DEFINITIONS

A

"Acceptable Level of Risk"

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.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Accreditation"

The official approval by CSE to allow a SIGINT facility, including telecommunications and information technology systems to operate using a particular set of safeguards at an acceptable level of risk.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Action-on"

Any action taken

Source: OPS-5-9 - Procedure - October 25, 2001
OPS-5-9, Procedure, 10 May 2002

"Action-on"

Action-on is defined as any action taken

Source: OPS-1-1 6 December 2002, Procedures for

"Action-on"

Action-on is any action, or decision to act, taken (

Source: OPS 5-3, Procedures, Revised October 18, 2002

"Action on "

Any action, or decision to act, taken

Source: Canadian SIGINT Security Standards, 1 March 1995

"Assurance"

The degree of confidence that a product correctly implements the security policy.

s.15(1)
s.16(2)(c)

Source: Canadian SIGINT Security Standards, 1 March 1995

"Australian citizens and organizations"

Australians are defined as Australian citizens or organizations.
An *Australian citizen* is a person holding or entitled to hold an Australian passport, residing anywhere. This does not include permanent residents.
An *Australian organization* is a body which is wholly or majority owned or controlled by Australians, regardless of location or place of registration.

Source: Procedures Summary (April 28, 1999)

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)

"Authorization"

An authorization is provided in writing by the Minister of National Defence to CSE to permit CSE to intercept a private communication in relation to an activity or class of activities specified in the authorization pursuant to s.273.65(1) of the NDA for the sole purpose of obtaining foreign intelligence or pursuant to s. 273.65(3) for the sole purpose of protecting the computer systems or networks of the Government of Canada.

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

"Authorized Organization"

A Canadian organization approved by the Chief of CSE to receive and retain SIGINT, specifically COMINT. Authorized organizations are normally federal-level government departments or agencies, including overseas missions and military commands, but can also include private contractors of such organizations.

Source: CSSD-2101, June 6, 1995

"Authorized Organization"

A Canadian organization approved by the CCSE to receive and retain SIGINT, but specifically COMINT; normally federal-level government departments or agencies, including overseas missions and military commands, but can also include private contractors of such organizations.

Source: Canadian SIGINT Security Standards, 1 March 1995

s.15(1)
s.16(2)(c)

"Authorized Organizations"

Canadian organizations approved by the Chief, CSE, to receive and retain SIGINT, specifically COMINT and COMINT-related information.

Source: CSSD 2121 - 30 April 1999 - The ECI System

"Authorized Purposes"

RIPA, ISA and HRA allow GCHQ to use its intelligence powers for the following purposes only:

- National security
- Safeguarding the economic well-being of the UK, or
- In support of the prevention or detection of serious crime.

RIPA - The *Regulation of Investigatory Powers Act* came into effect on 2 October 2000. It replaces the *Interception of Communications Act 1985* (IOCA) and forms the legal basis for GCHQ=s interception operations.

HRA - The UK Human Rights Act 1998 came into force on 2 October 2000. It incorporates the European Convention on Human Rights into UK law.This legislation, among other things, requires GCHQ to be in a position to answer complaints, from any person in the world, about alleged interception from UK sites.

ISA - The Intelligence Services Act, 1994, applies to all operations under the control of the Director GCHQ.

Source: OPS-2-1, Procedures for sites, 28 June 2001, Revised January 2002

"Authorized Target"

Authorized targets are approved foreign countries, organizations and persons listed in the

Source: OPS-3-3, Procedures, Revised 20 June 2002

B

"Breach of Security"

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

Source: Canadian SIGINT Security Standards, 1 March 1995

s.15(1)
s.16(2)(c)

C

"Canadian"
means

a) a Canadian citizen or a permanent resident, within the meaning of subsection 2(1) of the *Immigration Act*; or

b) a corporation incorporated under an Act of Parliament or of the legislature of a province.

Source: *National Defence Act*, Part V.1, Section 273.61
OPS-1-6 Procedures for , 25 June 2002

Above Def. Plus For the purposes of this procedure, 'Canadian organizations' are also accorded the same protection as Canadian citizens and corporations.

Source: OPS-1-1 6 December 2002, Procedures for

"Canadian"

'Canadian' refers to a Canadian person or Canadian corporation (*National Defence Act*, section 273.61)

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

"Canadian"

Canadian' refers to:

- a Canadian citizen
- a permanent resident within the meaning of the *Immigration Act*, or
- a corporation incorporated by or under an Act of Parliament or of the legislature of a province.

