Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSSS-100

Canadian SIGINT Security Standards

The overall classification of this document is SECRET

SIGINT

Canada

146552-v6

EFFECTIVE DATE

The effective date of this version of CSSS-100, *Canadian SIGINT Security Standards* is:
2 September 2011.

RECORD OF AMENDMENTS

Amendment No.	Date of Amendment	Date of Entry	Entered By

Table of Contents

CHAPTER 1

INTRODUCTION

1.1 Introduction

1.1.1 Contents

This chapter contains the following topics:

Topic
1.1 Introduction
1.2 Authorities
1.3 What is SIGINT?
1.4 CSEC and the CSSS
1.5 Application

1.1.2 Objective

The objective of the *Canadian SIGINT Security Standards* (CSSS) is to ensure consistent protection of Signals Intelligence (SIGINT) disseminated to and used by affected Government of Canada (GC) departments and agencies. The CSSS are issued under the authority of the Chief of the Communications Security Establishment Canada (CSEC).

1.1.3 Contents of the CSSS

CSSS covers all aspects of SIGINT security including:

- Special Intelligence (SI)[1] classification and markings;
- departmental requests for access to SI;
- SI handling procedures;
- Electronic Intelligence (ELINT) and Foreign Signals Instrumentation Intelligence (FISINT) handling procedures;
- the SIGINT Information Technology (IT) and Physical Security certification and accreditation process;
- personnel security related to the indoctrinations required to work with SIGINT; and
- information security for SIGINT systems.

Additional documentation concerning the protection and control of SIGINT is contained in the CSSS-100 series[2] of policy instruments (all of those that are referenced in this document are available on the CSEC page on the Canadian Top Secret Network (CTSN)[3] central site), which supplement CSSS when more detailed information is required on specific subjects.

[1] Special Intelligence (SI) replaces the COMINT control system marking, for more details see *Chapter 2: Special Intelligence Classification and Markings.*
[2] The CSSS series policy instruments will replace the former OPS-5 series of procedures.
[3] The CTSN replaces MANDRAKE.

1.2 Authorities

1.2.1 Legislative Context

Pursuant to the *National Defence Act* (NDA) (Part V.1):

- CSEC's mandate is to acquire and use information from the Global Information Infrastructure (GII) for the purpose of providing foreign intelligence, in accordance with Government of Canada (GC) intelligence priorities (NDA, Section 273.64 (1)(a)). The information so acquired and used is referred to as SIGINT.

- The Chief of CSEC (CCSEC), under the direction of the Minister of National Defence or any person designated by the Minister, has the management and control of the Establishment and all matters relating to it (NDA, Section 273.62(2)). The CCSEC is responsible for all aspects of SIGINT policy, operations and administration in Canada and affecting GC departments and agencies. The CCSEC has delegated responsibility for SIGINT security policy to the Deputy Chief, SIGINT (DC SIGINT).

1.2.2 Authority

These standards are issued under the authority of Appendix B, "Responsibilities of Lead Security Agencies," in the *Policy on Government Security* (PGS). This part of the policy identifies CSEC as the Government of Canada's national authority for SIGINT. As such, CSEC is the lead agency responsible for SIGINT security in Canada.

1.2.3 National Authority for SIGINT

CSEC is the only Canadian organization authorized to:

- collect SIGINT for foreign intelligence purposes; and
- conduct liaison with Canada's cryptologic allies.

1.2.4 Policy

Consistent with the PGS, the following principles must be followed in the application of these standards:

- there must be a balance between the use of SIGINT and the requirement to protect it - risk management should be used to achieve this balance;
- where possible, CSEC will delegate responsibility for SIGINT accreditation to departments and agencies who have the capacity to exercise such functions (see *Chapter 6: SIGINT Certification and Accreditation*); and
- CSEC will adopt a service-oriented approach in the delivery of advice and assistance to client departments and agencies.

1.3 What is SIGINT?

1.3.1 What is SIGINT?

The term SIGINT potentially covers a wide range of activities; within this document SIGINT refers to the following:

- SIGINT is information or intelligence intercepted or acquired from the GII and other communication and non-communication sources;
- SIGINT activities and methods refer to the acquisition, processing, analysis, reporting, and dissemination of information or intelligence from the GII and other communication and non-communication sources. This can involve traditional interception and processing methods as well as alternative techniques designed to collect or enable the acquisition or processing of information from specific information systems and communications; and
- SIGINT comprises, either individually or in combination, COMINT, ELINT and FISINT.

1.3.2 Why protect SIGINT?

SIGINT, and in particular COMINT, is vulnerable to easily applied countermeasures. Hence, the CSSS is primarily concerned with the protection of COMINT. ELINT and FISINT generally require less restrictive handling, and are addressed separately in *Chapter 5: Protection of ELINT and FISINT*. When security measures are intended to apply to all three components, the term SIGINT will be used; otherwise the terms COMINT, ELINT and FISINT will be used separately.

1.4 CSEC and the CSSS

1.4.1 CSEC and the CSSS

CSEC's unique role as the national GC agency that produces SIGINT reports and manages the distribution and handling of SIGINT has the following implications:

- CSEC is responsible for producing the CSSS, which is a set of standards to ensure the protection of SIGINT in GC departments and agencies;
- CSEC is empowered to authorize other GC departments or agencies to either retain and/or process SI or to receive SI read-only service (using processes described in *Chapter 3: Departmental Requests for Access to Special Intelligence*); and
- CSEC is required to carry out the provisions contained in the CSSS. However, because of its role as the producer of SIGINT, the responsibilities assigned to specific position-holders (e.g. the Senior Indoctrinated Official (SIO), COMINT Control Officer (COMCO), IT Security Coordinator (ITSC), etc.) in GC organizations may be structured differently in CSEC (e.g. duties assigned to a COMCO may be distributed across various position-holders or business areas rather than being discharged by a single person).

The contact at CSEC for questions related to any of the provisions contained in the CSSS is the SIGINT Security Management Office (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN). This office will direct questions to the person or area in CSEC best able to answer them.

1.5 Application

1.5.1 Who can receive SIGINT?

Any department or agency of the GC is eligible to receive SIGINT; the GC means a federal institution, as defined in subsection 3(1) of the *Official Languages Act*. In the CSSS, GC departments and agencies that are accredited to receive and retain SIGINT are referred to as Authorized Organizations; those that are not so accredited are referred to as Client Organizations.

1.5.2 Application

The CSSS are applicable to all Canadian organizations and individuals authorized to have access to SIGINT information and assets.

1.5.3 What happens if standards are not applied?

The consequences of not applying these standards could include:

- security breaches or violations leading to the loss or compromise of classified information, intelligence sources or other assets;
- breaches of international agreements which provide for the exchange of intelligence or intelligence technology;
- the withdrawal of services from and loss of access to SIGINT by the offending agency and/or individual(s); and
- possible prosecution under the *Security of Information Act* (SOIA) since SIGINT may constitute special operational information as defined under that *Act* (see *Chapter 4: Protection of SIGINT Information* for more information on safeguarding SIGINT).

1.5.4 Enquiries

The Manager of the SIGINT Security Management Office at CSEC should be contacted about all questions that relate to these standards (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN).

CHAPTER 2

SPECIAL INTELLIGENCE CLASSIFICATION AND MARKINGS

Chapter 2: Special Intelligence Classification and Markings

2.1 Introduction

2.1.1 Contents

This chapter contains the following topics:

2.1.2 Purpose

In accordance with the objectives of the *Policy on Government Security* (PGS) to ensure that GC information is safeguarded from compromise, classified information must be marked or otherwise identified at the time it is created or collected, to alert those who use it that it must be protected at the applicable level. The originator of information is responsible for applying the classification marking to the material. This chapter should be used by readers as a guide to assist in correctly classifying, and if necessary, adding control markings to documentation.

Note: CSEC document CSSS-103, *The SIGINT Classification System*, provides details on different classification markings. CSSS-103 is available from the CSEC page on the CTSN central site.

2.1.3 What is SIGINT?

Signals Intelligence (SIGINT) is technical information and/or intelligence comprised of (individually or in combination) communications intelligence (COMINT), electronics intelligence (ELINT) and foreign instrumentation signals intelligence (FISINT).

2.1.4 Classifying COMINT

SIGINT is classified as prescribed in this document. The control systems and special markings described in this chapter normally only apply to information protected by the Special Intelligence (SI) control system (see section 2.2.2). Other types of SIGINT, notably ELINT and FISINT, are normally classified only in the national interest, e.g. SECRET, with no special control systems required. (See *Chapter 5: Protection of ELINT and FISINT* for information on the handling of ELINT and FISINT.)

2.1.5 General Principles

Safeguarding classified and protected information is the responsibility of everyone holding a security clearance. The following list provides some basic principles for the classification of information:

- SI, particularly Exceptionally Controlled Information (ECI) and GAMMA, may be considered "Special Operational Information", as defined in and protected by the *Security of Information Act* (SOIA);
- information "originators," i.e. SIGINT elements, are responsible for setting the classification level of their sources, methods, or reports (in consultation with intelligence partners or Second Party counterparts, where necessary);
- authorized consumers of information who believe that the classification is not correct are encouraged to challenge the originator regarding the classification;
- classified information provided by allies is safeguarded in the same way as Canadian classified information and vice versa (see section 2.6); and
- conditions concerning further dissemination and control of proprietary information or sensitive allied information are respected.

2.1.6 Who Can Help?

The following officials within Authorized Organizations can be or should be consulted:

- a Senior Indoctrinated Official (SIO);
- a COMINT Control Officer (COMCO);
- a Deputy COMCO (D/COMCO); and
- an Information Systems Security Officer (ISSO) where SIGINT-related systems are present.

If the Authorized Organization wishes to store GAMMA, it must also appoint a GAMMA Control Officer (GCO). This can be the same person as the COMCO or the D/COMCO.

Authorized Organizations that do not rely entirely on electronic storage of SI must also establish within the SIGINT Secure Area (SSA), a registry system to receive, distribute, and store SIGINT, specifically SI, separately from other classified non-SI information. The individuals listed in this paragraph can provide advice and guidance in any areas related to the protection of SIGINT. Their specific duties are discussed in *Chapter 3: Departmental Requests for Access to Special Intelligence*.

2.2 The Special Intelligence Control System

2.2.1 Control Systems

Control systems are in place in Canada and in the countries of its SIGINT partners to give additional protection to classified information derived from or concerning sensitive sources, methods or techniques. An "indoctrination" consisting of a formal briefing and a signed acknowledgement is required before accessing any information protected within a control system. Such information is known as "compartmented information".

The control systems in use within Canada are:

- Special Intelligence (portion marking is **SI**); and
- TALENT KEYHOLE (portion marking is **TK**).

2.2.2 The Special Intelligence Control System

The Special Intelligence control system refers to a method that is used to ensure the secure handling and control of intelligence derived from communications intelligence. SI control system markings must be applied to information that, if compromised, could injure national interests. The SI control system must not be used as a means of providing increased security for non-SI information.

Note: In May 2011, the US Controlled Access Program Coordination Office (CAPCO) obsoleted 'COMINT' as a control system marking and replaced it with 'SI'. Following CAPCO's decision, CSEC is now using the 'SI' control system marking to protect COMINT information, and the COMINT control system is now the Special Intelligence control system. While these changes affect the use of COMINT as a control system marking or the name of a control system, COMINT remains the appropriate abbreviation for communications intelligence as a discipline.

2.2.3 Special Intelligence Sub-Control Systems

SI derived from or referring to especially sensitive sources and methods may be further compartmentalized and disseminated to a limited number of recipients on a strict need-to-know basis. SI sub-control system markings are used for this purpose; they include GAMMA and ECI, both of which may **only** be classified in the national interest at the TOP SECRET level, e.g. ECI can never be simply SECRET.

2.2.4 Originator Controlled (ORCON)

ORCON is a US dissemination control marking added to SIGINT information to indicate that dissemination beyond listed addressees is subject to approval by the originator of the report.

CSEC Operational Policy [redacted]@cse-cst.gc.ca on CTSN) must be notified and asked to obtain approval for actions taken with regard to SIGINT reports issued by Second-Party agencies (i.e. DSD, GCHQ, GCSB and NSA) that are marked ORCON and that will be disseminated outside Canada to organizations that are not on the original dissemination list.

2.3 Determining What to Classify

2.3.1 What Materials are SI?

Material that contains COMINT must bear the security classification appropriate to the most highly classified COMINT included, as well as any associated sub-control and/or dissemination control markings as appropriate. The following are some examples of the types of material that may be classified SI (the list is not exhaustive):

- papers;
- documents;
- assessments;
- summaries;
- briefings;
- reports
- data; and/or
- essential elements of information.

Additionally, any format in which such SI classified material may be stored, e.g. paper or soft copy, diskette or cd-rom, should be marked with the classification of the most sensitive information contained in or on such media. SI conversations via a secure communications device are also technically considered classified.

2.3.2 Classifying E-mail, Electronic Calendar Entries and Attachments

E-mail and electronic calendar entries should bear the classification and control markings relevant to the content, including attachments. E-mail and electronic calendars must not contain information classified any higher than that to which the IT system or network is accredited. All users of a system or network should be aware of the highest possible classification of data allowed on the system.

E-mails or electronic calendar entries referring to the URLs of classified websites do not need to be classified unless:

- the content of the e-mail itself or an attached document requires classification; or
- the website URL itself discloses classified targets, sources or methods.

Signature blocks of e-mails must be unclassified and must not refer to identifiable sources, targets or intelligence-gathering methods.

2.3.3 Classifying Non-SI Information

The classification of material that does not contain SI, but is related to COMINT and COMINT activities, often presents problems for the originator in determining which classification to apply. Although such documentation may not contain SI, it may nevertheless require SI protection because if it were compromised, it could cause injury to national interests, specifically to COMINT activities, such as the loss of a valuable COMINT source. Therefore, a document which:

- indicates or implies success in the production of COMINT; and/or
- concerns a COMINT technique; and/or
- reveals the scale and direction of the COMINT effort to a degree that might result in countermeasures

must bear the security classification appropriate to the most highly classified COMINT to which it relates.

Examples:

- details of the nature and extent of COMINT collaboration with Second Parties or other governments; and
- the fact that a GC department or agency is a SI consumer.

2.3.4 Classifying Information Referring to COMINT

On some occasions, information that is not strictly SI may still reveal enough detail about COMINT activities to warrant protection in the national interest, such that the use of dissemination markings is appropriate. This information must be protected in the same manner as material that actually contains SI.

Examples:

- correspondence concerning lists of SIGINT-indoctrinated and de-indoctrinated personnel;
- COMINT procedural documentation; and
- administrative details such as safe combinations, or passwords used to access systems handling/storing, or processing SI.

2.4 Classifying Information

2.4.1 National Classification Levels

As indicated in the PGS (section 3.1), government security includes the assurance that information is protected against compromise. National classification markings are used to safeguard information and ensure its proper handling. All information must be classified according to the degree of damage to Canadian national interests that could result should this information be compromised. The creator of a document is responsible for classifying it at the appropriate level. As shown in the following table, information may be TOP SECRET, SECRET, CONFIDENTIAL or UNCLASSIFIED, depending on the damage that might reasonably be expected to occur from compromise.

If the information is…	Then the compromise could reasonably be expected to cause…
TOP SECRET	**Exceptionally grave injury** to the national interest
SECRET	**Grave injury** to the national interest
CONFIDENTIAL	**Injury** to the national interest
UNCLASSIFIED	**No injury** to the national interest

2.4.2 What is Meant by Injury?

Each GC department or agency that receives or handles classified material will have its own possible consequences from the compromise of such assets. The following table is intended only to provide some examples of likely consequences. The list is not exhaustive.

Compromise of assets marked…	Consequences
TOP SECRET	• threat to the stability of Canada or friendly nations • loss of life • exceptionally grave damage to the effectiveness or security of Canadian or allied forces • exceptionally grave damage to relations with friendly governments • exceptionally grave damage to the effectiveness of extremely valuable intelligence operations • severe long-term damage to the Canadian economy
SECRET	• increased international tension • serious damage to international relations • serious damage to the operational effectiveness of the Canadian Forces • serious damage to valuable intelligence operations • significant threats to the national critical infrastructure • serious damage to civil order
CONFIDENTIAL	• damage to Canada's diplomatic relations • damage to the operational effectiveness of the Canadian Forces • damage in the short term to economic interests • damage to the effectiveness of intelligence operations

2.4.3 Constructing a Classification Line

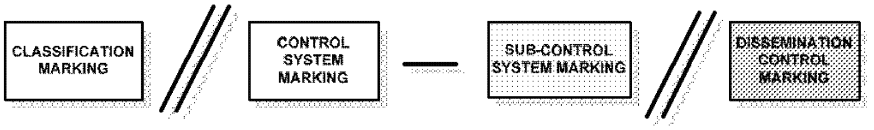
For SI information, the classification line normally consists of three components:

- classification in the national interest;
- control system and possibly sub-control system markings; and
- dissemination control markings.

The components are separated by a double slash, i.e. "//". Control, sub-control, and dissemination control markings distinguish SI from information classified solely in the national interest.

A typical classification line might appear as follows:

TEMPLATE:



EXAMPLE:

TOP SECRET//SI-GAMMA//REL TO CAN, AUS, GBR, NZL, USA

2.4.4 Dissemination Control Markings

Dissemination control markings are used to limit the distribution of SI to specific individuals, groups, or nationalities. A dissemination control marking can take any form provided it is understood by the reader. Examples of dissemination control markings include, but are not limited to:

- ORCON;
- RESTRICTED;
- Canadian Eyes Only (CEO); and
- Release (REL) to … (where CAN is always placed first, then the trigraphs of the other countries in alphabetical order, separated by commas, see paragraph 2.4.3 for an example).

Dissemination control markings may be used with any classification level, including UNCLASSIFIED, in some cases.

2.4.5 Overall Classification

When combining materials with different classification lines into one document, the overall classification must reflect:

- the **highest** classification of any portion used;
- **all** control and sub-control system markings; and
- the **most restrictive** dissemination control markings.

Example:
A document that quotes material classified CONFIDENTIAL//CEO + material from another source classified SECRET//SI//REL to CAN, GBR, USA = SECRET//SI//CEO.

2.4.6 Default National Releasability

Where there are no dissemination control markings in the classification line, the following default national releasability is assumed:

- for SI reports/paragraphs, i.e. (S//SI) or (TS//SI), the default national releasability is REL to CAN, AUS, GBR, NZL, USA; and
- for non-SI paragraphs, i.e. (S), the default national releasability is the national releasability of the SIGINT report.

The following table gives examples:

If classification of a SIGINT report is…	Then the national releasability of a non-SI paragraph is…
TS//SI	CAN, AUS, GBR, NZL and USA
TS//SI//REL to CAN, GBR, USA	CAN, GBR and USA
TS//SI//REL to CAN, AUS, GBR, USA	CAN, AUS, GBR and USA

2.4.7 RESTRICTED

RESTRICTED is a dissemination control marking applied by CSEC to its own product to ensure that certain information is only accessible by named individuals due to the sensitivity of the content or source. RESTRICTED is used only in conjunction with:

- TOP SECRET//SI//Canadian Eyes Only; or
- TOP SECRET//SI-GAMMA//Canadian Eyes Only.

A RESTRICTED report may be identified by the serial number it bears, e.g. R[redacted]

2.4.8 Communities of Interest (COI)

A COI is a dissemination control that protects information in accordance with a common security statement defining the criteria for entitlement to access a COI and the required protection of the COI. Access to a COI is limited to authorized individuals following a formal indoctrination.

