAC and ITCan; now DFATD)
DFATD	Department of Foreign Affairs, Trade and Development Canada (formerly DFAIT)
DFO	Department of Fisheries and Oceans
DGA	Directorate General, Access
DGI	Directorate General, Intelligence
DGINT	Director General Intelligence (DND) (now CDI)
DGP	Directorate General, Programs
DGPC	Directorate General, Policy and Communications
DLS	Directorate of Legal Services
DM	Deputy Minister
DND	Department of National Defence
DNI	Digital Network Intelligence
[redacted]	
DNR	Dialed Number Recognition
DOE	Division of efforts
DSD	Defence Signals Directorate (Australia)
[redacted]	
ECI	Exceptionally Controlled Information
ELINT	Electronic Intelligence
EPR	End-Product Report
ExCom	Executive Committee
FAC	Foreign Affairs Canada (now DFATD)

FAMIS	Financial and Asset Management Information System
FBIS	Foreign Broadcast Information Service
FI	Foreign Intelligence
FIPS	Foreign Intelligence Priorities
FISA	Foreign Intelligence Surveillance Act (US)
FISINT	Foreign Instrumentation Intelligence
[redacted]	
FTE	Full Time Equivalent
FTP	File Transfer Protocol
G&O	Goals and Objectives
GC	Government of Canada
GCHQ	Government Communications Headquarters (UK)
GCR	Government of Canada Requirement
GCSB	Government Communications Security Bureau (New Zealand)
GII	Global Information Infrastructure
[redacted]	
[redacted]	
GSA	Global Security Agenda
[redacted]	
GSO	Group Security Officer
GUI	Graphical User Interface
GWOT	Global War On Terrorism
[redacted]	
HOM (or HoM)	Head of Mission
HR	Human Resources
HRM	Human Resource Management
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HUMINT	Human Intelligence

HVCCO	Handle Via COMINT Channels Only
I&W	Indications and Warnings
IAC	Intelligence Advisory Committee
ICSI	Interdepartmental Committee on Security and Intelligence
IED	Improvised Explosive Device
IEG	Interdepartmental Experts Group
IM/IT	Information Management/Information Technology
[redacted]	
INFOSEC	Information Security
[redacted]	
IO	Information Operations or Intelligence Officer
IP	Internet Protocol
IPG	Intelligence Priorities Group
[redacted]	
ISAF	International Security Assistance Force
ISDN	Integrated Services Digital Network
[redacted]	
ISP	Internet Service Provider
ITAC	Integrated Threat Assessment Centre
ITCan	International Trade Canada (now DFATD)
ITS	Information Technology Security
JESI	Joint Executive for SIGINT Interoperability
JINTAC	Joint International Terrorism Activity Cells
L&D	Learning & Development
LAN	Local Area Network

LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agency
LESA	Law Enforcement and Security Agencies
[redacted]	
LO	Liaison Officer
MC	Memorandum to Cabinet
[redacted]	
MOU	Memorandum Of Understanding
[redacted]	
MSN	Microsoft Network
MTF	Management Team Forum
[redacted]	
NDHQ	National Defence Headquarters
[redacted]	
NRRB	New Requirements and Request for information Review Board
NSA	National Security Advisor (Canada)
NSA	National Security Agency (US)
[redacted]	
OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness (now PSEPC)
[redacted]	
OCR	Optical Character Reader/Recognition
OCS	Office of Cryptologic Studies (formerly OSS)
OCT	Office of Counter Terrorism
OGD	Other Government Department
OPI	Office of Primary Interest

ORCON	Originator Controlled
[redacted]	
OSS	Office of SIGINT Studies [redacted]
PCO	Privy Council Office
PCO-IAS	Privy Council Office – Intelligence Assessment Secretariat
PDA	Personal Digital Assistant
[redacted]	
PID	Portable Information Device
PIQ	Position Information Questionnaire
PKI	Public Key Infrastructure
[redacted]	
PLM	Product Line Manager
PM	Production Manager or Prime Minister
PMO	Prime Minister's Office
[redacted]	
PPR	Performance Planning and Review
PSAT	Public Safety and Anti-Terrorism
PSEP	Public Safety and Emergency Preparedness (replaced OCIPEP)
PSEPC	Public Safety and Emergen Preparedness Canada
[redacted]	
RCMP	Royal Canadian Mounted Police
[redacted]	
RFC	Request for Comment
RFI	Request For Information
ROPI	Responsible Office of Primary Interest
S&I	Security and Intelligence
[redacted]	
SA	Special Access

SAFP	SIGINT Adjunct Faculty Program
SAGA	Strength and Gap Analysis
[redacted]	
SD	SIGINT Development
SEAM	Senior Executive Account Manager
SI	Security Intelligence or Special Intelligence
[redacted]	
[redacted]	
SIGINT	Signals Intelligence
SLA	Support to Lawful Access
SLE	Support to Law Enforcement
SME	Subject Matter Expert
SMO	Support to Military Operations
[redacted]	
SMT	Senior Management Team
[redacted]	
SOLGEN	Solicitor General
[redacted]	
SRCL	Security Requirements Check List
[redacted]	
[redacted]	
STE	Secure Terminal Equipment
SUSLOO	Special US Liaison Office Ottawa

SWE	Salary Wage Envelope
SWOT	Strengths, Weaknesses, Opportunities, Threats
[redacted]	
TAG	Topic and Area Guide
[redacted]	
[redacted]	
TDY	Temporary Duty
TK	Talent-Keyhole
TL	Team (or Task) Leader
[redacted]	
TSSA	Top Secret Special Access
[redacted]	
VBIED	Vehicle-Borne Improvised Explosive Device
[redacted]	
VRK	Very Restricted Knowledge
[redacted]	
WMD	Weapons of Mass Destruction
WTR	Write-to-Release
[redacted]	

Index