Source: OPS-3-3 Procedures, Revised 20 June 2002

"Canadian (n.)"

According to section 273.61 of the *National Defence Act*, the noun "Canadian" refers to a Canadian person or a Canadian corporation. It is CSE policy to extend this meaning to refer to

a Canadian organization as well (see definitions below).

Source: Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002

"Canadian communication"

A Canadian communication is:

- a private communication (as defined below) originating or terminating anywhere in Canada; or
- a communication originated by or destined to a Canadian person, corporation or organization, located anywhere in the world.

Source: Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002

"Canadian Corporation"

A *Canadian corporation* is a business, company, firm, financial institution or other commercial enterprise that is incorporated in Canada.
Subsidiaries of Canadian companies incorporated in a foreign country are not considered Canadian companies.

Source: Procedures Summary (April 28, 1999)
OPS-5-13, Procedures for
12 December 2002

"Canadian corporation"

A Canadian corporation is a business, company, firm, financial institution or other enterprise that is incorporated in Canada under an Act of Parliament or of the legislature of a province.

Source: Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002
Safeguarding the Privacy of Canadians Annual Report for the period January – December 2001, April 2002

"Canadian Corporation"

A Canadian corporation is a business, company, firm, financial institution or other commercial enterprise that is incorporated in Canada.
An entity that is incorporated in another country is not Canadian even if it is a subsidiary of a Canadian corporation.

Source:

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)

Procedures - (Formerly Chapter 3 of the CSE SIGINT Reporting Procedures)

"Canadian corporation"

A business, company, firm, financial institution or other commercial enterprise that is incorporated in Canada either under federal or provincial legislation, including any subsidiary of a Canadian corporation which is itself incorporated in Canada.

Source: Directive, DGP/D-2102, March 27, 1998, (Directive supersedes and amalgamates DGP/D-2101,] Policy of 9 October 1990, and DGP/D-2102, Policy of 1 March 1991)

"Canadian corporation"

A Canadian corporation is a corporation that is incorporated under an Act of Parliament or of the legislature of a province.

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

"Canadian identity"

A Canadian identity refers to the identification of a Canadian entity

In cases where the identified entity is suspected to be Canadian, it is treated as a Canadian identity.

Source: Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002

"Canadian information"

Canadian information refers to:

- information about Canadians (see below), or
- a Canadian communication (see above) or signals-related information thereof.

Source: Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2001, April 2002

s.15(1)

Source: OPS-1-4 October 25, 2001

"Canadian Organization"

A *Canadian organization* is:

- an unincorporated association, such as a political party, a religious group or unincorporated business headquartered in Canada.

A Canadian-flagged (registered), non-governmental aircraft or vessel is treated in the same manner as a Canadian organization.

Source: Procedures Summary (April 28, 1999)

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)
Procedures - (Formerly Chapter 3 of the CSE SIGINT Reporting Procedures)
Directive, DGP/D-2102, March 27, 1998, (Directive supersedes and amalgamates DGP/D-2101, of 9 October 1990, and DGP/D-2102, Policy of 1 March 1991)
OPS-5-13, Procedures for
12 December 2002
Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002

"Canadian Person"

A *Canadian person* is:

- a citizen of Canada
- a permanent resident of Canada

within the meaning of the *Immigration Act*.

Source: Procedures Summary (April 28, 1999)

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)
Procedures - (Formerly Chapter 3 of the CSE SIGINT Reporting Procedures)
OPS-5-13, Procedures for
12 December 2002

"Canadian person"

A Canadian person is:

- a citizen of Canada, or
- a permanent resident of Canada within the meaning of subsection 2(1) of the *Immigration Act*.

Source: Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002

"Canadian person"

A Canadian person is:

- a citizen of Canada, or
- a permanent resident of Canada within the meaning of subsection 2(1) of the *Immigration Act*.

This means a person who:
(a) has been granted landing,
(b) has not become a Canadian citizen, and
(c) has not ceased to be a permanent resident pursuant to section 24 or 25.1.

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

"Canadian Solicitor"

'Canadian solicitor' refers to a person authorized to practice as an advocate or notary in Quebec or as a barrister or solicitor in any territory or other province of Canada, and any person employed in a solicitor's office.