When applied to classification markings, COIs are included in the dissemination control section of the classification and are separated from other dissemination controls with a single slash. The COI is the last dissemination control applied to a classification marking:

- TOP SECRET//SI//REL TO CAN, US/[COI NAME]

2.4.9 Portion Marking

Portion markings are abbreviated classification markings that are used to classify individual paragraphs or sections of a report. The following table defines the components of portion markings that are most common on classified documents:

The portion marking component…	Is an abbreviation for…
(TS)	TOP SECRET
(S)	SECRET
(C)	CONFIDENTIAL
(U)	UNCLASSIFIED
(SI)	Special Intelligence
(ECI)	Exceptionally Controlled Information
(G)	GAMMA
(TK)	TALENT KEYHOLE
(CEO)	Canadian Eyes Only
REL to	Releasable to…(followed by the trigraph of the relevant nations)
(OC)	ORCON (Originator Controlled)

2.4.10 Placement of a Classification Marking

The Treasury Board Secretariat requires that security markings appear on the top right corner of each page with the classification level and any subsequent Control System Markings in block capitals. Dissemination Control Markings which follow this may or may not be in block capitals.

2.4.11 When UNCLASSIFIED Becomes Classified

Information that is UNCLASSIFIED may need to be classified when it is either:

- compiled with other UNCLASSIFIED information, and if the ensuing compilation reveals sensitive information about intelligence operations, (also known as the "Mosaic Effect"); or
- associated with intelligence operations.

2.4.12 When Classified Becomes UNCLASSIFIED

Classified information may become "UNCLASSIFIED" either through declassification or sanitization.

- Declassification is defined as "the authorized change in the status of information from classified to UNCLASSIFIED." The information remains unaltered. Declassification is normally applied to historic information. The permission of the originating agency (or its successor) is required; and
- Sanitization is defined as "the process of editing or otherwise disguising SI to protect sensitive sources, methods or techniques. The aim of sanitization is to permit wider dissemination outside of SI channels."

UNCLASSIFIED information concerning official SIGINT business, or resulting from the declassification or the sanitization of SI, must not be gratuitously disseminated for non-official use. Nor does UNCLASSIFIED mean information may be publicly released. Departments may add their own dissemination control markings to UNCLASSIFIED material to remind recipients not to disseminate the information unnecessarily, for example, "For Official Use Only".

2.4.13 Automatic Declassification

Canadian SI material is not subject to automatic declassification after a given time-period.

2.5 Obsolete Classification Markings

2.5.1 Obsolete SI Codewords

Prior to 1999, SI was protected by 5-letter "codewords" and/or caveats. Because the codewords themselves were classified CONFIDENTIAL until 1997, unclassified references had to use generic wording, e.g. "TOP SECRET CODEWORD" (TSC) and "TOP SECRET Special Material". Information protected by obsolete codewords is still classified, and the level of protection against unauthorized disclosure mandated by the original classification and codeword must still be applied.

2.5.2 More Recent Codewords

The following table illustrates which codewords and their variations were in use from 1968, and may still be seen on SI reporting; for example, where systems cannot be modified to accept the marking "SI", or on historical documents.

Classification	Codeword	Abbr.	Category	Current Usage	
				CSEC Serial #	SI Control Markings
TOP SECRET	UMBRA	TSC TSU	III	[redacted]… [redacted].. [redacted]… R[redacted]…	TOP SECRET//SI
SECRET	SPOKE	SC SS	II	[redacted]… [redacted]..	SECRET//SI
	MORAY	SCX	IIX	(no current equivalent)	

2.5.3 Category I (CAT I)

Category I or CAT I referred to less sensitive information that was derived from COMINT but did not require SI protection. CAT I reports were issued at the CONFIDENTIAL or SECRET level (serial numbers began with "C" or "1", respectively). Although they are occasionally seen now, they are rare. CAT I also referred to an indoctrination allowing site access; this is now called SIGINT Facility Access (SFA).

2.5.4 HVCCO "*Handle Via COMINT Channels Only*" was a caveat or warning applied to information at any classification level that was not considered COMINT, but related to COMINT sources or methods. It is no longer used on SIGINT reporting; it has been replaced by dissemination control markings.

2.6 Second Party Classifications

2.6.1 Sharing Intelligence with the 5-Eyes A significant volume of SI information is shared between Canada and its four key allies: Australia, New Zealand, UK and USA. Collectively, this community of interest is called the 5-Eyes. When receiving SIGINT from Canada, 5-Eyes countries are expected to mark the information to ensure it is protected at a comparable level to its Canadian classification.

2.6.2 5-Eyes Equivalencies of Canadian Classifications Canada's allied SIGINT partners (also called Second Parties) -- the National Security Agency (NSA) in the US, the Government Communications Headquarters (GCHQ) in the UK, the Defense Signals Directorate (DSD) in Australia, and the Government Communications Security Bureau (GCSB) in New Zealand -- do use certain control, sub-control, and dissemination control markings that are different from those used in Canada (see section 2.7). Nevertheless, these markings are recognized in Canada and should be accorded the same protection given to Canadian SIGINT.

2.7 5-Eyes Equivalencies of Canadian Classifications

Canadian Marking	US marking:	UK marking:	Australian marking:	New Zealand marking:
CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIAL
CONFIDENTIAL//SI	CONFIDENTIAL//SI	[redacted]		
SECRET	SECRET	SECRET	SECRET	SECRET
SECRET//SI	SECRET//SI	[redacted]		
SECRET//SI//ORCON	SECRET//SI//ORCON			
TOP SECRET	TOP SECRET	TOP SECRET	TOP SECRET	TOP SECRET
TOP SECRET//SI	TOP SECRET//SI	[redacted]		
TOP SECRET//SI// ORCON	TOP SECRET//SI// ORCON			
TOP SECRET//SI-GAMMA//ORCON	TOP SECRET//SI-GAMMA//ORCON			

CHAPTER 3

DEPARTMENTAL REQUESTS FOR ACCESS TO SPECIAL INTELLIGENCE

Chapter 3: Departmental Requests for Access to Special Intelligence

3.1 Introduction

3.1.1 Contents

This chapter contains the following topics:

Topic
3.1 Introduction
3.2 SIGINT Security Personnel Structure
3.3 Authorization to Receive SIGINT
3.4 Authorization for Special Intelligence Read-Only Service

3.1.2 Introduction

This chapter describes the different levels of service that CSEC provides to Government of Canada (GC) organizations, including:

- how departments can request SIGINT service from CSEC; and
- associated departmental roles.

3.1.3 CSEC as Lead Agency

As described in Appendix B of the *Policy on Government Security* (PGS), CSEC is the national authority for SIGINT and COMSEC. It is also responsible for developing policy instruments related to information technology (IT) security for approval by Treasury Board Secretariat. In its role as national authority for SIGINT, CSEC is responsible for:

- developing operational standards and technical documentation as it relates to SIGINT;
- providing the approval to operate for all facilities and IT systems accredited to process and store SIGINT information;
- developing and providing specialized SIGINT training;
- managing the distribution of SIGINT;
- maintaining the national inventory of personnel cleared for access to SIGINT;
- representing the GC on national and international SIGINT committees and initiatives; and
- negotiating agreements with allied agencies.

3.1.4 CSEC Representatives

The Director SIGINT Requirements is the approval authority for requests from government departments or agencies to access SIGINT information (ssmo-dl@cse-cst.gc.ca on the unclassified Internet or [redacted]@cse-cst.gc.ca on CTSN).

For these procedures, the following directorates may assist clients with their requests for access to SIGINT information:

- Director General Military SIGINT (DGMS) is the CSEC representative for requests from Canadian military organizations including CFIOG; or
- Director General Intelligence (DGI) is the CSEC representative for requests from other GC organizations.

3.1.5 Types of Access

There are two main types of access that an organization may obtain depending on its needs:

- authorization to receive and retain SIGINT (Authorized Organizations); or
- read-only access (Client Organizations).

3.1.6 What is an Authorized Organization?

An Authorized Organization is a GC department or agency which has been certified and accredited by CSEC to retain and/or process SIGINT, specifically Special Intelligence (SI).

Note: Normally, Authorized Organizations are GC departments and agencies, including overseas missions and military commands, but they can also include private contractors of such organizations.

3.1.7 How to Become an Authorized Organization

A senior-level manager at a potential Authorized Organization should request approval to retain or process SI by sending a letter to the CSEC Director SIGINT Requirements (at P.O. Box 9703, Terminal, Ottawa, ON, K1G 3Z4). A CSEC representative may assist the requesting manager in the definition of the request for SIGINT.

Requests to receive and retain SI hard copy information may necessitate significant upgrades to physical security, while requests to process SI may require approval from the CTSN board of management (if the requesting agency is not already a member of CTSN). Departments should engage first with CSEC to establish their requirement to process SI information (see 3.3 for further information).

3.1.8 What is a Client Organization?

A Client Organization is a GC organization that has not been certified or accredited by CSEC, and therefore, may not retain and/or process any SI. A Client Organization receives SI read-only service from CSEC Client Relations Officers (CROs).

3.2 SIGINT Security Personnel Structure

3.2.1 Requirements

In accordance with the PGS and related standards, deputy heads of all departments are responsible for appointing a departmental security officer (DSO) to manage the department's overall security program. This includes the safeguarding of SIGINT and other classified information. As the national authority for SIGINT, CSEC is responsible for policy governing the handling of SIGINT information. To ensure such information is afforded appropriate protection, a SIGINT security organizational and administrative structure must be in place in every Authorized Organization, and must include:

- a Departmental Security Officer (DSO);
- a Senior Indoctrinated Official (SIO);
- a COMINT Control Officer (COMCO);
- a Deputy COMCO (D/COMCO); and
- an Information Systems Security Officer (ISSO).

If an Authorized Organization wishes to store GAMMA, it must also appoint a GAMMA Control Officer (GCO). This can be the same person as the COMCO or the D/COMCO.

If an Authorized Organization does not rely exclusively on the electronic delivery of SI reports, it must also establish, within its SIGINT Secure Area (SSA), a Registry system to receive, distribute, and store SIGINT material, specifically SI reports, separately from other classified non-SI reports.

3.2.2 Departmental Security Officer (DSO)

The DSO should have sufficient security experience and be strategically placed within the organization to provide organization-wide strategic advice and guidance to senior management.

The DSO's duties as they concern SIGINT include cooperating with the COMCO and ISSO on issues including, but not limited to, the following:

- general administration of organizational procedures;
- security training and awareness;
- identification of assets;
- security risk management;
- access limitations;
- security screening and clearances;
- physical security;
- IT security; and
- investigations of SIGINT security violations.

3.2.3 Senior Indoctrinated Official (SIO)

Each Authorized Organization is required to appoint an SIO. The SIO should be of sufficient seniority to ensure that SIGINT security is fully considered in the operations of the Authorized Organization. The SIO in every Authorized Organization has overall responsibility for SIGINT security. The SIO is responsible for how SIGINT is used by his/her organization, as well as for the following:

- determining the classification of information about the relationship between the Authorized Organization and CSEC;
- defining who within the Organization can approve requests for indoctrination of personnel;
- providing input whenever there is a question about the need-to-know related to SIGINT issues (e.g. indoctrination for access to GAMMA, etc.); and
- acting as the Organization's Point of Contact (POC) for SIGINT issues.

The SIO may delegate routine oversight of these responsibilities to the COMCO.

3.2.4 COMINT Control Officer (COMCO)

A COMCO and D/COMCO must be appointed for every SSA established. In addition to any responsibilities delegated by the SIO, the COMCO is responsible for SIGINT security on a day-to-day basis. These responsibilities include:

- ensuring that SIGINT and SIGINT-related information is handled (stored, disseminated and destroyed) in accordance with security requirements including these standards and any other specific standards issued by CSEC;
- obtaining the appropriate clearances for departmental personnel to be indoctrinated for access to SIGINT;
- indoctrinating and de-indoctrinating departmental personnel, if authorized by CSEC;
- maintaining a departmental indoctrination list, and forwarding updates to CSEC regularly;
- advising indoctrinated personnel on SIGINT security;
- notifying CSEC of any changes to SIO, COMCO, or D/COMCO appointments;
- investigating violations, compromises, or suspected compromises of SIGINT security, and reporting to the SIO and CSEC (see *Chapter 4: Protection of SIGINT Information*); and
- mustering SIGINT documents, when required.

3.2.5 Information Systems Security Officer (ISSO)

To establish and maintain accreditation, an Authorized Organization must appoint an Information Systems Security Officer (ISSO) for each separately accredited IT system and network containing SIGINT (an ISSO may be responsible for more than one system/network). In cooperation with the COMCO, the ISSO ensures that IT systems and networks are compliant with SIGINT standards for IT security. Specific ISSO responsibilities include, but are not limited to:

- ensuring that a SIGINT IT system is designed, developed, operated, used and maintained, according to these standards;

Continued on next page

3.2.5 Information Systems Security Officer (ISSO) (continued)

- evaluating known vulnerabilities to determine whether additional safeguards are needed;
- ensuring that users have the required clearances and authorizations, have been indoctrinated, and are familiar with documented security practices before gaining access to the system;
- ensuring that these procedures are applied to all personnel who have access to a SIGINT IT system;
- investigating and resolving network security incidents and/or violations leading to or involving the potential for compromise of SIGINT;
- evaluating the security performance of the network;
- reviewing network activity; and
- reporting security incidents to the COMCO.

ISSOs should not be confused with the IT Security Coordinators (ITSC) required for compliance with the *Operational Security Standard: Management of IT Security* (MITS) policy. ITSCs deal with general IT security issues and are required for MITS compliance. ISSOs are responsible for the security of SIGINT-bearing information systems and are required for SIGINT accreditation at Authorized Organizations.

3.2.6 GAMMA Control Officer (GCO)

In most Authorized Organizations, the position of GCO will likely be filled by the COMCO or D/COMCO; however, a separate individual may be appointed to this position. Responsibilities of the GCO include, but are not limited to:

- implementing indoctrination processes at the Authorized Organization in accordance with section 3.10 of CSSS-104, *Gamma Handling Standards*[4] (i.e. reviewing requests for access to GAMMA, and seeking advice from the departmental Personnel Security office about an applicant's GAMMA access request);

Continued on next page

[4] Previously OPS-5-8.

3.2.6 GAMMA Control Officer (GCO) (continued)

- controlling and tracking access to GAMMA material in accordance with these standards; ensuring that users of GAMMA information within their organization handle the material in accordance with these standards;
- consulting with the CSEC GCO for guidance on procedural and technical GAMMA issues;
- overseeing the central GAMMA Registry within their organization;
- reporting compromises or suspected compromises of GAMMA material to the SIO within their organization; and
- verifying GAMMA indoctrination status of staff within their respective departments.

These responsibilities pertain regardless of whether the GCO role is part of the duties of the COMCO or D/COMCO or of a discrete individual.

3.3 Authorization to Receive SIGINT

3.3.1 Types of SIGINT Delivery

There are several ways an Authorized Organization can access SIGINT information. These include:

- hard copy access via a CSEC Client Relations Officer (CRO), usually within the client office;
- hard copy access from within a central SIGINT registry;
- electronic access through CTSN or another IT system accredited for SIGINT via fixed departmental systems that are located within an SSA; and
- electronic access to a [redacted]

3.3.2 Content of a Request

The requesting organization must complete and forward a request to receive SIGINT to the Director SIGINT Requirements (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN). The request must include:

- the type of SIGINT delivery requested;
- a rationale for the request, including the mandate of the organization and the proposed use of SIGINT;
- the POC (i.e. SIO) who can explain the organization's need for SIGINT; and
- the steps for the establishment of an SSA, if one does not yet exist.

3.3.3 Approval of a Request

Upon receipt of a GC organization's request to receive SIGINT, Director SIGINT Requirements will:

- review the request to determine if:
  - the stated business case is consistent with CSEC's mandate, and
  - CSEC has the appropriate resources;
- approve or deny the request; and
- provide a reply to the organization, which includes required follow-up action by the organization.

3.3.4 Formal Agreement

If an organization's request to become an Authorized Organization is approved, CSEC's DGI and the Department's SIO will sign a Memorandum of Understanding (MoU) related to the handling and use of SIGINT. The content of the MoU will include:

- the purpose of the MoU;
- departmental mandates and authorities;
- dissemination methods, conditions and departmental obligations;
- departmental POCs; and
- the effective date, scheduled MoU reviews and signatures.

3.3.5 Certification and Accreditation

For requests that involve the retention and/or processing of SIGINT, part of the establishment process involves the SIGINT Certification and Accreditation (C&A) of an Authorized Organization's system and/or facility. As described in *Chapter 6: SIGINT Certification and Accreditation*, C&A is required to ensure that appropriate security features and safeguards are implemented to protect SI information. Authorized Organizations are responsible for maintaining the integrity of any accreditation that has been granted to them under these procedures. Authorized Organizations must consult with the Director SIGINT Requirements before making any modifications that could affect the accreditation status. CSEC reserves the right to:

- request any documentation created by the Authorized Organization respecting its maintenance of the integrity of its accredited facility; and
- carry out site visits, for example:
  - during the re-accreditation of facilities, which should occur every five years, or
  - to conduct spot audits as part of an investigation or in response to complaints.

3.3.6 Indoctrination process

Departmental COMCOs, D/COMCOs, GCOs, and CSEC CROs will normally indoctrinate new clients requiring SI and/or GAMMA access in Authorized Organizations. In exceptional circumstances, the CSEC SIGINT Security Management Office (SSMO) may indoctrinate clients for SIGINT and/or GAMMA access. See *Chapter 7: Personnel Security* for details on the indoctrination of new clients.

3.4 Authorization for Special Intelligence Read-Only Service

3.4.1 How to Request Read-Only Service

The Director SIGINT Requirements is the CSEC approval authority for requests from clients or Authorized Organizations to view SIGINT reports.

3.4.2 Content of Request

The request should include:

- the rationale: mandate of the requesting organization and its proposed use of SI; and
- the client's POC.

3.4.3 Approval of Request

Upon receipt of the Client Organization's request to receive SI, Director SIGINT Requirements in consultation with DGI, will review the Client's request to:

- determine
  - if the client's stated business case is consistent with CSEC's mandate and priorities, and
  - if CSEC has the appropriate resources;
- approve or deny the client's request; and/or
- provide a reply to the client, which includes any required follow-up action by the client.

3.4.4 Formal Agreement

If a potential new Client Organization's request for read-only service is approved, CSEC DGI and the Department's SIO will sign an MoU related to the handling and use of SIGINT. The content of the MoU will include:

- the purpose of the MoU;
- departmental mandates and authorities;
- read-only service conditions and departmental obligations;
- departmental POCs; and
- the effective date, scheduled MoU reviews and signatures.

3.4.5 Indoctrination Process

The CSEC CRO will normally indoctrinate new read-only clients at Client Organizations. See *Chapter 7: Personnel Security* for details on the indoctrination of new clients.

CHAPTER 4

PROTECTION OF SIGINT INFORMATION

Chapter 4: Protection of SIGINT Information

4.1 Introduction

4.1.1 Contents This chapter contains the following topics:

4.1.2 Introduction This chapter describes procedures that must be followed by users when handling SIGINT/Special Intelligence (SI) information. Specifically, this chapter covers the handling of SI documents and SI reporting.