Source: OPS-3-3, Procedures, Revised 20 June 2002

"Canadian Solicitor-client telecommunication"

'Canadian solicitor-client telecommunication' refers to any telecommunication of a confidential character between a client and a solicitor directly related to the seeking, formulating or giving of legal advice or legal assistance.

Source: OPS-3-3, Procedures, Revised 20 June 2002

"Canadian vessel"

is one registered as sailing under the Canadian flag, regardless of ownership.

Source: Directive, DGP/D-2102, March 27, 1998, (Directive supersedes and amalgamates DGP/D-2101, Policy of 9 October 1990, and DGP/D-2102, Policy of 1 March 1991)

s.15(1)

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

Source: OPS-5-13, Procedures for
12 December 2002

Source: Canadian SIGINT Security Standards, 1 March 1995

"Category"

See COMINT Category.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Caveat"

See COMINT Caveat.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Certification"

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 establishes the extent to which a particular design and implementation meets a specified set of security requirements. Certification is a mandatory part of the accreditation process.

Source: Canadian SIGINT Security Standards, 1 March 1995

"CFSRS"

Canadian Forces Supplementary Radio System.

Source:Canadian SIGINT Security Standards, 1 March 1995

s.15(1)

Source: OPS-3-1, Procedures for 27 August 2002

"Codeword"

See COMINT CODEWORD.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Codeword Material"

Any material requiring the protection of a COMINT codeword in addition to a security classification.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Collaborating Country"

One whose SIGINT organization collaborates with that of Canada, specifically the USA, UK, Australia and New Zealand.

Source: Canadian SIGINT Security Standards, 1 March 1995

"COMCO"

See COMINT Control Officer.

Source: Canadian SIGINT Security Standards, 1 March 1995

"COMINT"

COMINT is technical information and intelligence information derived from the intercept of

foreign communications

Source: DGP/D-2116 - CSE SIGINT REPORTING PROCEDURES - June 18, 1999
CSSD-2101, June 30, 1999
Canadian SIGINT Security Standards, 1 March 1995

"COMINT Activities"

Activities involved in the production of COMINT,

Source: Canadian SIGINT Security Standards, 1 March 1995

"COMINT Category"

A level or grouping to which COMINT or COMINT-related information is assigned, according to degree of sensitivity and vulnerability to foreign communications security measures. Currently, there are three COMINT categories - Categories III, II and I - and one Sub-Category - Category II(X); Category III is the highest.

Source: Canadian SIGINT Security Standards, 1 March 1995

COMINT Caveat"

A word or phrase applied to COMINT or COMINT-related information to indicate additional handling or dissemination restrictions or procedures,

Source: Canadian SIGINT Security Standards, 1 March 1995

"COMINT Channels"

The means of handling and transmitting COMINT, ensuring only appropriately cleared and indoctrinated persons have access to classified material marked "COMINT".

Source: OPS-5-9 Procedure - October 25, 2001
OPS-5-9, Procedure, 10 May 2002

"COMINT Channels"

The methods and means authorized for handling or transmitting COMINT and COMINT-related information whereby the information is provided exclusively to those persons appropriately cleared and indoctrinated for access to COMINT. A COMINT document is "handled via COMINT channels" when it is transmitted via a COMINT-approved communications circuit or transported by a COMINT-indoctrinated courier to a SIGINT Secure Area/SIGINT Registry within an Authorized Organization, and subsequently disseminated only to appropriately COMINT-indoctrinated readers.

Source: CSSD-2101, June 6, 1995
Canadian SIGINT Security Standards, 1 March 1995

"COMINT Codeword"
A word attached to a security classification

Source: Canadian SIGINT Security Standards, 1 March 1995

"COMINT Control Officer (COMCO)"
The person designated to receive COMINT material on behalf of an Authorized Organization. The COMCO is also responsible for SIGINT security on a day-to-day basis.
Source: Canadian SIGINT Security Standards, 1 March 1995

"COMINT Control System"
See COMINT Channels
Source: Canadian SIGINT Security Standards, 1 March 1995

"COMINT-Related Information"
Information which is not COMINT per se, but is about or related to COMINT.
Source: Canadian SIGINT Security Standards, 1 March 1995

"Communications Electronic Security (COMSEC)"
The measures or instructions needed to protect the security of information being transmitted over communication links
or to guard against the detection and interception

COMSEC is also concerned with the authentication of transmitted information. COMSEC is a component of Information Technology Security (ITS).
Source: Canadian SIGINT Security Standards, 1 March 1995

"Compartmentation"
A means by which especially sensitive COMINT and COMINT-related information is segregated from regular COMINT. The VRK Control System is a compartment system.
Source: Canadian SIGINT Security Standards, 1 March 1995

"Compromise"
The disclosure of classified material, in whole or in part, to unauthorized persons through loss,

s.15(1)
s.16(2)(c)

theft, capture, recovery or salvage, defection of individuals, unauthorized viewing, or any other means.

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: **OPS-1-6 Procedures for** , 25
June 2002

Source: **OPS-1-6 Procedures for** 25
June 2002

"COMSEC"

See Communications Security.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Counter-Measures"

Communications security measures undertaken by a COMINT target to prevent further exploitation of its communications,

Source: Canadian SIGINT Security Standards, 1 March 1995

"Covername"

A single name authorized by the CCSE to designate

Source: Canadian SIGINT Security Standards, 1 March 1995

"Covernames"

"Criminal intelligence (CI)"
information that may be used in the investigation or prosecution of an alleged contravention of any federal or provincial law in Canada.
Source: Procedures, June 30, 1999

"CRO"
Customer Relations Officer.
Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Ops-2-3, Undated)

Source: Ops-2-3, (Undated)

"CSE collection"

Source: **OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002**, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

Source: Ops-2-3, (Undated)

"CSSD"

Canadian SIGINT Security Directive.

Source: Canadian SIGINT Security Standards, 1 March 1995

"CSSS"

Canadian SIGINT Security Standards.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Customer"

refers to a COMINT-indoctrinated Federal Official receiving SIGINT from CSE.

Source: Directive, DGP/D-2102, March 27, 1998, (Directive supersedes and amalgamates DGP/D-210 Policy of 9 October 1990, and DGP/D-2102, Policy of 1 March 1991)

D

"Declassification"

The removal of all classification, making the information "unclassified".

Source: OPS-5-9 - October 25, 2001
OPS-5-9, 10 May 2002

"Declassification"

Removing the classified status of information.

Source: Canadian SIGINT Security Standards, 1 March 1995

"De-indoctrination"

The act of "signing off" indoctrinated persons who no longer require access to SIGINT,

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Ops-2-3, (Undated)

"Downgrading"

The lowering of the classification level of information.

Source: CSSD-2101, June 6, 1995
Canadian SIGINT Security Standards, 1 March 1995

"DSD"

Defence Signals Directorate. The Australian Government SIGINT organization.

Source: Canadian SIGINT Security Standards, 1 March 1995

"DSO"

Departmental Security Officer.

Source: Canadian SIGINT Security Standards, 1 March 1995

E

"ECI"

(The ECI system replaces the Very Restricted Knowledge (VRK) system. This Directive supersedes CSSD-2104 - *The Control of Very Sensitive SIGINT Activities* (30 Nov 93), as well as CSSD-2104, Annex A)

Exceptionally Controlled Information control system for the most sensitive aspects of SIGINT.

ECI Program Manager -CSE person who is accountable for managing an ECI program (referred to as Subject Authority in the VRK system).

ECI Awareness Briefing -an informal briefing normally provided by ECI Program Managers to those who, in order to perform their duties, require some general knowledge, but not the sensitive details, of an ECI program. The briefing should be tailored to the specific staff role (e.g. collection, analysis etc.). No record need be retained of these briefings as they do not constitute an ECI access indoctrination.

Source: CSSD 2121 - 30 April 1999 - The ECI System

"Electronic Intelligence"

ELINT.

Source: Canadian SIGINT Security Standards, 1 March 1995

"ELINT"

Electronic Intelligence. Technical and intelligence information derived from foreign non-communications electromagnetic emissions

Source: Canadian SIGINT Security Standards, 1 March 1995
DGP/D-2116 - CSE SIGINT REPORTING PROCEDURES - June 18, 1999
CSSD-2102, June 6, 1995

"Emission Security"

The measures taken to deny the intercept and analysis of compromising emanations from crypto-equipment, information processing equipment, and telecommunications systems. The term TEMPEST refers to investigations and studies of compromising emanations, but in usage it has become synonymous with emission security.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Encryption"

The transformation of information from a readily interpreted, or "plain-text" form to a specially coded form that hides the content of the information. A special encryption key or password is used as a mathematical key to code and decode (decrypt) the information.