Note: CSEC document CSSS-104, *GAMMA Handling Standards* provides details on handling GAMMA material; Annex 3 of this chapter contains a GAMMA indoctrination briefing, which is offered by the SIGINT Security Management Office (SSMO). CSEC document CSSS-102, *ECI Handling Standards*[5], provides details on handling ECI material. These policy instruments are available from the CSEC page on CTSN.

[5] Formerly OPS-5-7

4.2 Access to Special Intelligence

4.2.1 General

The basic rule governing the distribution and handling of SI material is that it may be passed only to Authorized Organizations and, within them, only to persons who have been indoctrinated for SIGINT Information Access and have a need-to-know. If an Authorized Organization prints or otherwise transfers information from a CSEC-controlled information system (e.g. [redacted] that information comes under the control of the Authorized Organization and must be handled in accordance with these standards. An Authorized Organization must not disseminate any SIGINT end-product report to another Authorized Organization without the approval of CSEC. For further guidance on the dissemination of SIGINT, please refer to Operational Policy at CSEC ([redacted]@cse-cst.gc.ca on CTSN).

It is the responsibility of indoctrinated persons to ensure that any individual with whom they wish to discuss an item of SIGINT is indoctrinated to the appropriate level and has a need-to-know for the information. Verification of SIGINT indoctrination level can be obtained from the department's COMINT Control Officer (COMCO) or the CSEC Client Relations Officer (CRO). This information is also available on CTSN.

4.2.2 Requirements for Direct Access to SI Information

Anyone who requires direct access to SI and SI-related information must:

- be a Canadian citizen (see *Chapter 7: Personnel Security* for information on integrees [redacted]
- hold a TOP SECRET security clearance;
- have successfully completed a subject interview for Special Access to compartmented intelligence; and
- be indoctrinated to SIGINT Information Access (formerly CAT III).

Note: Clients must also be indoctrinated for access to GAMMA prior to handling any GAMMA material. Furthermore, clients who are indoctrinated for GAMMA must be informed of their obligations under the *Security of Information Act* (SOIA).

4.2.3 Access to SIGINT: Contractors and Consultants

A contractor or consultant requiring access to SI material must meet the same conditions as any other individual in Canada who requires access. If SIGINT is to be retained by contractors or consultants, their facilities, including information technology (IT) systems, must meet the physical and IT Security standards established for the protection of SIGINT (see *Chapter 8: Information Security for SIGINT Systems*).

4.2.4 Access to SIGINT: Integrees [redacted]

See *Chapter 7: Personnel Security* for information on integrees [redacted]

4.2.5 Requirements for SIGINT Facility Access Privileges

SIGINT Facility Access privileges pertain to individuals who require access to a SIGINT facility, but not to SIGINT information. These individuals must:

- be a Canadian citizen OR hold permanent resident status in Canada (see additional requirements below for permanent residents);
- hold a TOP SECRET security clearance; and
- be indoctrinated to SIGINT Facility Access (formerly CAT I) level (see *Chapter 7: Personnel Security*, section 7.3 for SIGINT indoctrination categories).

Persons with permanent resident status in Canada must be considered on a case-by-case basis, and are subject to an additional screening risk assessment to evaluate their eligibility. At CSEC, the Director SIGINT Requirements approves indoctrinations of such individuals for SIGINT Facility Access. In Authorized Organizations, the SIO provides approval.

4.2.6 Record Keeping: Indoctrination Status of SI Users

The COMCO in each Authorized Organization must maintain an updated list of SIGINT-indoctrinated staff and their positions within their respective departments, and must provide this list to the Personnel Security Office at CSEC at the end of each calendar year, or whenever requested [redacted]@cse-cst.gc.ca on CTSN). The COMCO must also promptly inform CSEC of any changes in the indoctrination status (i.e. indoctrination or de-indoctrination) of an individual.

CSEC Personnel Security maintains a list of all Government of Canada (GC) employees who are indoctrinated for access to SIGINT, GAMMA and ECI. (See also *Chapter 7: Personnel Security* and CSSS-102 *ECI Handling Standards* for more information.)

4.3 Distribution and Registry of SIGINT in the Work Area

4.3.1 Basic Rule for Distribution

The basic rule governing the distribution and handling of SI material is that it may be passed only to Authorized Organizations and, within them, only to persons who have been indoctrinated for SIGINT Information Access (SIA) (formerly Category III) and have a need-to-know. An Authorized Organization may not disseminate any SIGINT end-product report to another Authorized Organization without the approval of CSEC. This means that SIGINT cannot be shared in its original or modified form without written permission from CSEC (see section 4.7 of this chapter for more information on disseminating SIGINT).

4.3.2 Registry System

Authorized Organizations that do not rely entirely on electronic storage of SI material must establish a registry (sometimes referred to as a "Special Registry") within an SSA where SI material is handled and stored separately from other classified information. Registry document-control procedures, such as the registering of incoming/outgoing material, distribution and destruction, must be established to permit audit trails, when necessary (CSEC does not need to be informed about who accesses each individual report).When the volume of SI material is such that regular, detailed document accountability procedures are impractical (e.g. large volumes of end-product reporting received electronically), adequate records must be maintained to indicate which material was received and/or transmitted. Records related to transmitting and receiving documents must be retained for two years.

4.4 Protection of SIGINT in the Work Area

4.4.1 General

Within an Authorized Organization, SI material must be circulated, worked on, discussed and stored so that there is no possibility of unindoctrinated persons gaining access to it. Introduction of such material into a room where there are unindoctrinated persons must be avoided; CSEC must be consulted regarding any possible exceptions.

4.4.2 Movement of SIGINT Material Inside an Authorized Organization

SI material being carried by indoctrinated persons from one authorized SIGINT work area to another, within their organization, must be carried in an envelope or similar pocket-type folder, or a secure briefcase; such material does not need to be wrapped and sealed. If the material is to be carried outside an Authorized Organization, e.g. for a meeting at another department, it must be wrapped and marked in accordance with the procedures described in section 4.4.9, "Marking: Outer Envelope".

4.4.3 Discussing SI

It is the responsibility of indoctrinated persons to ensure that any individual with whom they wish to discuss an item of SIGINT is indoctrinated to the appropriate level and has a need-to-know for the information. Verification of SIGINT indoctrination level can be obtained from the department's COMCO or the CSEC CRO, and is also available on CTSN. Indoctrinated personnel should ensure that any such authorized conversations are conducted in a secure location or in such a way so as to ensure that they may not be overheard by unindoctrinated personnel.

Note: Because of national dissemination restrictions applied by Second Parties on their own reporting (e.g. ORCON), Canadian recipients must obtain approval from CSEC's Operational Policy section [redacted]@cse-cst.gc.ca on CTSN) prior to discussing a SIGINT end-product report with a Second Party national whose nation or organization is not included on the original distribution list.

4.4.4 Telephone Discussions

Telephone discussions involving SI must be conducted only on a secure device. Callers are responsible for verifying the identity and indoctrination status of the person being contacted.

When SI is to be discussed on the secure telephone, care must be taken that unindoctrinated persons are not within hearing, and that no listening device (intercom) or other telephone is in use in the vicinity.

4.4.5 Electronic Devices Used for SI

Electronic data processing or storage devices (e.g., PCs, lap-top computers, USB devices or memory sticks) are subject to individual departmental control mechanisms established to control and approve their use for SI. At a minimum these controls should include the following precautions:

- devices containing SI must be clearly labeled with the classification of the most sensitive information they contain;
- devices must only be used on SI-accredited systems;
- whenever possible, SI information stored on these devices should be encrypted;
- when not in use, devices should be stored in an SSA in a safe that meets RCMP standards for holding SI material; contact CSEC's Physical Security Services ([redacted]@cse-cst.gc on CTSN) for information on safes that meet the RCMP standards; and
- devices should be destroyed when no longer required; destruction methods for devices should ensure that the time and cost of recovering data from the device is greater than the value of the data (CSEC's IT Security Guidance (ITSG)-06, *Clearing and Declassifying Electronic Data Storage Devices*, identifies methods for destroying electronic data devices, ITSG-06 is available on CSEC's unclassified Internet site at www.cse-cst.gc.ca).

4.4.6 E-mailing SI

SI information can only be transmitted electronically on networks that have been appropriately certified and accredited by CSEC, and may only be forwarded to individuals who are indoctrinated for SIGINT Information Access and have a need-to-know. Also, GAMMA information can only be transmitted electronically on networks that have been accredited for GAMMA.

It is the responsibility of the sender to verify that the recipient has the appropriate indoctrinations.

4.4.7 Electronic Storage

Soft copies of SI information must be stored in electronic files in a TOP SECRET//SI environment and with access limited to persons who have:

- a SIGINT Information Access indoctrination; and
- a need-to-know.

4.4.8 Re-use of Electronic and Electro-Magnetic Media

Electronic and electromagnetic media used to process and/or store SIGINT must not be re-used in a non-SIGINT environment. Once used to process and/or store SIGINT, electronic and electromagnetic media retain the highest classification of data stored on them, or of the system they were attached to. This means that a disk that has been used to store data classified TOP SECRET//SI becomes TOP SECRET//SI itself and must be disposed of accordingly. If re-use of media is required, CSEC will determine, on a case-by-case basis, if measures such as degaussing or overwriting can make it possible to re-use TOP SECRET//SI media.

4.4.9 Physical Storage of SI

SI material must be stored in approved security containers, unless the room or area has been approved as an open storage area (equivalent vault protection) or a continuous operation area. Safeguarding of associated keys, safe combinations and system passwords must be commensurate with the highest level of SIGINT they protect. Safe combinations should be changed annually, or when there is a change of personnel, or for cause.

4.4.10 Printing SI

Clients may print SI information; however, hard copy SI material must:

- display appropriate classification markings;
- be stored in an approved container; and
- remain within a SIGINT Secure Area (SSA).

For GAMMA material, clients must ensure that the material:

- is protected from the view of persons who are not indoctrinated for GAMMA;
- is locked in approved containers that are only accessible by GAMMA-indoctrinated personnel; and
- remains within a SSA.

Note: Printers should be handled as SI system components, particularly if they store information so that it is vulnerable to forensic exploitation if storage components, such as internal hard drives, are recovered.

4.4.11 Toner Cartridges

This applies to all equipment that uses similar technology (a laser printer with removable toner cartridge) as part of its production process (i.e. laser faxes, printers, copiers, etc.). Used toner cartridges may be treated, handled, stored and disposed of as UNCLASSIFIED, when removed from equipment that has successfully completed its last print cycle.

However, should a print cycle not be completed, there is the potential that residual toner may be left on the drum that could cause an information compromise. The following procedures should be followed for those situations where the print cycle was not successfully completed.

- when a laser printer has not completed the printing cycle (e.g., a paper jam or power failure occurs), completing a subsequent print cycle before removal of cartridge is sufficient to wipe residual toner from the cartridge drum;

- when the print cycle is interrupted by a jam or other action, and the toner cartridge is removed from service at the same time, the toner cartridge drum will be inspected for residual toner by lifting the protective flap and viewing the exposed portion of the drum. If residual toner is present, manually rotating the drum is sufficient to wipe off residual toner material present; and

- the used toner cartridge may be treated, handled, stored and disposed of as UNCLASSIFIED and be returned for recycling or other agency approved method of disposal. In keeping with Environmental Protection Agency policy, agencies/departments are encouraged to establish procedures for recycling properly sanitized toner cartridges.

4.4.12 Photocopying

Unless otherwise indicated, SIGINT material up to and including TOP SECRET//SI may be photocopied. Copying of SI material must be done by appropriately indoctrinated personnel in an SSA, and the document being copied must show the additional distribution. Normally, additional copies of numbered documents and publications produced by CSEC or a Second Party organization can be obtained from CSEC; however, should it be necessary to photocopy a numbered document, it must be given a unique copy number and the distribution recorded.

Note: Photocopiers should be handled as SI system components, particularly if they store information so that it is vulnerable to forensic exploitation if storage components, such as internal hard drives, are recovered.

4.5 Transport of SIGINT Material

4.5.1 Transporting SI Material

Physical SI material is moved between Authorized Organizations by courier. Material forwarded by courier, including that being transferred between buildings of the same Authorized Organization, is wrapped and carried in a locked container (secure briefcase, bag, box, etc.), and is sent via SIGINT registries and sub-registries only. In the Ottawa area, CSEC provides a SIGINT courier service to and from CSEC and all Authorized Organizations.

4.5.2 Shipping Equipment Used with SI

Approved channels must be used when shipping equipment (including components and ancillary devices) on which SI material has been or will be processed, stored or transmitted. All such equipment must be transported in accordance with the procedures that apply to ITSG-10, *COMSEC Material Control Manual*. Equipment used to process, store or transmit SI must be transported in accordance with the procedures outlined in the RCMP G1-009, *Transport and Transmittal of Protected and Classified Information.* CSEC must be consulted prior to shipping equipment which is the property of CSEC.

4.5.3 Sending SI via Courier

SI in hard copy format must not be mailed through any commercial mail system (e.g. national postal services), but it may be sent as hard copy to a recipient via cleared and indoctrinated couriers.

When sending SI, the following points must be observed:

- clients must **not** forward SI reports beyond their own department without CSEC approval;
- SI material must be sent in sealed envelopes that are addressed only to those who are appropriately indoctrinated;
- transmittal receipts, bearing the correct classification with and without the attachment, but giving no COMINT details, must accompany any SI materials being sent;
- materials classified as TOP SECRET//SI or higher (e.g. GAMMA) must be hand delivered by CSEC CROs, or by couriers cleared to TOP SECRET and indoctrinated for SIGINT Information Access; and
- such material must also be accompanied by an appropriately completed transmittal receipt which must be retained for two years.

It is imperative to ensure that the recipient of SI material has the appropriate clearances and a need-to-know.

4.5.4 Courier Certificates

An authorized courier delivering SIGINT material via a mode of transportation where passengers must undergo security screening or inspection, or while crossing an international border, must carry a completed DND-468 Courier Certificate. This written authorization includes:

- the identity of the relevant Authorized Organization;
- confirmation that the bearer of the certificate is authorized to carry/escort classified material in a locked/sealed container;
- a request to police, customs, immigration or security officials to extend to the classified material immunity from search or examination; and
- identification of a departmental official who can be contacted for clarification or verification of the certificate.

4.5.5 Mail

SI material may **not** be sent to another Authorized Organization within Canada by Canada Post or any commercial courier service. Contact CSEC for information about authorized courier services.

4.6 Packaging of SIGINT Material

4.6.1 General

The packaging and carrying case used for the transport and transmittal of classified material should be durable enough to protect the information from accidental exposure and damage, and make it easy to detect any tampering.

4.6.2 Wrapping

SI material prepared for delivery by courier or mail must be double-wrapped, and the material must be accompanied by a transmittal/receipt form. Receipts are attached to the material being forwarded, not on the outside of the envelope.

4.6.3 Marking: Inner Envelopes

Inner envelopes must be sealed with security approved or gum-reinforced tape, and must show the security classification at the top and bottom, both sides. If more than one item is included, the security classification must reflect the highest security content of the package. "SI" is not to be marked on the envelope, but is indicated by the identifier "Special Material" placed below the security classification markings on both sides of the wrapping. Caveats such as "Canadian Eyes Only" are similarly marked on both sides; Special Series Product and ECI labels are affixed, as appropriate. The reference or receipt number should also be shown on the envelope.

4.6.4 Addressing SI Material

SI material must be addressed to the COMCO by name (or by name to the indoctrinated individual delegated by the COMCO to receive, sign for and open packages marked Special Material), with the full Special Registry address and full return address.

If the contents of the package are for a specific individual within an Authorized Organization, the inner wrapping may also be marked :

- "For the Attention of ..."; or
- if it is to be opened only by a named individual, "Private For..."; or
- "To Be Opened Only By...".

Special Series Product is addressed to the GAMMA Control Officer, with specific recipients included, as required; ECI material is addressed to the intended recipient only. At a minimum, addressing on inner envelopes must contain the following:

- the name of the intended recipient;
- the recipient's title, department; and
- the full, special registry return address.

4.6.5 Marking the Outer Envelope

SIGINT security-related markings must not be shown on outer envelopes. The only terms shown on an outer envelope will be:

- Via Courier; or
- by Safe Hand.

Outer envelopes should be sealed with reinforced tape.

4.6.6 Addressing the Outer Envelope

Addressing on the outer envelope must include only the following:

- the name of the COMCO (but not the term "COMCO"), or the name of the person appointed by the COMCO to receive, sign for and open packages marked "Special Material";
- the full Special Registry address (but no reference to the term Special Registry); and
- a full return address.

4.7 Carrying SIGINT by Hand

4.7.1 Wrapping and Marking

SI material being carried by indoctrinated individuals to and from meetings, discussions, or briefings, outside their own building, must be wrapped in a single envelope sealed with reinforced or other security-approved tape, and carried in a locked container/briefcase.

The locked container or briefcase serves as the outer wrapping, and should be tagged with a return office address and telephone number. The envelope must be marked with the appropriate security classification, and may also be marked "By Safe Hand". The envelope must be self-addressed, but at a minimum must include name, title or position designator, and department, and a telephone number.

A transmittal/receipt form is not required unless the material is intended for actual delivery to another Authorized Organization, but the contents of the package should be recorded to assist in tracing and preparing damage assessments should the package be lost or stolen.

4.8 Declassification and Disclosure

4.8.1 Declassifying and Downgrading

There is no automatic expiry date for the safeguarding of SIGINT sources or techniques; consequently, SIGINT and SIGINT-related information are not automatically declassified or downgraded (see *Chapter 2: Special Intelligence Classification and Markings*). In Canada, CSEC is the sole authority for downgrading and declassifying SIGINT information and assets; therefore all requests for, or queries related to, SIGINT declassification and downgrading must be referred to and approved by CSEC's Operational Policy section ([redacted]@cse-cst.gc.ca on CTSN).

4.8.2 Downgrading or Declassifying SIGINT Information Prior to Transfer to Library and Archives Canada (LAC)

Library and Archives Canada (LAC) does not currently possess facilities to house information classified within SI channels. Therefore, in accordance with Records Disposition Authority 2008/003, CSEC shall review archival records marked SI for the purpose of possible downgrading and declassification prior to their transfer to LAC to ensure that no records so marked are transferred to LAC custody and control.

4.8.3 Access Requests

All departments that receive requests made under the *Access to Information Act* (ATIA) and/or the *Privacy Act* (PA) for information received from, or that relates to, the activities of CSEC, including SIGINT activities and/or SIGINT records, must consult the Director, Access to Information and Privacy (DAIP), Department of National Defence, who will in turn contact CSEC's ATIP authorities.

4.8.4 Public Statements

CSEC's SIGINT role has been publicly avowed as follows:

> "CSEC's purpose is to provide, with the assistance of the Canadian Forces Information Operations Group (CFIOG), a service of foreign signals intelligence in support of Canada's foreign and defence policies."

The current *Policy on Government Security* (PGS) also describes, in an UNCLASSIFIED form, CSEC's role and responsibilities with respect to SIGINT. In addition, the "fact of" SIGINT collaboration between or among Canada/CSEC and the US/NSA, the UK/GCHQ, Australia/DSD and New Zealand/GCSB is UNCLASSIFIED. However, these statements regarding CSEC, although UNCLASSIFIED, must not be disclosed gratuitously.

All proposed public statements that may contain information derived from SIGINT, or concerning COMINT and/or SIGINT activities, must be referred to CSEC for review and approval prior to release (public.affairs-affaires.publiques@cse-cst.gc.ca on the Internet).