Source: Canadian SIGINT Security Standards, 1 March 1995

See

Source: Canadian SIGINT Security Standards, 1 March 1995

"Entity"

means a person, group, trust, partnership or fund or an unincorporated association or organization and includes a state or a political subdivision or agency of a state.

Source: *National Defence Act*, Part V.1, Section 273.61

OPS-1-6 Procedures for ,25 June 2002

"Entity"

An entity is a person, group, trust, partnership, or fund or an unincorporated association or organization and includes a state or political subdivision or agency of a state (*National Defence Act*, section 273.61).

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002

Source: OPS-1-6 Procedures for (25 June 2002

s.15(1)
s.16(2)(c)

F

"Federal officials and organizations"

include federal Ministers, federal public servants, armed forces personnel, federal departments and agencies, crown corporations, government owned buildings, and vessels or aircraft belonging to the armed forces or other government organizations.

Source: Directive, DGP/D-2102, March 27, 1998, (Directive supersedes and amalgamates DGP/D-2101, Policy of 9 October 1990, and DGP/D-2102, Policy of 1 March 1991)

"FIS"

Foreign Instrumentation Signals. Electromagnetic emissions, associated with the testing

Source: Canadian SIGINT Security Standards, 1 March 1995

"FISINT"

Foreign Instrumentation Signals Intelligence. Technical and intelligence information derived from intercept of foreign instrumentation signals (FIS).

Source: Canadian SIGINT Security Standards, 1 March 1995

"FISINT"

Foreign Instrumentation Signals Intelligence. Technical and intelligence information derived from intercept of foreign instrumentation signals (FIS).

Source: CSSD-2101, June 6, 1995

Source: Ops-2-3, (Undated)

"Foreign"

Other than of Canada, the US, the UK, Australia or New Zealand

Source: Procedures Summary (April 28, 1999)

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)

"Foreign"

In the context of the *National Defence Act* and the *CSIS Act*, 'foreign' refers to non-Canadian.

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

"Foreign communication"

A foreign communication is a communication:

–

outside Canada, or

–

***Note:**

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

"Foreign Communications"

All communications except those of the governments of Canada

Source: Canadian SIGINT Security Standards, 1 March 1995

"Foreign Communications"

are all communications except those of the governments of Canada

Source: Directive, DGP/D-2102, March 27, 1998, (Directive supersedes and amalgamates DGP/D-2101, Policy of 9 October 1990, and DGP/D-2102, Policy of 1 March 1991)

Source: Procedures - (Formerly Chapter 3 of the CSE SIGINT Reporting Procedures)

"Foreign Instrumentation Signals"

See FIS.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Foreign Instrumentation Signals Intelligence"

See FISINT.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Foreign Intelligence"

is information concerning the capabilities, intentions, or activities of a foreign: state, person or organization in relation to Canadian national defence, security, foreign relations, or economic interests.

Source: Directive, DGP/D-2102, March 27, 1998, (Directive supersedes and amalgamates DGP/D-2101, Policy of 9 October 1990,

and DGP/D-2102, 1 Policy of 1 March 1991)

"Foreign intelligence (FI)"

information relating to the capabilities, intentions or activities of a foreign state. person or corporation in relation to the defence of Canada or the conduct of the international affairs of Canada.

Source: - June 30, 1999

Procedures, June 30, 1999

"Foreign Intelligence"

means 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.

Source: *National Defence Act,* Part V.1, Section 273.61

OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

OPS-1-6 Procedures for 25 June 2002

"Foreign Intelligence"

'foreign intelligence' is

defined as:

"in relation to the defence of Canada or the conduct of the international affairs of Canada, information or intelligence relating to the capabilities, intentions or activities of a foreign state, person or corporation."

Source: 1987

OPS-3-3, Procedures, Revised 20 June 2002

G

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: OPS-1-6 Procedures for 25 June 2002

"GCHQ"

Government Communications Headquarters. The United Kingdom Government SIGINT organization.

Source: Canadian SIGINT Security Standards, 1 March 1995

"GCSB"

Government Communications Security Bureau. The New Zealand Government SIGINT organization.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Global Information Infrastructure"

Global information infrastructure 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.

Source: *National Defence Act,* Part V.1, Section 273.61

OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

H

"HANDLE VIA COMINT CHANNELS ONLY"

The caveat applied to material which does not require a COMINT codeword but reveals, or from which can be deduced, some details or aspect of COMINT activities.

Source: Canadian SIGINT Security Standards, 1 March 1995

"HVCCO"

Handle Via COMINT Channels Only.

Source: Canadian SIGINT Security Standards, 1 March 1995

I

Source: OPS-1-4 October 25, 2001

Source: Safeguarding the Privacy of Canadians Annual Report for the period January – December 2001, April 2002

"Indoctrination"

The formal process of briefing an individual about SIGINT, specifically COMINT and COMINT activities, prior to being permitted access to COMINT. There are two level of indoctrination, Category III and Category I.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Information about Canadians"

Information about Canadians is defined as information which allows a unique Canadian entity to be identified.

Source: Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002

"Information about Canadians"

TOP SECRET COMINT
2003-03

Source: Procedures, June 30, 1999

"Information about Canadians"

For the purposes of this document, the phrase, 'information about Canadians'

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

"Information about Canadians"

For the purpose of these procedures, the term 'information about Canadians' refers to:

- any personal information about a Canadian citizen or permanent resident, or
- any information about a Canadian corporation.

Source: OPS-1-6 Procedures for , 25 June 2002

"Information about Canadians"

For the purposes of these procedures, 'information about Canadians' is defined as:

information or intelligence about Canadians, whatever its origin:

Source: 1987

OPS-3-3, Procedures, Revised 20 June 2002

"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.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Information Technology Security"

The protection resulting from an integrated set of safeguards designed to ensure confidentiality of information electronically stored, processed or transmitted; the integrity of the information and related processes; and the availability of systems and services.

Source: Canadian SIGINT Security Standards, 1 March 1995

"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.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Intelligence Information"

Information of potential intelligence value concerning the capabilities, intentions, and activities of any foreign power, organization or associated personnel.

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Canadian SIGINT Security Standards, 1 March 1995

"Intercept"

an interference between the place of origination and the place of destination of the communication (cc / 297)

includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof (cc / 294)

NOTE:

"Intercept"

(verb)

To intercept is the process of acquiring information, from the Global Information Infrastructure (GII).

(noun)

Intercept is any data or technical information carried on, contained in or relating to the GII; sometimes referred to as traffic.

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

"ISSO"

Information Systems Security Officer. The ISSO, in cooperation with the COMCO, ensures that IT systems and networks operate in compliance with SIGINT Standards.

Source: Canadian SIGINT Security Standards, 1 March 1995

J

K

"Keying Material"

Cryptographic material specifying cryptographic equipment arrangements and settings or used directly in encryption and decryption. Also defined as keying material is 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.

Source: Canadian SIGINT Security Standards, 1 March 1995

L

"Level of Assurance"

See Assurance.

Source: Canadian SIGINT Security Standards, 1 March 1995

s.15(1)
s.16(2)(c)

M

Source: Ops-2-3, (Undated)

Source: Canadian SIGINT Security Standards, 1 March 1995

N

"National Interest"

Concerns the defence and maintenance of the social, political and economic stability of Canada.

Source: Canadian SIGINT Security Standards, 1 March 1995

"National Security"

In the context of these procedures, national security is defined as something 'for which the executive government bears the responsibility and alone has access to sources of information that qualify it to judge what the necessary action is". This usually includes counter-terrorism, counter-intelligence, counter-proliferation activities, and activities in support of military forces and defence.

Source: OPS-2-1, Procedures for I
28 June 2001, Revised January 2002

"National Sensitivity"

Special national sensitivity is defined as information that might diminish or negate an advantage that Canada would gain from this information

Source: Procedures, June 30, 1999

s.15(1)
s.16(2)(c)

Source: OPS 5-5, Procedures for I Reporting, August 2001, Revised
23 Jan 2002

"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 CSE official, (b) used primarily for the transmission of intelligence, and (c) may provide connectivity among IT systems operated by various intelligence components.