4.9 Retention and Destruction

4.9.1 Retention and Disposition

SIGINT records and information must be retained no longer than absolutely necessary. As the originator of end-product SIGINT reports, CSEC is the organization responsible for the disposition of this material in accordance with Records Disposition Authority 2008/003.
In consultation with affected Government of Canada (GC) departments, CSEC will establish procedures and guidelines for the retention and disposition (destruction or transfer to Library and Archives Canada (LAC), see Chapter 4: Protection of SIGINT Information) of records or information generated in support of CSEC's Foreign Intelligence function. CSEC maintains a historical file of SIGINT end-product reporting, and can provide copies of previously published reports as required.

4.9.2 Destruction of SIGINT Information

In Authorized Organizations that maintain a SIGINT Registry, the authority to action the destruction of SIGINT material rests with the COMCO, unless otherwise designated by CSEC. In Authorized Organizations that rely primarily on the electronic delivery of SIGINT, individual users are responsible for the destruction of any hard copies they generate.

SIGINT material, including removable digital media, must be destroyed by methods and equipment approved for the destruction of TOP SECRET material. Approved methods for destroying printed material include:

- burning;
- shredding in a TOP SECRET approved shredder; or
- pulping (or a combination of the above).

For destroying information on removable digital media refer to CSEC's IT Security Guidance (ITSG)-06, *Clearing and Declassifying Electronic Data Storage Devices* (ITSG-06 is available on CSEC's unclassified Internet site at www.cse-cst.gc.ca).

Pulverizing or crushing should be used to physically destroy items such as hard drives or compact disks. Because of the aggregate information stored on electronic and electromagnetic media, it is recommended that they be erased prior to destruction.

The destruction of SI material must be witnessed by at least one individual indoctrinated to the category of SI being destroyed. Unless requested, certificates of destruction or notification of registration of destruction need not be forwarded to CSEC.

4.9.3 Emergency Destruction

Where local conditions dictate, emergency destruction procedures for SIGINT material must be developed by each Authorized Organization, in consultation with CSEC.

4.10 Sanitization and Action-On

4.10.1 What is Sanitization?

Sanitization is the process of editing or otherwise altering SI to permit wider dissemination of useful information to non-indoctrinated persons. The primary aim of sanitization is to conceal the fact that the information is derived from COMINT, thus protecting COMINT sources, methods and techniques (see *Chapter 2: Special Intelligence Classification and Markings*).

4.10.2 What is Action-on?

Action-on is taking action based on SI. However, a user taking action based on SI can potentially tip off unindoctrinated persons or adversaries that a COMINT source is supporting the user's actions. Action-on is normally, but not necessarily, taken in conjunction with sanitization.

4.10.3 What is [redacted]

[redacted]

4.10.4 Authority for Sanitization

CSEC is the sole authority in Canada for approving sanitization and action-on requests; when appropriate, CSEC consults Second Parties on sanitization and/or action-on requests based on their product ([redacted]@cse-cst.gc.ca on CTSN).

4.10.5 Risk vs. Benefit

The use of SI outside SI channels risks divulging information about COMINT tasks, techniques or capabilities. Any decision to make such use of SI, even while applying appropriate countermeasures, must be based on the determination that the advantage to be gained in taking the action clearly outweighs the risk to, or loss of, the COMINT source. SI should be sanitized for dissemination outside of SI channels only when it cannot otherwise be used to its fullest potential.

4.10.6 When Not to Request a Sanitization

SI should not be sanitized if any of the following criteria applies:

- the intended recipient is appropriately indoctrinated and has access to the SI report;
- the information relates to the communications characteristics of a target; or
- the information is available from a non-COMINT source.

4.10.7 Sanitization Request Checklist

Clients who have a valid requirement to share SI information with a non-indoctrinated colleague must submit a request for sanitization to the Operational Policy Section at CSEC ([redacted]@cse-cst.gc.ca on CTSN) either directly or through a CSEC CRO.

Requests for sanitization must include the following:

- report serial number;
- client name, title, and department;
- rationale;
- intended recipients;
- proposed text;
- proposed classification;
- [redacted]
- any possible action-on; and
- desired due date.

Note: Sanitization procedures are available in the CSEC document CSSS-106, *End-Product Sanitization/Action-on Procedures* (available from the CSEC page on CTSN) and in a CSEC sponsored sanitization course ([redacted]@cse-cst.gc.ca on CTSN).

4.10.8 Preparing Sanitized Wording

The following guidelines should be kept in mind when preparing sanitization wording:

- the sanitized version of a SI product must present the minimum amount of intelligence required to adequately inform the intended recipient, i.e. in most cases the sanitization should be a simple statement of fact; and
- any COMINT-related details must be omitted, such as:
  - information that reveals collection sources, techniques or analytical methods,
  - information about communication or signal characteristics,
  - SI codewords or any associated caveats,
  - information for which there is no [redacted] and
  - direct quotations, which must be paraphrased.

4.10.9 Handling SECRET Paragraphs from SI Reports

Many reports (called "Write-to-Release" (WTR) or "tear-line" reports) contain paragraphs that are already classified at only the SECRET level. These SECRET paragraphs may be shared with SECRET-cleared colleagues who have a need-to-know and are not indoctrinated for SIGINT Information Access; however, no attribution may be made to a SIGINT agency. If questioned about the source of SECRET paragraphs by their non-indoctrinated colleagues, indoctrinated clients must not reveal any source-related information in their response.

Note: [redacted] allows users to preview and print SECRET versions of certain SI reports. However, users must ensure that these printed SECRET versions do not contain any marking that reveals a link to a SIGINT agency (e.g. a web address banner at the top or bottom of the printed page which identifies CSEC or another SIGINT agency).

4.10.10 Exercise SIGINT

Because of the potential for compromise of "real world" SIGINT capabilities, sources and methods, "exercise" or "simulated" SI must bear special markings to ensure that it is recognized as exercise reporting, and is handled in accordance with the procedures established for the distribution, handling, and use of SIGINT as described in these standards. CSEC's Events and Exercise team must approve all requests to use exercise SIGINT in an exercise scenario ([redacted]@cse-cst.gc.ca on CTSN).

4.10.11 What is Permission to Quote?

Permission to quote refers to wording that is taken directly from a SECRET//SI or TOP SECRET//SI report (not a GAMMA or Restricted report) and used in a second document that is:

- also marked SI; and
- disseminated within Canadian channels.

The second document must be classified at the same level as the original SI report, and recipients must be indoctrinated to SIGINT Information Access and have a need-to-know to receive the information.

Note: Approval from CSEC Operational Policy is not required to use SI in a permission to quote situation when the dissemination is:

- from a non-ORCON report;
- inside Canadian channels; or
- to an agency of a Second Party who was on the original distribution of the report, e.g. a New Zealand government organization when the original reporting dissemination was "REL to CAN, AUS, NZL and USA".

However, approval from Operational Policy is required when the wording to be used is taken from a GAMMA report or a report whose dissemination is controlled by the originator (e.g. ORCON, RELIDO).

4.10.12 Including Quoted SI Wording in Other Documents

When wording taken directly from SI-controlled reports is to be used, along with information from other sources with varying classification levels in summaries or assessments to be disseminated within national channels, the user will:

- clearly portion mark the paragraph(s) containing the SI information, e.g. "TS//SI", and apply other appropriate portion-markings, such as CEO, when applicable;
- include an attribution indicator (i.e. original SI report serial number);
- apply the overall classification, e.g. "TOP SECRET//SI ", and other markings that were afforded the original SI report to the summary or assessment; and
- ensure that the recipient or audience is indoctrinated for access to SIGINT Information Access and has a need-to-know.

Note: CSEC Operational Policy staff must approve any proposed dissemination of SI material or sanitizations of SI material that is disseminated beyond Canadian channels ([redacted]@cse-cst.gc.ca on CTSN).

See *Chapter 2: Special Intelligence Classification and Markings*, for details on how to classify information.

4.10.13 After-hours Contact for Sanitization Requests

Urgent sanitization requests related to threat-to-life situations should be directed to CSEC's 24/7 Watch Office ([redacted]@cse-cst.gc.ca on CTSN).

4.11 Security Breaches

4.11.1 What is a Security Breach?

A security breach occurs when classified or protected information or assets become the subject of unauthorized disclosure.

4.11.2 What is a Violation of SIGINT Security?

In the context of SIGINT security, a violation is considered to have occurred when there has been a failure to observe a SIGINT security regulation.

4.11.3 What is a Compromise of SIGINT?

A compromise of SIGINT occurs when SIGINT information has or could reasonably be suspected to have become accessible to an unauthorized person (e.g. an unindoctrinated person). A compromise may occur either by:

- design (e.g. espionage, defection, wilful revelation); or
- accident (e.g. mishandling, inadequate protection, communications insecurity, and other errors in the observance of security regulations).

4.11.4 Violations Involving GAMMA or ECI Material

All security violations involving GAMMA or ECI material, including:

- incidents (i.e. disclosure of GAMMA or ECI material to unauthorized persons);
- violations (i.e. procedural errors such as inappropriate storage, possibly leading to breaches);
- lost GAMMA or ECI documents; and
- possible compromises,

must be reported immediately to the CSEC Director SIGINT Requirements (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN).

At Authorized Organizations, the COMCO or Deputy COMCO (D/COMCO) must report compromises or suspected compromises to the Senior Indoctrinated Official (SIO) or to their own GCO (for GAMMA) who, in turn, must immediately inform the CSEC Director SIGINT Requirements and arrange an investigation. Authorized Organizations should also refer to their internal policies and procedures.

4.11.5 Unauthorized Exposure to SI

Unauthorized exposure or accidental compromise to any compartmented information (e.g. SI, GAMMA, ECI) does not justify a "need-to-know" or indoctrination for that particular compartment.

If, through accidental compromise, SIGINT becomes available to a non-indoctrinated person, the individual must be informed of the national security implications and be cautioned that further disclosure could constitute an offence under the *Security of Information Act* (SOIA). The person must sign the "Unauthorized Exposure to Compartmented Intelligence" form in Annex 1 of this chapter, and have it placed in their personnel security file. A Criminal Records Name Check (CRNC) and a CSIS indices check should also be conducted. The individual's consent must be obtained prior to conducting such checks.

4.12 Investigation of SIGINT Breaches

4.12.1 Investigating Breaches: General

Any breach or potential violation of SIGINT security must be reported to the relevant COMCO or D/COMCO, who must ensure that violations or potential violations of SIGINT security policy are promptly investigated. The extent of the investigation should be commensurate with the seriousness of the violation. Investigations should:

- determine whether a breach of security has occurred or is likely to occur;
- determine whether a compromise of SIGINT has occurred or is likely to occur;
- if pertinent, include a thorough search to eliminate the possibility that unaccounted for SIGINT or SIGINT assets may have been misplaced;
- identify weaknesses in security regulations;
- provide useful background information in support of security education programs; and
- identify repeat offenders.

As a general rule, breaches or security violations are not reported to CSEC unless, in the opinion of the COMCO or D/COMCO, the seriousness of the event (e.g. a continually repeated offence) warrants advice and guidance from CSEC. Employees who become aware of any security breach must notify their COMCO or D/COMCO as soon as possible.

4.12.2 Investigating a Compromise of SIGINT

The COMCO or D/COMCO must report compromises or suspected compromises of SIGINT to the Authorized Organization's Departmental Security Officer (DSO) who, in turn, must immediately inform the Director SIGINT Requirements at CSEC to arrange an investigation. The investigation, conducted in accordance with the Authorized Organization's policies and procedures for dealing with breaches of security, must determine/identify:

- how, when and where the compromise occurred;
- the potential/actual damage caused by the compromise, including an assessment as to whether the SIGINT may have become available to a foreign national(s);
- the subsequent action taken;
- weaknesses in the Authorized Organization's SIGINT security posture; and
- corrective measures to be taken.

4.12.3 Investigation Report

A copy of the investigation report must be forwarded to the Director SIGINT Requirements at CSEC (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN). Depending on the nature of the compromise and/or the potential injury to national security, CSEC will refer the matter to CSIS. If necessary, CSEC will also inform its Second Party partners.

4.12.4 Security Investigations: Sanctions

All security incidents at Authorized Organizations will be investigated according to the CSSS and internal procedures, and appropriate administrative, disciplinary or corrective action taken. Measures include, but are not limited to:

- additional training for staff involved;
- a note placed in staff members' security file;
- de-indoctrination from a compartment; and
- removal of an individual's SIGINT indoctrination (see *Chapter 7: Personnel Security* for this procedure).

Further sanctions may be taken if deemed necessary, in accordance with internal departmental policies and procedures.

4.12.5 Emergency Indoctrination

IRRELEVANT

4.13 SIGINT to NATO

4.13.1 General

IRRELEVANT

4.13.2 CSEC and NATO

4.13.3 NATO SIGINT Policy

4.13.4 NATO SIGINT Control System

NATO has its own system for the classification and protection of SIGINT. SIGINT approved for release to NATO must be classified COSMIC TOP SECRET – BOHEMIA (BOHEMIA is the designator for SI) and generally consists of material classified nationally as SECRET//SI. Only CSEC may approve the release to NATO of TOP SECRET//SI material and, when such release is authorized, that material will also bear the security classification COSMIC TOP SECRET – BOHEMIA (CTS-B). The NATO classification system is described in detail in Section 3 and Annex D of *MC-101*.

For information related to the sanitization of SIGINT for NATO, contact CSEC Operational Policy [redacted]@cse-cst.gc.ca on CTSN).

4.13.5 Indoctrination for NATO SIGINT

Individuals requiring access to information as described above must be NATO SI indoctrinated. Since NATO has no means of security vetting, it uses national indoctrinations to SIGINT Information Access as certification that individuals have been properly vetted. Thus, individuals must be nationally indoctrinated for SIGINT Information Access and hold the NATO security clearance COSMIC TOP SECRET before they may be indoctrinated to BOHEMIA (the NATO SI indoctrination).

4.14 Contact Information

4.14.1 Contact Information

Unless otherwise noted, the CTSN system may be used to contact the following offices at CSEC.

Name or Office	Contact address
Director SIGINT Requirements (*also valid on the unclassified Internet system*)	ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN
Operational Policy	[redacted]@cse-cst.gc.ca
24 hour Watch Office	[redacted]@cse-cst.gc.ca
GAMMA Control Officer	ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN
Personnel Security	[redacted]@cse-cst.gc.ca
Public Affairs Office (*on the unclassified Internet system*)	public.affairs-affaires.publiques@cse-cst.gc.ca

Annex 1: Unauthorized Exposure to Compartmented Intelligence

(This form is PROTECTED B when completed)

UNAUTHORIZED EXPOSURE TO COMPARTMENTED INTELLIGENCE

1. You have been exposed to highly sensitive intelligence that you are not authorized to access. As this intelligence is handled in compartmented security channels and requires a formal indoctrination before access is authorized, it is necessary to inform you of your obligations to safeguard this intelligence, and for you to sign the attached declaration in which you affirm these obligations.

2. Your exposure to this compartment and your signature on the attached document *does not* constitute indoctrination to the compartment.

DECLARATION TO BE SIGNED FOLLOWING UNAUTHORIZED EXPOSURE TO:

_____
(Identify Intelligence Compartment)

I, the undersigned, affirm that I will obey all the instructions pertaining to the security of the intelligence compartment identified above.

I affirm that I will not attempt to obtain further access to this compartment, nor will I discuss it with others, unless I am formally indoctrinated to the compartment.

I am aware of the provisions of the *Security of Information Act* and that all information concerning this compartment is deemed to be protected from unauthorized disclosure under the *Act*.

I understand that the preservation of this compartment is of the utmost importance to Canada, that its loss would be irreparable, and that the need to maintain security concerning this compartment never expires.

Full Name _____
(Print in Block Letters)

PRI/Service Number _____ Date of Birth _____

Classification/Rank _____ Position _____

Branch/Division/Department or Organization _____

Signature _____

Name and Title of Compartment Manager _____
(Print in Block Letters)

Signature of Compartment Manager _____

Name and Title of Personnel Security Officer _____
(Print in Block Letters)

Signature of Personnel Security Officer _____

Dated on this _____ of _____, _____, at _____
(Day) (Month) (Year) (Location/City)

Annex 2: SIGINT Indoctrination Briefing

A2.1 The following SIGINT handling briefing is used as the SIGINT Indoctrination Briefing.

A2.2 Overview This document covers the following issues related to the handling of COMINT material:

- what is COMINT?
- Special Intelligence (SI) control system;
- SI markings;
- access to SI;
- handling of SI;
- indoctrination status of others; and
- sanitization.

Note 1: For more information about SI handling procedures please refer to the *Canadian SIGINT Security Standards* (which is a CSEC document issued to all Government of Canada (GC) client departments), and related departmental procedures.

Note 2: For information about the handling procedures of non-SI classified material, please refer to your departmental procedures which are based on the *Policy on Government Security* issued by the Treasury Board Secretariat.

A2.3 What is COMINT?

Communications Intelligence (COMINT) is technical information and intelligence derived from the interception and processing of foreign communications passed by radio, wire, or other electromagnetic means.

CSEC issues end-product reports based on COMINT, and also has access to similar reports issued by our Allied Agencies (i.e. National Security Agency (US), Government Communications Head Quarters (UK), Defense Signals Directorate (Australia), and Government Communications Security Branch (New Zealand)). These reports are available to GC client departments via Client Relations Officers (CROs), and electronic means.

Because of the sensitivity of COMINT sources and related inter-agency agreements, CSEC and GC client departments must comply with community standards for handling COMINT material.

A2.4 The Special Intelligence (SI) Control System

Control systems give additional protection to classified information derived from or concerning sensitive sources, methods or techniques. An "indoctrination" consisting of a formal briefing and a signed acknowledgement is required before accessing any information protected within a control system.

The SI control system protects intelligence derived from communications intelligence by prescribing standards regarding access, marking, handling and control of COMINT information. The SI control system must never be used to provide increased security for non-SI information.

A2.5 GAMMA

The term GAMMA refers to a special control system which provides extra protection for SI end-product reports that are considered to be very sensitive. A SIGINT Information Access indoctrination does **not** provide access to GAMMA. A separate GAMMA indoctrination is required for access to GAMMA material.

A2.6 SI markings

COMINT material includes the marking "SI" in the classification line (e.g. TOP SECRET//SI).

Note: CSEC and allied agencies are converting all electronic systems and networks to recognize the marking SI in the classification line. However, because of delays in this conversion, some reports may still bear the former markings of COMINT, UMBRA, SPOKE, or MORAY (instead of SI) in the classification line. Furthermore, older SI material may feature the caveat Handle Via COMINT Channels Only, or its acronym HVCCO.

A2.7 Access to SI

For access to SI material, clients must:

- be cleared to TOP SECRET;
- have undergone a subject interview;
- be appropriately indoctrinated for SIGINT Information Access; and
- have a requirement (need-to-know) to view the material.

A2.8 Handling of SI

The following table describes key handling issues for SI documents.

Handling issue	Detail
Discussing SI	Clients may only discuss information from SI material with individuals who are appropriately indoctrinated and who have a requirement for this information. **Note 1:** It is the responsibility of the client to confirm the indoctrination status of these individuals. **Note 2:** Clients must obtain approval from the Operational Policy Section at CSEC prior to discussing a SI end-product report with a Second Party national [redacted]@cse-cst.gc.ca on CTSN).

Continued on next page

Handling issue	Detail
Including SI in other documents	All documents or briefings containing information from SI end-product reports will be afforded the same protection as the original reports, and classified at the level of the most highly classified SI. When wording taken directly from SI reports is used in another document, such as a summary or assessment, together with information from other sources and of varying classification levels, the user will: • clearly portion-mark the paragraph(s) containing the SI information, e.g. "TS//SI" for TOP SECRET//SI, and apply other appropriate portion markings, such as CEO, when applicable; • include an attribution indicator (i.e. the original SI report serial number); • apply the overall classification, e.g. "TOP SECRET//SI" and other markings that were afforded the original SI report to the summary or assessment; and • ensure that the recipient or audience is indoctrinated for SIGINT Information Access and has a need-to-know **Note 1:** SI material can only be cut-and-pasted into applications that are accredited for SI. **Note 2:** Clients must obtain approval from the Operational Policy Section at CSEC if the proposed dissemination of their documents or briefings (that include information from SI end-product reports) is beyond the original dissemination (See the paragraph in this chapter on permission to quote.) [redacted]@cse-cst.gc.ca on CTSN.)

Continued on next page

Handling issue	Detail
Printing/Storing	Clients may print SI information; however any hard copy SI material must: • display appropriate classification markings; • remain within a TOP SECRET//SI environment; and • be stored in an approved container.
E-mailing	SI material can only be transmitted electronically on networks that have been appropriately accredited by CSEC.

A2.9 Indoctrination status of others

COMINT Control Officers (COMCOs) at Authorized Organizations must maintain an updated list of staff indoctrinated for SIGINT Information Access within their respective departments, and must promptly inform the Special Material Control Officer at CSEC of any changes to this list.

The CSEC Personnel Security Office maintains a list of all GC employees who are indoctrinated for access to SI.

A2.10 Sanitization

(Sharing SI with non-indoctrinated colleagues)

Definition: Sanitization is the process of editing or disguising SI to protect sensitive sources and methods in order to release the information outside of "SI Channels".

Clients who have a valid requirement to share SI information with a non-indoctrinated colleague must submit a request for sanitization to a CSEC CRO, or to the Operational Policy Section at CSEC ([redacted]@cse-cst.gc.ca on CTSN).

Note: Information about requesting a sanitization is available in the CSSS, on CTSN from the CSEC page, and in a CSEC sponsored course.

A2.11 Handling of SECRET paragraphs from SI reports

Many reports contain paragraphs that are already classified at the SECRET level. Clients may share these SECRET paragraphs with SECRET-cleared colleagues who have a need-to-know but are not indoctrinated for SIGINT Information Access; however, no attribution can be made to a SIGINT agency. If questioned about the source of SECRET paragraphs by their non-indoctrinated colleagues, indoctrinated clients must not reveal any source-related information in their response.

Note: [redacted] allows users to preview and print SECRET versions of certain SI reports. However, users must ensure that these SECRET versions do not contain any marking that reveals a link to a SIGINT agency (e.g. a web address banner at the top or bottom of the printed page which identifies CSEC).

A2.12 Related security issues

Other security issues that apply to most Authorized Organizations are:

- the computer terminals must have password-protected screen savers that are automatically activated when the terminals are left unattended for a five-minutes or more;
- clients must shut down their computer terminals at the end of the working day to ensure any security software upgrades sent through the system overnight are loaded and installed;
- clients must not save SIGINT information to floppy disks and local hard-drives unless this is done on a SIGINT accredited network;
- clients must report all security violations and security breaches to the departmental COMINT Control Officer (COMCO); and
- clients must ensure that all hard copy SI is securely stored at the end of the work day.

A2.13 Enquiries

For more information on the handling of SI, please consult:

- the Canadian SIGINT Security Standards (CSSS) series of policy instruments;
- departmental policy and procedures;
- your departmental COMINT Control Officer (COMCO); or
- the SIGINT Requirements directorate at CSEC (ssmo-dl@cse-cst.gc.ca on the unclassified Internet o[redacted]@cse-cst.gc.ca on CTSN).

Annex 3: GAMMA Indoctrination Briefing

A3.1 Introduction

The GAMMA indoctrination briefing is intended for staff who, in order to perform their duties, require access to SIGINT reports and related material (e.g. briefing documents) that are classified TOP SECRET//SI-GAMMA.

A3.2 Content of briefing

The GAMMA indoctrination briefing provides a high-level description of the GAMMA sub-control system, and includes related information about access, classification markings, and handling standards. CSEC document CSSS-104, *GAMMA Handling Standards,* provides a more detailed description of the GAMMA sub-control system.

A3.3 What is GAMMA?

The term GAMMA refers to a special sub-control system which provides extra protection for SIGINT reports and related material that are considered to be very sensitive. The sensitivity of these reports relates to one or more of the following:

- the topic;
- the target;
- the collection method; or
- the technique used to analyze or process the intercept.

A3.4 GAMMA vs. ECI

The GAMMA and the Exceptionally Controlled Information (ECI) sub-control systems both provide optimum protection for SIGINT information. The main difference between the two is that GAMMA is used to protect SIGINT reports, whereas ECI is used to protect information about SIGINT operations and is never applied to SIGINT reports. SIGINT reports resulting from ECI sources or techniques may be issued within the GAMMA sub-control system.

A3.5 GAMMA markings

GAMMA end-product reports feature the classification and control system marking of TOP SECRET//SI-GAMMA, and include the [redacted] in the serial number (e.g. [redacted] The markings can also include other restrictive caveats such as Originator Controlled (ORCON), or Canadian Eyes Only (CEO).

A3.6 Access to GAMMA

For access to any GAMMA material, staff must:

- be cleared to TOP SECRET;
- have a Subject Interview;
- have held a SIGINT Information Access (SIA) indoctrination for a minimum of six months, or have received a waiver from CSEC's Director SIGINT Requirements;
- be indoctrinated for GAMMA; and
- have a requirement to view the material.

A3.7 Handling of GAMMA The following table describes key handling issues for GAMMA documents.

Handling issue	Detail
Including GAMMA in other documents	All documents or briefings containing information from GAMMA end-product reports will be afforded the same protection as the original reports and therefore include the classification marking of TOP SECRET//SI-GAMMA. At Authorized Organizations, these documents must be registered with the GAMMA Registry. When wording is taken directly from a report classified GAMMA and used in another document, such as a summary or assessment, together with information from other sources and of varying classification levels, the user will: • clearly portion-mark the paragraph(s) containing the GAMMA information, e.g. "TS//SI-G" for TOP SECRET//SI-GAMMA" and apply other appropriate portion markings, such as CEO, when applicable; • include an attribution indicator (i.e. the original report serial number); • apply the overall classification, e.g. "TOP SECRET//SI-GAMMA," and other markings that were afforded the original GAMMA report to the summary or assessment; and • ensure that the recipient or audience is indoctrinated for access to GAMMA and has a need-to-know.

Continued on next page

Handling issue	Detail
Discussion	The user may only discuss information from GAMMA documents with individuals who are indoctrinated for GAMMA and who have a requirement to see this information. It is the responsibility of the user to confirm the indoctrination status of these individuals.
Storage	GAMMA documents may be held in a TOP SECRET//SI environment, provided that: • the holder is indoctrinated for GAMMA; • the documents are protected from the view of persons who are not indoctrinated for GAMMA; and • the documents are locked in approved containers when not in use.
Mailing	GAMMA documents are mailed in sealed envelopes that are addressed only to those indoctrinated for GAMMA. GAMMA documents must be hand-delivered by CROs or by couriers cleared to TOP SECRET and indoctrinated for SIGINT Information Access.
Electronic/soft copy	GAMMA documents can only be transmitted or handled/stored electronically on IT networks or systems that have been approved by CSEC to handle TOP SECRET//SI-GAMMA information.

A3.8 Who else has GAMMA?

Queries concerning GAMMA indoctrinations should be directed to GAMMA Control Officers (GCOs) at Authorized Organizations or to the CSEC GCO (Director SIGINT Requirements) at ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN.

CSEC Personnel Security Services maintain a master list, in [redacted] database, of all individuals within the GC who are indoctrinated for access to GAMMA. A link to this database is available on the CTSN site. [redacted]

CHAPTER 5

PROTECTION OF ELINT AND FISINT

Chapter 5: Protection of ELINT and FISINT

5.1 Introduction

5.1.1 Contents This chapter contains the following topics:

Topic
5.1 Introduction
5.2 Electronics Intelligence (ELINT)
5.3 ELINT and COMINT
5.4 Classification of ELINT
5.5 Authorization to receive ELINT
5.6 Foreign Instrumentation Signals Intelligence (FISINT)
5.7 Violations

5.1.2 Introduction

This chapter describes the handling procedures for ELINT and FISINT. As discussed in *Chapter 2: Special Intelligence Classification and Markings*, ELINT and FISINT reports are often classified solely in the national interest. Accordingly, ELINT and FISINT are generally handled according to departmental procedures for the handling of classified information which are based on the *Policy on Government Security Policy* (PSG) and related standards; however, there are certain specific procedures for handling ELINT and FISINT that contain COMINT, and these are addressed in this chapter.

Note: The CSEC document CSSS-103, *The SIGINT Classification System*[6], provides details on different classification markings. CSSS-103 is available from the CSEC page on the CTSN central site.

[6] Formerly OPS-5-14.

5.2 Electronic Intelligence (ELINT)

5.2.1 What is ELINT?

Electronic Intelligence (ELINT) is technical information and/or intelligence derived from the collection, processing, and analysis of electromagnetic non-communication emissions (e.g. radar, navigation aids, jamming systems and some remote control systems).

5.2.2 Classification

By definition, ELINT is a component of SIGINT; however, the requirements for the protection of ELINT are normally less restrictive than those established for the protection of COMINT.

Generally, ELINT is classified in the national interest (i.e., CONFIDENTIAL, SECRET or TOP SECRET) and, therefore, is subject to *Policy* on *Government Security* (PGS) personnel, physical and information technology (IT) standards for access to and safe handling of classified information.

5.2.3 Need for Authorized Organization Status

Government departments, including their private contractors, which receive only ELINT classified in the national interest, do not need to request Authorized Organization status. (Authorized Organization status is mandatory for departments receiving and retaining SI, see *Chapter 3: Departmental Requests for Access to Special Intelligence.*)

5.2.4 Dissemination

Although ELINT generally is classified in the national interest and is subject to different security requirements than those for safeguarding COMINT, ELINT remains a component of SIGINT. Dissemination of ELINT, therefore, is subject to the stipulations set out in this document.

For convenience and to ensure secure handling when ELINT is or is likely to be worked on in association with COMINT, ELINT should be handled in SI channels. However, when transmitted/transported in SI channels, such ELINT information must not be marked with any caveat that would restrict access only to SIGINT Information Access-indoctrinated persons.

5.2.5 Access

Access to ELINT is based on the need-to-know principle and the following direction:

- individuals who require access **only** to ELINT classified in the national interest are subject to normal security clearance procedures for access to classified information, but do not need to be indoctrinated for SIGINT Information Access; and

- individuals who have access to ELINT must be Canadian citizens. (Second Party secondees are excepted. Normally, such persons are appropriately security cleared by their own national authority prior to their secondment; otherwise, arrangements are made via CSEC. Contact [redacted]@cse-cst.gc.ca on CTSN).

Where staff includes integrated personnel, care must be taken to observe the restrictions imposed on the distribution of ELINT in accordance with departmental guidelines.

5.2.6 Contractors/ Consultants

ELINT may be released to appropriately GC-sponsored contractors or consultants with the approval of the Canadian national SIGINT authority, CSEC. CSEC consults with Second Parties on requests from contractors or consultants to work with ELINT originated by them.

In addition to meeting GC personnel screening standards for access to classified information, GC contractors who are to retain ELINT on their premises for the duration of a contract must also meet GC physical security standards (and, if applicable, IT security standards) as set out in the PGS and associated GC documentation, such as the *Operational Security Standard: Management of Information Technology Security* (MITS). Contractors' facilities approved for retention of ELINT must be re-accredited by CSEC prior to receiving and retaining any SI material.

5.3 ELINT and COMINT

5.3.1 Classification of ELINT Connected to COMINT

If an ELINT item has a direct connection with COMINT (e.g. it is combined with SI-controlled material), it bears the classification and control system markings corresponding to the highest category of COMINT involved, and is handled and disseminated according to the standards required for the protection of COMINT (i.e. it is retained in SI channels and disseminated only to SIGINT-indoctrinated persons). (See *Chapter 2: Special Intelligence Classification and Markings*.)

Note: For information on sanitizing SI-controlled material, see *Chapter 4: Protection of SIGINT Information.*

5.3.2 ELINT Classified Higher than Associated COMINT

If the ELINT information is of a higher security classification than the associated COMINT, the higher classification is used along with the relevant SI control system markings.

For example, ELINT classified TOP SECRET combined with COMINT material classified SECRET//SI is marked TOP SECRET//SI (see *Chapter 2: Special Intelligence Classification and Markings*).

5.3.3 ELINT and Sensitive Sources

ELINT may also be derived from other sensitive special collection sources, and therefore, may be subject to control requirements for that specific collection source. Normally, when details of source and method of exploitation are removed, such information may be released at the SECRET or TOP SECRET level.

ELINT material that is classified at the TOP SECRET//SI level is subject to the control requirements prescribed in the Information Systems Security Plan (ISSP) held by each Authorized Organization as part of the Information Management and Security program. (Contact the Authorized Organization Information Systems Security Officer (ISSO) for information.)

Note: All modifications or sanitizations of ELINT must be approved by Operational Policy at CSEC ([redacted]@cse-cst.gc.ca on CTSN).

5.4 Classification of ELINT

5.4.1 General Classification

ELINT is classified UNCLASSIFIED, CONFIDENTIAL, SECRET or TOP SECRET, depending on the:

- sensitivity of the content;
- method of intercept, technical evidence; and/or
- analytical techniques involved.

ELINT end-product reporting often bears dissemination control markings (e.g. Canadian Eyes Only). Examples of reasons for ELINT to be classified in the national interest follow; the examples described under SECRET and CONFIDENTIAL may require TOP SECRET or National Special Center protection if they are particularly sensitive.

5.4.2 ELINT Classified TOP SECRET or Above

ELINT that is classified TOP SECRET or beyond (e.g. TOP SECRET//SI) includes the following:

[redacted]

Note: ELINT classified at TOP SECRET and above may be subject to special handling and dissemination controls as described in this chapter.

5.4.3 ELINT Classified SECRET

ELINT that is classified SECRET includes the following:

[redacted]

5.4.4 ELINT Classified CONFIDENTIAL

ELINT that is classified CONFIDENTIAL includes the following:

[redacted]

5.4.5 UNCLASSIFIED ELINT

UNCLASSIFIED ELINT includes the following:

[redacted]

5.5 Authorization to Receive ELINT

5.5.1 How to Request ELINT Service

A senior level manager at a GC organization must forward a request for ELINT to the CSEC Director SIGINT Requirements (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN). A CSEC representative may assist this manager in the definition of the request for ELINT.

5.5.2 Review of Request

Upon receipt of a GC organization's request to receive ELINT, Director SIGINT Requirements will:

- review the client's request to determine if:
  - the client's stated business case is consistent with CSEC's mandate,
  - CSEC has the appropriate resources;
- approve or deny the client's request; and
- provide a reply to the client, which includes required follow-up action by the client.

5.5.3 Indoctrination Process

As laid out in this chapter, non-SI controlled material (e.g. ELINT) is treated according to departmental procedures which are based on the PGS.

A new client must have the appropriate clearance to view material classified in the national interest (e.g. TOP SECRET, SECRET, or CONFIDENTIAL); however, indoctrination for SIGINT Information Access is not required.

5.6 Foreign Instrumentation Signals Intelligence (FISINT)

5.6.1 Definition

FISINT is technical and intelligence information derived from the intercept of foreign instrumentation signals (FIS). FIS are defined as electromagnetic emissions associated with the testing and operational deployment of foreign aerospace, surface, and sub-surface systems, which may have either military or civilian application. FISINT includes, but is not limited to:

- signals from telemetry;
- beacon systems;
- electronic interrogators;
- arming, fusing, or firing systems; and
- computer command signals.

5.6.2 Classification, Handling, and Dissemination

The security requirements for FISINT are similar to those for ELINT, i.e. FISINT is classified according to normal rules for classifying information in the national interest when it is derived from conventional collection sources or when evidence of special collection sources and methods of exploitation have been removed. Certain FIS data and analysis are specially controlled and compartmented, but can be decompartmented for reporting at the SECRET or TOP SECRET level. FISINT end-product may also bear dissemination control markings.

5.6.3 FISINT and COMINT

If FISINT is derived from or fused with COMINT, the resulting product is subject to the classification standards and control markings established for the protection of COMINT (see *Chapter 2: Special Intelligence Classification and Markings*).

5.6.4 Access to FISINT

Access to FISINT end-product reporting classified SECRET or TOP SECRET in the national interest requires normal security clearance procedures for access to classified information. However, persons involved in or requiring access to compartmented FISINT data, analysis and reporting, as in the case of compartmented ELINT, must be indoctrinated to Special Access (see *Chapter 7: Personnel Security* for more information) and appropriate special compartmented control systems. Release of FISINT end-product reporting to contractors and consultants must be approved by CSEC ([redacted]@cse-cst.gc.ca on CTSN).

5.6.5 POC for FISINT

For more detailed information about FISINT collection, contact [redacted], at:

18 ST MGen George R. Pearkes Bldg,
101 Col By Drive,
Ottawa Ont K1A 0K2

5.7 Violations

5.7.1 Violations

Any security breach or incident involving ELINT and FISINT that is only classified in the national interest (i.e. CONFIDENTIAL, SECRET, TOP SECRET) must be treated according to departmental procedures for the handling of classified information, which are based on the PGS and related standards.

Any security breach or incident involving ELINT and FISINT that is marked as SIGINT must be handled according to the procedures outlined in this document in *Chapter 4: Protection of SIGINT Information*, and in *Chapter 7: Personnel Security*.

CHAPTER 6

SIGINT CERTIFICATION AND ACCREDITATION

Chapter 6: SIGINT Certification and Accreditation

6.1 Introduction

6.1.1 Contents This chapter contains the following topics:

Topic
6.1 Introduction
6.2 The SIGINT Certification and Accreditation Process
6.3 Physical Security Accreditation
6.4 Identified Security Roles at Authorized Organizations
6.5 Security Disciplines

6.1.2 Introduction This chapter describes the SIGINT certification and accreditation (C&A) process that applies in any Government of Canada (GC) organization that makes a request to CSEC to retain and/or process SI (after which, the organization is referred to as an "Authorized Organization". See *Chapter 3: Departmental Requests for Access to Special Intelligence*). The C&A process ensures that a CSEC-approved, cost-effective balance of security safeguards is implemented by the client organization to properly protect any SI it stores.

6.1.3 Context The Chief, CSEC (CCSEC), as manager of the SIGINT program in Canada, is responsible for all aspects of SIGINT policy, operation and administration. Responsibility for SIGINT security policy is delegated to the Deputy Chief, SIGINT (DC SIGINT). CSEC issues the Canadian SIGINT Security Standards (CSSS) as the lead agency for SIGINT security in Canada, and thereby sets SIGINT standards, for the certification and accreditation of facilities and Information Technology (IT) systems that handle SIGINT. Therefore, CSEC has a role not only in ensuring the security of its own SIGINT facilities and networks through C&A, but also in ensuring that other GC organizations with facilities and/or systems that process SIGINT have the appropriate C&A.

Continued on next page

6.1.3 Context (continued)

CSEC also has a responsibility under the *Policy on Government Security* (PGS) and the *Operational Security Standard: Management of Information Technology Security* (MITS) Standard with respect to C&A of all its IT systems. [redacted]

6.2 The SIGINT Certification and Accreditation Process

6.2.1 Purpose of Certification and Accreditation

The purpose of certification is to verify that the security requirements established for a particular system or service are met and that the controls and safeguards work as intended.

The purpose of a physical security accreditation is to establish the extent to which a particular facility meets security requirements, and ensures that appropriate security measures are established to protect the operating environment (see Section 6.3).

The purpose of IT systems accreditation is to signify that management has authorized the system or service to operate and has accepted the residual risk of operating the system or service, based on the certification evidence (MITS). Once systems have been certified and accredited, the SIGINT Operational Authority will grant the Authority to Operate. See *Chapter 8: Information Security for SIGINT Systems* for information on the accreditation process for IT systems.

6.2.2 Certification and Accreditation Policy

As per the PGS, CSEC is responsible for developing, approving and promulgating COMSEC- and SIGINT-related policy instruments for classified information and developing guidelines and tools related to IT security. Through this responsibility, the following standards are applied:

- Director SIGINT Requirements is the approval authority for requests from Client Organizations to access SIGINT information;
- GC organizations must be granted an Authority to Operate to access SIGINT information, after which they become Authorized Organizations;

Continued on next page

6.2.2 Certification and Accreditation Policy (continued)

- CSEC provides advice and assistance in the interpretation of operational standards and technical documentation related to SIGINT, Communications Security (COMSEC), and IT Security in terms of system C&A, risk and vulnerability analysis, product evaluation, system and network security analysis; and
- CSEC provides advice and assistance to departments on operational standards and technical documentation developed by CSEC.

6.2.3 Description of the SIGINT C&A Process

Once Director SIGINT Requirements receives a client request to access SIGINT information, and validates the business requirement, s/he will contact the appropriate stakeholders within CSEC to coordinate and assist the Client in defining and meeting the security requirements to obtain accreditation for their project/program, facility and/or system.

6.2.4 Details about Threat and Risk Assessments (TRA)

The next step in the C&A process involves the completion of a Threat and Risk Assessment (TRA) by the GC organization. The TRA is a part of risk management concerned with defining what requires protection, analyzing and assessing threats, analyzing and assessing risks, and making recommendations for the management of those risks.

The TRA must identify all security factors unique to the organization. These factors must then be reflected in the specific safeguards chosen.

6.2.5 CSEC Questionnaires/ Documentation

The GC organization seeking C&A must complete any questionnaires or related documentation CSEC requires after implementing the safeguards required by CSEC following the TRA.

6.3 Physical Security Accreditation

6.3.1 What is Physical Security Accreditation?

IRRELEVANT

6.3.2 Re-accreditation	IRRELEVANT
6.3.3 Balancing Security Measures	
6.3.4 Securing and Classifying Documentation	

[7] The U.S. refers to these facilities as Sensitive Compartmented Information Facilities (SCIFs).

6.4 Identified Security Roles at Authorized Organizations

6.4.1 Security Roles

The PGS and related standards have defined the security roles that must be identified and filled for organizations that have access to classified information. These roles include the:

- Departmental Security Officer (DSO);
- IT Security Coordinator (ITSC); and
- COMSEC authority or custodian.

For organizations with access to SI, the following roles must also be identified and filled:

- Senior Indoctrinated Official (SIO);
- COMINT Control Officer (COMCO);
- Deputy COMINT Control Officer (D/COMCO); and
- Information Systems Security Officer (ISSO).

In addition, in instances where the organization wishes to store GAMMA material on its premises (Authorized Organizations only), an individual must be identified to fill the role of GAMMA Control Officer (GCO). This can be the same person as the COMCO or D/COMCO.

See *Chapter 3: Departmental Requests for Access to Special Intelligence* for the responsibilities associated with each of these roles.

6.5 Security Disciplines

6.5.1 Security Disciplines

IRRELEVANT

Security Discipline	Examples of Security Features and Safeguards
IRRELEVANT	
Network Security	• network Security Zones (see *Chapter 8: Information Security for SIGINT Systems*); • requirements for TEMPEST; • authorizing/monitoring physical access; • storage/disposal of IT media and other assets; • vulnerability scans; • connection of different networks; and • monitoring of access to networks.

Continued on next page

Security Discipline	Examples of Security Features and Safeguards
Communications	• monitoring • network security and data integrity • COMSEC procedures (e.g. encryption)
Hardware	• use of devices such as routers, firewalls • hardware security control and maintenance
Software	• authorize, monitor and review the use of software • quality assurance and acceptance testing • access control, surveillance (e.g. user profiling) • database administration • anti-virus software • intrusion detection software • configuration management • malicious software management • software security controls • e-mail security
OPS Security (CONOPS, USOPS)	• mode of operation • day-to-day procedures and control • detection and surveillance records • cut-and-paste/printing/storage • backup and recovery plans • system access controls • user accounts and media control

CHAPTER 7

PERSONNEL SECURITY

Chapter 7: Personnel Security

7.1 Introduction

7.1.1 Contents This chapter contains the following topics:

Topic
7.1 Introduction
7.2 Categories of SIGINT Indoctrinations
7.3 Access to SIGINT
7.4 Indoctrinations, De-indoctrinations, Transfers, and Updates
7.5 Record Keeping
7.6 Sanctions
7.7 Personal Responsibilities
7.8 Point of Contact

7.1.2 Personnel Security Standard The requirements for access to SIGINT are established in accordance with CSEC's role and responsibilities as lead agency for SIGINT security in Canada, and are to be applied in conjunction with the Government's *Personnel Security Standard*. Government of Canada (GC) departments may add additional requirements as they see fit for their own personnel.

7.2 Categories of SIGINT Indoctrinations

7.2.1 General All persons who require direct access to Special Intelligence (SI) and SI-related information must be cleared to TOP SECRET SIGINT Information Access (see 7.2.5). Persons whose duties will result in indirect access to SI and SI-related information must be cleared to TOP SECRET SIGINT Facility Access (see 7.2.3).

7.2.2 Categories of SIGINT Indoctrinations

IRRELEVANT

7.2.3 SIGINT Facility Access (SFA)

7.2.4 SIGINT Indoctrination

7.2.5 SIGINT Information Access (SIA)

7.2.6 SIGINT Information Access Security Clearance Update

SIGINT security clearance updates must be conducted in accordance with the *Personnel Security Standard* referenced in the *Policy on Government Security* (PGS). The mandatory subject interview must also include a review of SIGINT security principles as described in CSEC's SIGINT Indoctrination Briefing Package (see this chapter).

7.2.7 Indoctrinating Ministers and Senators

By virtue of their positions and oaths of office, federal Ministers and Senators are eligible for access to TOP SECRET//SI and GAMMA information [redacted] When access to TOP SECRET//SI or GAMMA is required Ministers and Senators must be provided with an indoctrination briefing similar to that given to all other individuals indoctrinated for access to SI or GAMMA (see Chapter 4, Annex 2 and Annex 3).

By virtue of their position and Privy Councilor's oaths, the following ministers do not require formal indoctrinations and are granted full access to all ECI programs:

- Prime Minister;
- Deputy Prime Minister;
- Minister of National Defence;
- Minister of Foreign Affairs;
- Minister of Public Safety; and
- Minister of Justice and Attorney General of Canada.

As with access to TOP SECRET//SI and GAMMA information, the above ministers must receive a briefing on the sensitivity of ECI. All other ministers requiring access to specific ECI programs must be formally indoctrinated per CSSS-102, *ECI Handling Standards*.

7.3 Access to SIGINT

7.3.1 Access to SIGINT: General

Access to SI control or sub-control systems (i.e. GAMMA, ECI) by an individual is contingent upon application of the need-to-know principle and observation of those practices that ensure the security and integrity of the control system. An individual's access to SIGINT may be reduced or discontinued if the person does not follow SIGINT security practices (see this chapter for sanctions).

Note: See *Chapter 2: Special Intelligence Classification and Markings* for more detailed information on SIGINT control and sub-control systems.

7.3.2 Prerequisites for Direct Access to SIGINT

All persons who require direct access to SI and SI-related information must:

- be a Canadian citizen (see this chapter for information on integrees [redacted]
- hold a TOP SECRET security clearance ;
- have successfully completed a subject interview for Special Access to compartmented intelligence ("Special Access" replaces "SIGINT" which was formerly used); and
- be indoctrinated to SIGINT Information Access (SIA) (formerly CAT III).

7.3.3 Access to SIGINT: Integrees [redacted]

Integrees [redacted] must be security cleared to an equivalent level, and indoctrinated to SIGINT information access by [redacted] SIGINT authority prior to their integration. Integrees [redacted] must attend a Canadian Indoctrination Awareness Briefing session.

7.3.4 ELINT and FISINT

ELINT and FISINT information, although component parts of SIGINT, are not considered as sensitive as COMINT. Therefore, personnel working with these types of information do not necessarily require Special Access indoctrinations; however, they must be cleared to the appropriate level for the material's classification (i.e. CONFIDENTIAL, SECRET, TOP SECRET). See *Chapter 5: Protection of ELINT and FISINT*.

7.3.5 Procedure for Direct Access to SIGINT/ SI

Requests for an individual's direct access to SIGINT/SI information should follow the steps in the table below.

Note: Where an applicant for the SIGINT indoctrination is geographically so removed from the department COMCO or a CSEC representative that they cannot conduct the indoctrination, CSEC Personnel Security will authorize a representative from CSIS or DND to act on CSEC's behalf to conduct the indoctrination, on a case-by-case basis.

Step	Who does it	Action
1	Sponsoring authority in the department requesting direct access to SIGINT/SI on behalf of an individual	• Submits a request by e-mail or letter, including: ◦ full name ◦ date of birth ◦ place of birth ◦ issue date of the TOP SECRET clearance ◦ date of the subject interview ◦ justification of the individual's need to have access to SIGINT to the ◦ COMCO (in Authorized Organizations) ◦ CSEC Client Relations Officer (CRO) (in Client Organizations).
2	COMCO or CSEC representative	• Confirms applicant has valid TOP SECRET Special Access clearance (including subject interview) and a need-to-know.

Continued on next page

Step	Who does it	Action
3	Departmental Security Officer (DSO)	• If applicant is not yet appropriately cleared, processes TOP SECRET security clearance request (processing must include a subject interview conducted either by CSIS or the department).
4	COMCO or CSEC representative	• Indoctrinates applicant (see subsequent paragraphs regarding indoctrination) • Sends the original request from the sponsoring authority (see step #1) and the original signed indoctrination form (CSEC/CSTC SEC-047) to CSEC Personnel Security for retention. Note: hard copy forms are used for these transactions due to the privacy and security risks of using unencrypted e-mail on the Internet. • Ensures a copy of the signed indoctrination form remains with the COMCO for department files.
5	CSEC Personnel Security Office	• Updates the National SIGINT Registry.

7.3.6 Mandatory Subject Interviews

A subject interview is mandatory:

- as part of the initial TOP SECRET security clearance process for Special Access to SIGINT (i.e. the CSIS or departmental subject interview);
- during five-year security updates for continued Special Access to SIGINT (departments are responsible for conducting their own subject interviews for the five year update cycle); and
- for cause for any level of security clearance.

7.3.7 Conducting Subject Interviews

Interviews should be conducted face-to-face where possible.

7.3.9 Security Clearance Re-activation

A SIGINT security indoctrination may be re-activated within 12 months of the end of continuous employment by conducting a:

- credit check;
- Criminal Records Name Check (CRNC); and
- CSIS indices check.

In addition, an updated subject interview and re-indoctrination may be required depending on circumstances. The departmental security authorities will make this decision on a case-by-case basis.

7.4 Indoctrinations, De-indoctrinations, Transfers, and Updates

7.4.1 Forms for Indoctrination and De-indoctrination

All relevant forms will be provided by CSEC Personnel Security [redacted]@cse-cst.gc.ca on CTSN). Forms used for the basic SIGINT Information Access indoctrination are as follows:

- CSEC/CSTC #047, Indoctrination Form; and
- CSEC/CSTC #048, De-indoctrination Form.

Forms used for indoctrination to/de-indoctrination from SI sub-compartments (e.g. GAMMA, ECI) are as follows:

- SEC-007, Special Indoctrination Request;
- SEC-008, Special Indoctrination Form; and
- SEC-009, Special De-Indoctrination Form.

7.4.2 Who Conducts Indoctrinations?

Departmental COMCOs, D/COMCOs, GCOs, and CSEC CROs will normally indoctrinate new clients requiring SIGINT Information Access and/or GAMMA access in Authorized Organizations. In exceptional circumstances, the CSEC SIGINT Security Management Office (SSMO) may indoctrinate clients for SIGINT Information Access and/or GAMMA access.

7.4.3 Emergency Indoctrinations

Requests for emergency indoctrinations for access to SIGINT should be sent to the Director SIGINT Requirements at CSEC (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN). An information copy must also be sent via secure means to CSEC Personnel Security ([redacted]@cse-cst.gc.ca on CTSN).

7.4.4 Indoctrination Briefing Package

CSEC's Indoctrination Briefing package, which is provided by CSEC's SIGINT Security Management Office (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN), to those persons authorized to indoctrinate, provides full details on the process. It includes a formal indoctrination briefing along with form CSEC/CSTC #047, which must be signed and completed.

7.4.5 Waiving an Indoctrination

During exceptional circumstances (e.g. a national or international crisis) where there is a demonstrated operational requirement, certain aspects of an individual's security clearance and/or indoctrination may be waived. A request for a waiver must be sent to the Director SIGINT Requirements on CTSN.

All waivers must be approved by the Director SIGINT Requirements at CSEC (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN) with an information copy to CSEC Personnel Security ([redacted]@cse-cst.gc.ca on CTSN).

7.4.6 De-Indoctrination

De-indoctrination is the act of formally "signing off" indoctrinated persons who no longer require access to SIGINT, specifically SI. Responsibility for conducting the de-indoctrination at an Authorized Organization rests with the COMCO or D/COMCO, but the COMCO may also delegate this responsibility to a CSEC representative.

The de-indoctrination briefing contains the following elements:

- completing the De-Indoctrination form, CSEC/CSTC #048;
- ensuring that the individual understands that he/she will no longer have access to SIGINT, specifically SI;
- ensuring that the individual is aware of the provisions of the SOIA and the *Criminal Code* that apply, for life, to the confidentiality of classified information;
- the formal withdrawal of the individual's access privileges to SSAs and SIGINT-related information technology (IT) systems; and
- sending the original form to CSEC Personnel Security for retention and deletion of the person's name from the National SIGINT Registry.

Note: At CSEC, only designated personnel in the Corporate Security Directorate may carry out de-indoctrinations for CSEC staff.

7.4.7 Exceptions to Formal De-Indoctrination

There may be occasions when it is not possible to conduct a formal de-indoctrination briefing. In such cases, the individual may be administratively de-indoctrinated, and CSEC Personnel Security ([redacted]@cse-cst.gc.ca on CTSN) must be informed via secure means. CSEC will review each situation on a case-by-case basis, and advise on follow-on action as appropriate.

In an administrative de-indoctrination, the person conducting the de-indoctrination may sign the form on behalf of the person being de-indoctrinated. The person who has been de-indoctrinated must be informed of the de-indoctrination as soon as possible after the fact.

7.4.8 Transfer of Indoctrination Status

A SIGINT Information Access indoctrination is normally not transferable when an indoctrinated person moves from one GC organization to another. However, it may be transferred in the case of a secondment or other temporary assignment where it has been determined that access to SI is required for the new position. CSEC Personnel Security must be consulted about exceptions.

7.4.9 Transfer Within the Same Organization

Persons being transferred from one position to another within the same organization need not be de-indoctrinated if need-to-know in their new position has been established prior to their move; otherwise, such persons must be de-indoctrinated.

7.5 Record Keeping

7.5.1 Security Clearance and Indoctrination-Related Records

Where the COMCO or D/COMCO has been authorized to conduct indoctrinations, the COMCO office will retain a copy of the indoctrination forms.

7.5.2 Retention Period for Forms

CSEC will keep the original indoctrination forms for its employees indefinitely.

The original files will be maintained by CSEC Personnel Security as active as long as the person is employed at CSEC. After separation, the security office will hold the files for an additional two (2) years; they are then transferred to the records office where they are retained until the person reaches, or would have reached the age of 80, and are then disposed of.

Authorized Organizations will keep copies of the originals for as long as is necessary for operational purposes (time frames established for departmental retention and disposal schedules could be used as a guideline).

7.5.3 Lists of SIGINT-Indoctrinated Personnel

The COMCO in each Authorized Organization must maintain a current list of:

- the department's SIGINT-indoctrinated personnel; and
- their positions

and must provide this list to the Personnel Security Office at CSEC at the end of each calendar year, or whenever requested ([redacted]@cse-cst.gc.ca on CTSN). The COMCO must also promptly inform CSEC of any changes in the indoctrination status (i.e. indoctrination or de-indoctrination) of an individual.

The list must include:

- the first, all middle, and the last name of indoctrinated persons;
- the date and place of birth;
- position title;
- company name (if a contractor or consultant);
- military service number or personal record identifier; and
- indoctrination level (i.e. SIA or SFA).

Under specific government-wide responsibilities outlined in the PGS, CSEC is responsible for maintaining the national inventory of personnel cleared and indoctrinated for access to SIGINT.

7.5.4 Verification of SIGINT-Indoctrinated Personnel Lists

CSEC Personnel Security will periodically request that each Authorized Organization confirm its list of personnel indoctrinated for SIGINT Information Access as compiled by CSEC based on indoctrination and de-indoctrination forms submitted, and other amendments or corrections received.

7.6 Sanctions

7.6.1 General

Persons who do not observe proper SIGINT security practices will be subject to sanctions. Sanctions will vary, depending on the frequency and/or seriousness of the violation(s) (see *Chapter 4: Protection of SIGINT Information*).

Examples of sanctions are:

- a notation in the person's security file;
- reduced access to SIGINT;
- removal of SIGINT indoctrination;
- removal of security clearance; or
- criminal prosecution.

7.6.2 Authority to Reduce or Remove SIGINT Access

CSEC or Authorized Organizations may reduce or remove SIGINT access for security reasons. Authorized Organizations are to notify CSEC immediately of any intent to reduce or remove a person's SIGINT access.

7.6.3 Removal of SIGINT Indoctrination

A SIGINT, GAMMA, or ECI indoctrination may be removed in the case of a security concern by following the procedure below:

Step	Who	Does What
1	COMCO at the Authorized Organization	• Notifies Director SIGINT Requirements, at CSEC of security concerns with a person. Concerns must be serious enough to call into question the person's continued access to the compartment.
2	Director SIGINT Requirements, at CSEC	• Consults the COMCO at the Authorized Organization, the Authorized Organization Personnel Security, CSEC Personnel Security, and other departments or agencies (e.g. CSIS) as needed to substantiate the concerns. • Investigates concerns. • If concerns are substantiated, recommends to Deputy Chief, SIGINT (DC SIGINT) that the indoctrination be removed.
3	DC SIGINT at CSEC	• Approves or rejects the recommendation. • Asks the Director SIGINT Requirements to advise the COMCO at the Authorized Organization of the decision.
4	COMCO at the Authorized Organization	• De-indoctrinates the person from the compartment if the decision was to revoke the indoctrination.
5	Personnel Security at the Authorized Organization, or Personnel Security at CSEC	• Enters the de-indoctrination into the person's security file.
Note: The subject of this process may appeal the de-indoctrination decision: • through the Authorized Organization COMCO to the DC SIGINT at CSEC; or • to the Chief, CSEC (CCSEC) as the last recourse.		

7.6.4 Unauthorized Exposure to SI

Unauthorized exposure or accidental compromise to any compartmented information (e.g. SI, GAMMA, ECI) does not justify a "need-to-know" or indoctrination for that particular compartment. Rather, it is considered a security incident which must be recorded and investigated according to the procedures outlined in *Chapter 4: Protection of SIGINT Information.*

7.7 Personal Responsibilities

7.7.1 Change in Personal Circumstances

Personnel who have access to either of the SIGINT indoctrination levels (SIA or SFA) must re-submit the Personnel Security Clearance Questionnaire (form TBS/SCT 330-60E) to their departmental security officer when there is a change in personal status including, but not limited to, the following examples:

- legal change of name (CSEC Personnel Security must be informed of the name change);
- change in marital status; or
- change in living arrangements (such as sharing of living quarters).

Any additional personal circumstances that may affect an individual's security clearance should be discussed with the Departmental Security Officer (DSO).

7.7.2 Private Travel

There are no standing travel restrictions for SIGINT-indoctrinated personnel, and there are no longer any post-employment travel restrictions for de-indoctrinated personnel.

However, with the exception of those Authorized Organizations where reporting of personal travel abroad is mandatory, any SIGINT-indoctrinated person who plans to travel abroad should inform his or her COMCO who, in turn, can notify the individual of any special security concerns associated with the destination.

7.7.3 Reporting Contacts

SIGINT-indoctrinated persons are obliged to report to their COMCO [redacted] any "untoward contact" whether by a foreign national or a Canadian, in Canada or abroad. Untoward contact is defined as any contact in which illegal or unauthorized access is sought to sensitive information. It can also be interpreted as any concern arising when an individual believes they are or have been the target of an attempted exploitation to obtain sensitive material or assets. This includes any unauthorized contact with non-allied foreign diplomats/military/consular officials.

7.8 Point of Contact

7.8.1 Point of Contact at CSEC

For additional information contact your COMCO or Director SIGINT Requirements, at CSEC (ssmo-dl@cse-cst.gc.ca or [redacted]@cse-cst.gc.ca on CTSN).

CHAPTER 8

INFORMATION SECURITY FOR SIGINT SYSTEMS

Chapter 8: Information Security for SIGINT Systems

8.1 Introduction

8.1.1 Contents

This chapter contains the following topics:

8.1.2 Authority

Section 3.3 of the *Policy on Government Security* (PGS) states that managing security within government departments requires continuous risk assessment as well as implementation, monitoring and maintenance of internal management controls involving prevention, detection, response and recovery.

Section 3.4 of the PGS addresses government-wide security and requires security threats, risks and incidents to be proactively managed, with support from lead security agencies, to help protect the government's critical assets, information and services, as well as national security. Annex B of the PGS establishes CSEC as the lead and coordinating agency for ensuring the protection of electronic information and information systems of importance to the Government of Canada.

Consequently, the security requirements for the protection of SIGINT within secure IT systems are set by CSEC in accordance with the PGS and the document, *Operational Security Standard: Management of Information Technology Security* (MITS). Every department must have an IT Security Policy based on the PGS, MITS, and other related policies, standards and technical documentation.

8.1.3 Definition of IT Security

The PGS defines IT Security as "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information." MITS expands the definition of IT Security to include "safeguards applied to assets used to gather, process, receive, display, transmit, reconfigure, scan, store or destroy information electronically."

8.1.4 Context

CSEC relies on information and information systems to provide actionable intelligence and conduct cyber defence operations in support of its mission and mandates. CSEC collects, processes, stores and transmits an immense quantity of high-value information in the conduct of its business. As a result, the security of information and information systems is essential. Without the implementation of effective information security controls both by CSEC and by GC client organizations, CSEC's critical information assets are vulnerable to disruption and compromise.

8.1.5 Protection of SIGINT on IT Systems

SIGINT on any IT System must be afforded the same degree of protection as SIGINT assets. See *Chapter 2: Special Intelligence Classification and Markings*, and *Chapter 4: Protection of SIGINT Information*, for instructions on protecting SIGINT.

IT Systems and Networks used for processing, storing, or transmitting SIGINT must equally comply with all personnel and physical security measures required for use, handling, display, transmission, or storage of SIGINT material, in particular, Special Intelligence (SI) material. The variety of applications and technical security mechanisms make it impractical to describe specific and detailed standards for every possible SIGINT IT situation. SIGINT IT Security safeguards must include basic mandatory requirements, and additional safeguards which may be identified as a result of Threat and Risk Assessments (TRA).

8.1.6 Before Accreditation

Before being accredited by CSEC, Authorized Organizations must certify all SIGINT IT Systems, which includes networks, telecommunications and other equipment that is connected or interconnected, and the facilities in which they are housed.

8.1.7 Accreditation of SIGINT Systems

Accreditation of a SIGINT IT System is the formal approval by CSEC to allow the system to operate:

- within a particular security zone;
- with a prescribed set of technical and non-technical security safeguards;
- against a defined threat, in a properly secured area, in a given operational environment;
- under a stated Concept of Operations (CONOP);
- with stated interconnections to other information facilities; and
- with a known and acceptable level of residual risk.

See *Chapter 6: SIGINT Certification and Accreditation* for information on the Certification and Accreditation process.

8.2 Administration and Organization

8.2.1 Life Cycle Management

Given the difficulty of implementing cost-effective IT Security safeguards after a system has been deployed, and because technologies and threats constantly change, departments must address security, and adjust security requirements to meet those changes throughout all stages of the system-development life cycle. SIGINT IT Systems must also be managed throughout their life cycle, from the earliest planning stages through maintenance to disposal, and must ensure the following:

- security must be included in each stage of the development life cycle; and
- system documentation must be developed and maintained, recording important decisions at each stage, and incorporating practices related to the disciplines of project management, risk management, and quality assurance.

Given that systems underlie most programs and services, the system life cycle approach to IT Security also applies to the management of programs and services.

8.2.2 Security Risk Management

Departments must continuously manage the security risks to information and IT assets throughout the life of their programs and services. Security risk management activities include:

- a TRA;
- business impact analyses;
- privacy impact assessments;
- self-assessments;
- monitoring;
- security investigations;
- vulnerability assessments; and
- business continuity planning.

8.2.3 Procedures for Configuration Control

The processes for the configuration control of SIGINT equipment and systems and for the updating of operating procedures must be laid out in an instructional document such as an operating instruction or procedure.

8.2.4 Operations Security

Security procedures and administrative controls supporting the operation of a SIGINT System must be developed and implemented. The correct application of operations security will do the following:

- provide a level of assurance for all users of a system and its applications;
- ensure that available protective mechanisms will be used correctly; and
- ensure that the system will be administered and operated in a secure manner.

8.2.5 SIGINT IT Systems Management

Each separately accredited IT System that handles SIGINT data must be managed by an Information Technology Security Coordinator (ITSC) who, in cooperation with the COMINT Control Officer (COMCO), will ensure that all hardware, software, communications, and operations security procedures are applied in accordance with the requirements established for the protection of SIGINT assets.

The responsibilities of the ITSC are described in more detail in *Chapter 3, Departmental Requests for Access to Special Intelligence* in section 3.2.5.

8.2.6 Maintenance of SIGINT IT Systems

The following points must be adhered to with regard to the maintenance of SIGINT IT Systems:

- all SIGINT IT System hardware and software maintenance must be performed where the equipment is located on site or remotely, as appropriate, or within an accredited secure area;
- departmental IT System maintenance personnel must hold the appropriate security clearance, and must be SIGINT-indoctrinated if SI-processing IT systems are involved; and
- contractor personnel may not carry out maintenance on SIGINT IT Systems without the written approval of CSEC.

In emergency situations, it may be necessary for uncleared personnel to be given access to secure areas to work on IT systems. In such cases, these individuals must be fully escorted and their work must be overseen by the responsible cleared and indoctrinated person.

8.2.7 Vulnerability Management of SIGINT IT Systems

Departments must continuously manage vulnerabilities for their programs, systems, and services. This management includes the discovery of vulnerabilities, estimating the associated risk, and the development, testing and implementation of solutions that reduce the risk to an acceptable level. As part of this discovery, departments must actively review sources of vulnerability information to determine the potential effect on their programs, systems and services.

Reviews of SIGINT IT Systems involve the formal examination or inspection of safeguards to determine compliance with these standards, and to develop recommendations accordingly. Security reviews of SIGINT IT Systems must be performed in consultation with CSEC ([redacted]@cse-cst.gc.ca on CTSN) when significant changes to design, operations, or the environment threaten to alter existing safeguards.

8.3 Technical Security

8.3.1 Network Security and Perimeter Defence

Departments must segregate networks into Security Zones, and implement perimeter defence and network security safeguards. The IT Security Guidelines (ITSG) *Baseline Security Requirements for Network Security Zones in the Government of Canada* (ITSG-22) describes such an implementation. The use of IT Network Security Zones by all departments ensures a consistent, minimum level of protection of data communication networks across the GC.

Departments must strictly control all public zone interfaces, including all external uncontrolled networks such as the Internet, at a defined security perimeter. Departments must use perimeter defence safeguards, e.g. firewalls and routers, to mediate all traffic and to protect secure servers.

8.3.2 Network Security Zones

There are seven defined Network Security Zones:

- Public Zone;
- Public Access Zone;
- Operations Zone;
- Restricted Zone;
- Highly Restricted Zone;
- Restricted Extranet Zone; and
- Special Access Zone.

The zones are defined to minimize network complexity, to ensure effective and efficient delivery of network services, to promote interoperability and to provide a consistent level of security for services provided within and across zones. Zone boundaries are well-defined and respect assigned accountabilities for network security.

(see *Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)* for more detailed information)

8.3.3 Objective for Network Security Zones

The objective of the Network Security Zones is to develop a consistent, GC-wide, network security environment that:

- establishes baseline requirements while providing departments with flexibility to meet their specific security obligations;
- promotes interoperability and network interconnectivity; and
- provides a consistent level of security for platforms and applications within a given zone.

8.3.4 Transmission Security (TRANSEC)

SIGINT, like other sensitive information, must be protected when transmitted electronically.

Transmission security (TRANSEC) is the component of Communications Security (COMSEC) that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

8.3.5 Procedures for TRANSEC

Procedures for TRANSEC must be developed and implemented, and should cover:

- maintenance of an inventory and configuration chart of communications hardware devices;
- authorization, documentation, and control of change to the communications hardware;
- network operations including maintenance, monitoring and management activities; and
- identification of problem resolution and testing approaches.

8.3.6 Cryptographic Security

Cryptographic Security includes the provision of means to encrypt the information communicated over IT Systems and telecommunications links, as well as the enforcement of sound and practicable cryptographic operating procedures.

Telecommunications and other electronic communications used to transmit SIGINT data must be protected with CSEC-approved or CSEC-endorsed encryption methods only. All cryptographic equipment, keying material, and algorithms must be installed, operated, maintained and protected in accordance with instructions issued by CSEC.

All cryptographic keying material and key-generation systems used for SIGINT systems must be produced and/or provided by CSEC.

8.3.7 Emanations Security (EMSEC)

Emanations Security (EMSEC) comprises measures taken to protect transmissions from interception, direction finding and electronic analysis.

Most electronic equipment radiates electromagnetic signals that, if intercepted, can compromise sensitive information. Two fundamental approaches to mitigating this risk are source suppression and containment of the information-bearing signals. Together, these safeguards are referred to as TEMPEST.
All IT systems accredited to carry SIGINT must have protective measures that will prevent the unauthorized interception and possible exploitation of compromising emanations. For example, the proper use of the following are measures employed to suppress or contain electromagnetic emanations:

- installation criteria;
- consideration of the environment; and
- zone control.

A TRA and a facility evaluation must be conducted to determine appropriate safeguards, in particular whether TEMPEST-compliant equipment is warranted. At posts abroad, departments should apply TEMPEST protection to all classified information when justified by a TRA.

8.3.8 Tele-communications Cabling

Departments must protect their telecommunications cabling from tampering and damage by authorizing, controlling and monitoring access to telecommunications wiring, spaces and pathways in a manner appropriate to the sensitivity level of the information being transmitted. Departments must ensure additional protection for the transmission of classified or SI information as identified by the results of an appropriate risk assessment. Where physical security safeguards are impractical, departments should use encryption or other methods approved by CSEC.

8.3.9 Inter-connections

Interconnections involving a SIGINT System must be approved by CSEC. Proposals to connect SIGINT Systems to other systems must satisfy the following conditions:

- all concerned parties must agree to the interconnection;
- all concerned systems must be certified and accredited by CSEC before interconnection can occur; and
- the terms, conditions and security requirements must be documented in a memorandum of understanding.

The intent is to ensure that safeguards are developed for the proposed networked SIGINT Systems and their interconnecting communications systems.

8.3.10 Software Integrity and Security Configurations

Establishing safeguards to prevent and detect damage to the integrity of the software can help to avoid many potential security incidents. Departments must:

- configure their operating systems and application software in accordance with security best practices, and should include access controls and administrator privileges;
- implement safeguards to "harden" software that is exposed to the Internet, or servers supporting sensitive applications;
- remove or disable unnecessary services and applications; and
- prohibit the use of unauthorized software.

For more information on software hardening and configuration best practices, consult CSEC ([redacted]@cse-cst.gc.ca on CTSN).

CHAPTER 9

PHYSICAL SECURITY

Chapter 9: Physical Security

9.1 Introduction

9.1.1 Contents This chapter contains the following topics:

Topic
9.1 Introduction
9.2 SIGINT Secure Areas

9.1.2 Introduction Physical security is the use of physical safeguards to prevent or delay unauthorized access to assets, to detect attempted and actual unauthorized access, and to activate appropriate responses. The Treasury Board's *Operational Standard for Physical Security* describes the physical security requirements to counter threats to Government of Canada (GC) employees, assets and service delivery. The physical security requirements for the protection of SIGINT are established by CSEC per the PGS, and their application is determined by CSEC on the basis of a Threat Risk Analysis (TRA), which takes into account the unique requirements of each Authorized Organization.

9.2 SIGINT Secure Areas (SSA)

9.2.1 General All Special Intelligence (SI) material must be processed and stored within a "High Security Zone". This zone, or "SIGINT Secure Area" (SSA), can be an entire building, a single room, a mobile platform such as an aircraft or ship, or it can be a temporary facility. The SIGINT Secure Area itself should be protected by progressively restrictive security zones.

Depending on the current construction and the results of the TRA, there could be a requirement to modify or upgrade facilities.

9.2.2 SSA Building Specifications

Buildings vary widely in design and construction. The degree of physical security necessary for a given site depends on the nature of the location itself, as well as the broader environment. Construction and storage requirements for SSAs located in multi-tenant buildings are generally more stringent than those that apply to single-purpose buildings occupied by a sole organization, and where additional, robust security safeguards are in place.

Appropriate physical security safeguards required for each proposed SSA, whether new or in existing accommodation, permanent or temporary, will be identified by CSEC in cooperation with each Authorized Organization on the basis of a TRA, specific requirements, and standards. All such security measures will comply with relevant codes and regulations, such as labour, fire, building and electrical regulations. SSAs must be accredited by CSEC prior to the client processing or storing SIGINT. The Physical Security Accreditation process is designed to take such varying factors into consideration in evaluating a given location.

Specifications for SSA construction are maintained by CSEC's Physical Security section and can be requested from Director SIGINT Requirements (ssmo-dl@cse-cst.gc.ca on unclassified e-mail or [redacted]@cse-cst.gc.ca on CTSN).

9.2.3 Physical Access

Access to an SSA is based on the "need-to-access" rule, and must be restricted to persons holding a Top Secret security clearance and SIGINT Facility Access or SIGINT Information Access indoctrination.

All other persons requiring access to the area must be escorted, or the room must be occupied by an appropriately indoctrinated staff member while the non-indoctrinated person is present.

Access points must be monitored by a guard service, specifically appointed employees, or an electronic access control system. The choice of access control will depend on the number of personnel having access to the area in conjunction with the findings of the TRA.

9.2.4 Wireless Devices in SSAs

Wireless devices are prohibited in SSAs as the associated risk is unacceptable in the absence of strict security controls. Only by exception and with the explicit approval of CSEC can wireless devices be approved for use in SSAs. There is a high level of risk associated with the introduction of such devices into an area accredited for SI, and a significant cost associated with risk mitigation. For some devices the risk can be mitigated by implementing various security measures such as locking down configurations and applications. However, this can impact the usability of the device. Departments who believe they have a strong business requirement for using wireless devices in an SSA must make a formal request to CSEC's Director SIGINT Requirements. The request must outline the following:

- business reason for using a wireless device in the SSA
- full name and position of the wireless device user(s)
- type of wireless device being considered
- duration of requirement
- location of the SSA

CSEC will consider requests on a case-by-case basis and will work with the requesting department to establish program requirements and mitigation measures that would allow for the use of specific wireless devices in SSAs.

DEFINITIONS

Definitions

Introduction

This chapter provides an alphabetical list of definitions of terms used throughout the CSSS.

A

Acceptable Level of Risk

This refers to a judicious and carefully considered assessment by the accrediting authority that the value of a facility, including information technology systems or networks, unambiguously outweighs the likelihood of potential damage to Canadian security interests in the event that information is compromised, damaged, or destroyed.

Accreditation

Accreditation, or SIGINT accreditation, is the CSEC validation of the SIGINT certification which is completed by the requesting Authorized Organization. SIGINT accreditation signifies that a GC Authorized Organization SIGINT Secure Area (SSA), including concomitant telecommunications and Information Technology (IT) systems, is ready to receive and safeguard SIGINT information.

Action-on

Action-on is any action, or decision to act, taken on the basis of SI information, which might jeopardize the COMINT source. Action-on usually involves a sanitization.

Authority to Operate

Authority to Operate is the official approval by CSEC to allow a project/program, facility and/or system to operate using a particular set of safeguards within an acceptable level of residual risk. (See *Chapter 6: SIGINT Certification and Accreditation.*)

Authorization to Receive Special Intelligence

Authorization to receive SI refers to the fact that an Authorized Organization may retain and/or process SI. The level of retention and/or processing is usually defined by its SIGINT accreditation status.

Authorization to Receive ELINT	Authorization to receive ELINT refers to the fact that an Authorized Organization may retain and/or process ELINT. The level of retention and/or processing is usually defined by its accreditation status.
Authorized Organization	An Authorized Organization is a GC department or agency which has been certified and accredited by CSEC to retain and/or process SI. Authorized organizations in the GC use information derived from SIGINT reports for strategic warning, policy formulation, decision-making, and/or day-to-day assessment of foreign capabilities and intentions. **Note:** Normally, Authorized Organizations are GC departments and agencies, including overseas missions and military commands, but they can also include private contractors of such organizations.

B

Breach of Security	A breach of security occurs when sensitive information or assets have been compromised. A compromise of SIGINT occurs when SIGINT has become, or could reasonably be suspected to have become, accessible to an unauthorized person.

C

Certificate of Destruction	A Certificate of Destruction is a signed document identifying and confirming the permanent destruction of computer files and/or media.
Certification	Certification, or SIGINT certification, is the comprehensive evaluation of the technical and non-technical security features of a SIGINT facility and IT system or network that establishes the extent to which a particular design and implementation meets a specified set of security requirements, made in support of the accreditation process.
CFIOG	CFIOG is the Canadian Forces Information Operations Group.

Client Organization	A Client Organization receives SI read-only service from CSEC Client Relations Officers (CROs) because it has not been certified or accredited by CSEC, and therefore, may not retain and/or process any SI.
Client Relations Officer (CRO)	A CRO is a CSEC employee who provides a tailored, personalized SIGINT service to GC Client Organizations and to select senior managers of Authorized Organizations. Client relations staff includes CROs responsible for providing SIGINT information to Client Organizations, and members of CFIOG teams supporting DND and CF clients.
COMINT	Communications Intelligence (COMINT) is technical information and/or intelligence derived from the exploitation of communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those systems or networks by other than the intended recipients or data owners.
COMINT Control Officer (COMCO)	This is the person designated to receive SI material on behalf of an Authorized Organization. The COMCO is also responsible for SIGINT security on a day-to-day basis.
COMINT Control System	A now-obsolete control system and marking used to protect COMINT information; SI (Special Intelligence) has replaced COMINT as the control system and marking for protecting COMINT information.
Communications Security (COMSEC)	Communications Security (COMSEC) refers to the measures or instructions needed to protect the security of information being transmitted over communication links (telephone lines, radio waves, fibre optic lines, microwaves, or other communication technologies), or to guard against the detection and interception of electromagnetic emissions from information technology and telecommunications equipment. COMSEC is also concerned with the authentication of transmitted information. COMSEC is a component of Information Technology (IT) Security.
Compromise	Compromise is the unauthorized disclosure, destruction, removal, modification, interruption, or use of information and assets.

Control Authority	The Control Authority is the executive-level staff (normally at the Director level) responsible for the program(s) or operation(s) covered by the ECI codeword. The Control Authority provides management oversight of the particular ECI program, and is accountable for the ECI protected information.
Covername	A covername is a single name authorized by the CCSEC to designate SIGINT-related projects, equipments and operations.
CSEC	Communications Security Establishment Canada. The Canadian national SIGINT authority.
CSSS	The Canadian SIGINT Security Standards.
CTSN	The Canadian Top Secret Network is a classified network that provides web and e-mail services and replaces MANDRAKE I and II.

D

Declassification	Declassification is the authorized change in the status of information from classified information to unclassified information. (See CSSS-106, *End-Product Sanitization/Action-On Procedures, Annex 1* for more information concerning the operational use of declassification.)
De-Indoctrination	De-indoctrination is the act of "signing off" indoctrinated persons who no longer require access to SIGINT, specifically SI and its sub-control systems (e.g. GAMMA, ECI Codeword).
Departmental Security Officer (DSO)	The Departmental Security Officer (DSO) is an individual within a GC organization who has sufficient security experience, and is strategically placed to provide department-wide strategic security advice and guidance to senior management.
Destruction	In records management, this is the most common form of disposition action. It involves shredding, pulping, burning, recycling or otherwise making unavailable the record in its original form.

Disposition	Disposition refers to the process which enables GC institutions to dispose of records which no longer have operational value, either by permitting their destruction (at the discretion of institutions), by requiring their transfer to the Library and Archives Canada, or by agreeing to their alienation from the control of the GC.
Dissemination Control Markings	Dissemination control markings are used to limit the distribution of SI to specific individuals, groups, or nationalities. A dissemination control marking can take any form provided it is understood by the reader. Examples of dissemination control markings include, but are not limited to: • RESTRICTED • Canadian Eyes Only (CEO) • Release (REL) to … (where CAN is always placed first, then the names of the other countries in alphabetical order, separated by commas); and • ORCON Dissemination control markings may be used with any classification level, including UNCLASSIFIED.
Downgrading	The lowering of the classification level of information, e.g. TOP SECRET//SI to SECRET.
DSD	Defence Signals Directorate. The Australian Government SIGINT organization.

E

ECI	Exceptionally Controlled Information (ECI) is a sub-control system of the SI control system that provides additional protection for very sensitive SIGINT operations. The operations' sensitivity can relate to: • [redacted] • [redacted] • [redacted] • [redacted] • [redacted]

ELINT	Electronic Intelligence (ELINT) is technical information and/or intelligence derived from the collection, processing, and analysis of electromagnetic non-communication emissions.
Emanations Security (EMSEC)	EMSEC comprises measures taken to protect transmissions from interception, direction finding and electronic analysis.

F

FISINT	Foreign Instrumentation Signals Intelligence (FISINT) is technical information and/or intelligence derived from the collection, processing and analysis of foreign instrumentation signals by other than the intended recipients.
Five-Eyes (5-Eyes)	Five-Eyes refers to Canada, Australia, New Zealand, the US and the UK (it is sometimes abbreviated in the US as "FVEY").
Foreign Intelligence (FI)	Foreign intelligence is 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*, section 273.61).

G

GAMMA	GAMMA is a sub-control system of the SI control system that provides additional protection for very sensitive SI reports and related material. A report's sensitivity can relate to the topic, target, collection method or technique used to analyze or process the intercept upon which the report is based, or any combination thereof.
GAMMA Control Officer (GCO)	The GCO is the person designated to receive, disseminate and account for the distribution of GAMMA material on behalf of an Authorized Organization.

GCHQ	Government Communications Headquarters. The UK Government SIGINT organization.
GCSB	Government Communications Security Bureau. The New Zealand Government SIGINT organization.
Global Information Infrastructure (GII)	The 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).
I	
Indoctrinating Officer	An indoctrinating officer is the person authorized to give an indoctrination briefing. This person is normally: • a CSEC representative; • the COMCO or D/COMCO; or • the GAMMA Control Officer or designate (for GAMMA).
Indoctrination	Indoctrination is the process by which an individual is given access to a control system (e.g. SI or TK) and/or a sub-control system (e.g. GAMMA). It includes a thorough briefing on a given program which provides an individual (the "indoctrinee") with an awareness of the security requirements and responsibilities associated with that program. To be eligible, an individual must hold the appropriate level of security clearance and have a legitimate need-to-know prior to being indoctrinated.
Information Technology	The scientific, technological and engineering disciplines and the management practices used in electronic information handling, communication and processing; the fields of electronic data processing, telecommunications, electronic networks, and their convergence in systems; applications and associated software and equipment together with their interaction with humans and machines.

Information Technology Security (IT Security)	IT Security refers to the safeguards employed to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.
Information System Security Officer (ISSO)	An individual within an Authorized Organization responsible for ensuring that IT systems and networks comply with SIGINT standards for IT security. An Authorized Organization must appoint an ISSO for each separately accredited IT system and network containing SIGINT.
Information Technology (IT) System	An IT system is an assembly of hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.
IT Network Security Zones	IT Network Security Zones make up a networking environment with a well-defined boundary, a security authority and a standard level of susceptibility to network threats.

K

Keying Material	Keying material is cryptographic material specifying cryptographic equipment arrangements and settings or used directly in encryption and decryption. It also includes cryptomaterial that specifies sequences or messages used for command, control or authentication of a command, or which can be used directly in their transmission. Keying material can be supplied in many forms, such as key lists, key cards and key tapes.

M

MANDRAKE	MANDRAKE was the GC Security & Intelligence community TS//SI level network and has now been replaced by the Canadian Top Secret Network. MANDRAKE incorporated two systems: • MANDRAKE I, which provides e-mail connectivity; and • MANDRAKE II, which provides an electronic intelligence-dissemination network using web technology.

Mode of Operation	This refers to the set of security-related elements and conditions which are integral to a computer system and its supporting environment. There are four modes of operation authorized for processing SIGINT: dedicated, system high, compartmented, and multi-level.

N

National Interest	The National Interest concerns the defence and maintenance of the social, political and economic stability of Canada.
Need-to-Know	Need-to-know is a determination made by an authorized holder of information to assess whether a possible recipient requires access to that information in order to perform an authorized GC function. Need-to-know is a fundamental aspect of CSEC's information handling system, and is a way of further restricting access to classified and protected information. It reflects the principle that not everyone who is cleared to see certain information necessarily needs to see all of it.
Network	Comprises communications media and all components attached thereto involved in the transfer of information among a collection of information systems or workstations. Network components include packet switches, front-end computers, network controllers, and technical control devices. In the context of these standards, such networks are (a) under the operational control of a CSEC official, (b) used primarily for the transmission of intelligence, and (c) may provide connectivity among IT systems operated by various intelligence components.
Network Security Devices	Network security devices are any hardware, firmware or software used within a network to protect against unauthorized access to the network; unauthorized access to information and unauthorized modification of information whether in storage, processing or in transit on the network.
Non-Communication Transmission	Non-communication transmissions perform functions other than conveying messages, e.g. radar, navigational aids, jamming transmissions, remote control systems.

NSA	National Security Agency. The US Government SIGINT organization.

O

Originator Controlled (ORCON)	ORCON is a US dissemination control marking added to SIGINT reporting to indicate that dissemination beyond listed addressees is subject to approval by the originator of the report. CSEC Operational Policy ([redacted]@cse-cst.gc.ca on CTSN) must be contacted and asked to obtain approval for SIGINT reports issued by Second-Party agencies (i.e. DSD, GCHQ, GCSB and NSA) that are marked ORCON and that will be disseminated outside Canada to organizations in countries that are not on the original dissemination list.

P

Permission to Quote	Permission to quote refers to wording that is taken directly from a SI report to be used in a second document that is: • also marked SI; and • disseminated within or outside Canadian channels.
Person Permanently Bound to Secrecy	A person permanently bound to secrecy is: • a current or former member or employee of a department, division, branch or office of the Public Service of Canada, or any of its parts, set out in the schedule of the *Security of Information Act* (SOIA); or • someone who has been personally served with a notice issued under subsection 10(1) of SOIA in respect of the person or who has been informed, in accordance with regulations made under subsection 11(2) of SOIA, of the issuance of such a notice in respect of the person.

[redacted]	[redacted]
Portion Marking	Portion markings are abbreviated classification markings that are used to classify individual paragraphs or sections of a report. Portion markings are required for reports, especially where all the information (title and all paragraphs) may not be classified at the same level. Portion marking may also indicate national releasability.

R

RESTRICTED	RESTRICTED is a dissemination control marking applied by CSEC to its own product to ensure certain information is only accessible by named individuals, due to the sensitivity of the content or source. RESTRICTED is used only in conjunction with: TOP SECRET//SI//Canadian Eyes Only; or TOP SECRET//SI-GAMMA//Canadian Eyes Only. A RESTRICTED report may be identified by its serial number, e.g. R-[redacted]
Risk Management	Risk management is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk.

S

Sanitization	Sanitization is the process of editing or otherwise disguising SI to protect sensitive sources, methods, techniques or other sensitive characteristics of the data, and providing [redacted] The aim of sanitization is to permit wider dissemination of information outside of SI channels. (See CSEC document OPS-5-9, *End Product Sanitization/Action-on Procedures*.) **Note**: There are two types of sanitization: • sanitization of end-product, e.g. a SIGINT-indoctrinated GC user requests a sanitization (either directly or through a CRO); and • sanitization of traffic ("Write to Release"), where CSEC includes sanitized SECRET paragraphs in end-product.
Second Parties	Second Parties refer to CSEC's SIGINT counterparts and include: the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD), and New Zealand's Government Communications Security Bureau (GCSB).
Sensitive Compartmented Information Facility (SCIF)	SCIF is a US term for a SIGINT Secure Area (SSA).
Security Risk Management	Security risk management is a component of an overall risk management process involving the organization and coordination of activities and processes for controlling security risk.
Senior Indoctrinated Official (SIO)	The Senior Indoctrinated Official in an Authorized Organization has overall responsibility for SIGINT security in that organization.

Sensitive Compartmented Information (SCI)	Sensitive Compartmented Information (SCI) is a US term for classified national intelligence information concerning or derived from intelligence sources, methods or analytical processes which must be handled within formal access control systems. There are three SCI control systems in use by the US: SI, TK, HCS. In the US, compartmented information is stored in a "SCIF" (Sensitive Compartmented Information Facility); whereas in Canada, we use the term "SSA".
SIGINT	Signals Intelligence (SIGINT) is technical information and/or intelligence comprised of (individually or in combination) Communications Intelligence (COMINT), Electronic Information (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT). Each of these components has been defined separately in this chapter.
SIGINT Accreditation	SIGINT accreditation is the CSEC validation of the SIGINT certification which is completed by the requesting client department. SIGINT accreditation signifies that a SIGINT facility, including telecommunications and information technology systems, is ready to operate.
SIGINT Certification	SIGINT certification is the comprehensive evaluation of the technical and non-technical security features and other safeguards of a SIGINT facility and/or IT systems or networks that established the extent to which a particular design and implementation meets a specified set of security requirements. (The security features and safeguards are grouped into eight security disciplines which are described in *Chapter 6: SIGINT Certification and Accreditation.*) **Note**: SIGINT certification is performed by the requesting client department (usually with CSEC guidance).
SIGINT Information Access (SIA)	The SIA indoctrination applies to individuals who will have access to information that either relates to the activities and methods used to acquire, process, analyze, report and disseminate SIGINT, or the results of this process, i.e. SIGINT reports.

SIGINT Reports

A SIGINT report refers to any report that is based on SIGINT. It includes, but is not limited to:

- End-product (a.k.a. SIGINT end-product; end-product reports);
- Analytic exchanges such as e-mails, i2 charts or other graphic representations, and Requests for Information (RFIs);
- Technical SIGINT Reports;
- Advance Reports: informal, partially vetted SIGINT reports containing incompletely analyzed information;
- Gists: reports containing partly assessed transcripts and associated metadata;
- [redacted]
- [redacted]

SIGINT Secure Area (SSA)

An SSA is an area (e.g. a building, a room, a mobile platform), accredited by CSEC to receive, process and store SI and SI-related information. An SSA can be permanent or temporary. The term "SIGINT facility" is a generic term also used to describe a SIGINT Secure Area.

A SIGINT Secure Area is known in the US as a SCIF (see Sensitive Compartmented Information Facility). For all Canadian procedures, use SSA vice SCIF.

SIGINT Facility Access (SFA)

Formerly known as SIGINT site access, the SFA indoctrination applies to individuals, such as maintenance personnel, who will not have direct access to SI but who, through their day-to-day duties, may be exposed to SI.

[redacted]

[redacted] is CSEC's web-based tool for the dissemination of multimedia and multilingual SIGINT information to client desktops. Analysts use [redacted] to capture their end-product reports. [redacted] is also used to manage SIGINT client information, SIGINT requirements and client feedback.

Special Intelligence Read-Only Service	SI read-only service refers to the fact that individuals at a Client Organization with a SIGINT Information Access indoctrination may only read SI reports that are shown to them by a CSEC CRO, but may not retain any of the SI material. A Client Organization that receives read-only service does not have a SI Registry, and does not have access to IT systems used to access SI reports.
Special Intelligence (SI)	Refers to information derived from COMINT. The 'SI' abbreviation for Special Intelligence is a control system marking used to indicate material or information subject to the handling controls prescribed by the Special Intelligence control system.
Special Intelligence Control System	A control system that protects intelligence derived from COMINT by prescribing standards for access, marking, handling and control of COMINT information.
Special Intelligence Sub-Control Systems	SI derived from or referring to especially sensitive sources and methods may be further compartmentalized and disseminated to a limited number of recipients on a strict need-to-know basis. SI sub-control system markings include GAMMA and ECI, both of which may **only** be classified in the national interest at the TOP SECRET level, e.g. ECI can never be classified only SECRET.
Special Operational Information (SOI)	Special Operational Information (SOI) means information that the GC is taking measures to safeguard which reveals, or from which may be inferred: • the identity of a person, agency, group, body or entity that is or is intended to be, has been approached to be, or has offered or agreed to be, a confidential source of information, intelligence or assistance to the GC; • the nature or content of plans of the GC for military operations in respect of a potential, imminent or present armed conflict; • the means that the GC used, uses or intends to use, or is capable of using, to covertly collect or obtain, or to decipher, assess, analyse, process, handle, report, communicate or otherwise deal with information or intelligence, including any vulnerabilities or limitations of those means;

Continued on next page

Special Operational Information (continued)	• the identity of any person who is, has been or is intended to be covertly engaged in an information- or intelligence-collection activity or program of the GC that is covert in nature; • whether a place, person, agency, group, body or entity was, is or is intended to be the object of a covert investigation, or a covert collection of information or intelligence, by the GC; • the means that the GC used, uses or intends to use, or is capable of using, to protect or exploit any information or intelligence referred to in any of sub-paragraphs a. to e., including, but not limited to, encryption and cryptographic systems, and any vulnerabilities or limitations of those means; or information or intelligence similar in nature to information or intelligence referred to in any of sub-paragraphs above that is in relation to, or received from, a foreign entity or terrorist group.
Sub-control System	A sub-control system is a means by which especially sensitive SI and SI-related information is segregated from regular SI. GAMMA and ECI are examples of SI sub-control systems. Information in control and sub-control systems is also sometimes called "compartmented information."
System	A system is a set of elements including personnel, physical, environmental, safeguards, technology, and other factors that are combined to fulfill a specified purpose or mission.

T

TALENT KEYHOLE (TK)	TALENT KEYHOLE (TK) is a control system for information related to, or derived from, satellite reconnaissance systems and products.

Threat Assessment	A threat assessment is concerned with defining what requires protection, analyzing and assessing threats, analyzing and assessing risks, and making recommendations for the management of those risks.
Traffic	Traffic is defined as content or payload of a communication [redacted] plus the associated metadata acquired from the Global Information Infrastructure (GII).
Transmission Security (TRANSEC)	TRANSEC is the component of Communications Security (COMSEC) that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

U

Untoward Contact	Untoward contact is defined as any contact in which illegal or unauthorized access is sought to sensitive information. It can also be interpreted as any concern arising when an individual believes they are or have been the target of an attempted exploitation to obtain sensitive material or assets. This includes any unauthorized contact with non-allied foreign diplomats/military/consular officials.

V

Violation	In the context of SIGINT security, a violation is considered to have occurred when there has been a failure to observe a SIGINT security regulation. (See also "Breach of Security".)
Vulnerability	A vulnerability is an inadequacy related to security that could permit a threat to cause injury.
Vulnerability Assessment	A vulnerability assessment is a determination of the existence of system vulnerabilities.

W

Write-to-Release	Write-to-release (WTR) is an initiative under which SI reports are issued at the lowest classification possible. WTR involves sanitizing, usually to the SECRET level, all key information that can be released outside SI channels. The result of this process is an intelligence report which contains SI and non-SI paragraphs.

REFERENCES

References

Introduction

IRRELEVANT

Legislation

GC Publications

CSEC Policy Instruments

Other Documentation

CSSS-100 Promulgation

Reviewed and Recommended for Approval

I have reviewed and hereby recommend CSSS-100, *Canadian SIGINT Security Standards* for approval.

James Abbott
Director General SIGINT Programs

29 August 2011
Date

Approved

I hereby approve CSSS-100, *Canadian SIGINT Security Standards*. This policy instrument is effective immediately.

Shelly Bruce
Deputy Chief SIGINT

2 Sept 2011
Date

Promulgation des NCSS-100

Examen et recommandation en vue de l'approbation

J'ai examiné les *Normes canadiennes sur la sécurité du SIGINT (NCSS-100)* et je recommande leur approbation.

James Abbott
Directeur général, Programmes SIGINT

29 August 2011
Date

Approbation

Par la présente, j'approuve les *Normes canadiennes sur la sécurité du SIGINT (NCSS-100)*. Cet instrument de politique entre en vigueur immédiatement.

Shelly Bruce
Chef adjointe, SIGINT

2 Sept 2011
Date