Source: Canadian SIGINT Security Standards, 1 March 1995

"New Zealand Person or Organization"

"***New Zealand person***" means:

a) a New Zealand citizen (i.e. a person holding or entitled to hold a New Zealand passport, which includes Cook Islanders and Niueans) residing anywhere in the world:

b) a citizen of any other country lawfully residing permanently in N Zealand. include foreign diplomats or consular officials accredited by other governments or by t United Nations to the Government of New Zealand, their foreign staff and dependents.

"***New Zealand Organization***"

means a body which is:

a) wholly or majority owned or controlled by a New Zealand person or persons, or by the Government of New Zealand, regardless of where incorporated or registered; or

b) a company or body that is incorporated in New Zealand; or

c) an unincorporated body of persons of which more than 50% of members are New Zealand persons,

but does not include a body which is an extension of a foreign government (e.g. the Bank of China) or of a foreign economic interest (e.g. Itochu Corp).

Source: Procedures Summary (April 28, 1999)

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)

"Non-Communication Transmissions"

Transmissions which perform functions other than conveying messages,

Source: Canadian SIGINT Security Standards, 1 March 1995

"NSA"

National Security Agency. The United States Government SIGINT organization.

Source: Canadian SIGINT Security Standards, 1 March 1995

s.15(1)
s.16(2)(c)

O

Source: OPS-1-4, October 25, 2001

Safeguarding the Privacy of Canadians Annual Report for the period January – December 2001, April 2002

"ORCON"

Originator Controlled.

Source: Canadian SIGINT Security Standards, 1 March 1995

P

"Person permanently bound to secrecy"

(a) 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; or

(r) a person who has been personally serviced with a notice issued under subsection 10(1) (*Security of Information Act*) in respect of the person or who has been informed, in accordance with regulations made under subsection 11(2), of the issuance of such a notice in respect of the person.

Source: *Security of Information Act*, Section 8

"Personal Information"

Personal Information means information that could be used to identify a person. For a definition of personal information, see section 3 of the *Privacy Act*.

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

OPS-1-6 Procedures for 25 June 2002

"Plain Language"

Unencrypted communications. Also called plain text.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Plain Text"

See PLAIN LANGUAGE.

Source:Canadian SIGINT Security Standards, 1 March 1995

"Platform"

A platform is a satellite or ground station.

Source: OPS-1-6 Procedures for 25 June 2002

i

Source: OPS 5-3, Procedures, Revised October 18, 2002

Source: OPS-5-9 Procedure - October 25, 2001
OPS-5-9, Procedure, 10 May 2002

"Portion Marking"

Portion marking consists of marking the title and paragraphs of reports with an appropriate classification plus, where applicable, foreign release markings. All CSE reports must be portion marked.

Source: OPS 5-3, Procedures, Revised October 18, 2002

"Private Communication"

A private communication is:

'any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it'.

Source: *Criminal Code*, section 183
OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the

Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002

"Private Communication"

has the same meaning as in section 183 of the *Criminal Code*.

"Private communication"

A private communication is a communication that originates or terminates in Canada made under circumstances where there exists a reasonable expectation of privacy.

'Any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it'. (*Criminal Code*, section 183)

Source: OPS-1-6 Procedures for 25 June 2002

Source: Procedures, June 30, 1999

"Proper Authority"

A senior official within an Authorized Organization delegated by CSE to approve requests Proper Authorities are appointed only in exceptional circumstances.

Source: Canadian SIGINT Security Standards, 1 March 1995

Q

R

"Radio Frequency (RF)"

Radio Frequency (RF) is the measured transmitted frequency of an unmodulated continuous waveform or the average center frequency of a symmetrically modulated waveform (also known as carrier frequency, center frequency, and rest frequency).

Source: OPS-1-6 Procedures for (25 June 2002

Source: Canadian SIGINT Security Standards, 1 March 1995

"Risk Assessment"

An evaluation of the chance of vulnerabilities being exploited, based on the effectiveness of existing or proposed security measures.

Source: Canadian SIGINT Security Standards, 1 March 1995

S

Source: OPS-1-6 Procedures for , 25 June 2002

Source: OPS-5-9 - Procedure - October 25, 2001

Source: CSSD-2101, June 6, 1995

s.15(1)

Source: **OPS 5-3,** **Procedures, Revised October 18, 2002**

Source: OPS-5-9, **Procedure, 10 May 2002**

Source:Canadian SIGINT Security Standards, 1 March 1995

"SCI"

See Sensitive Compartment Information.

Source:Canadian SIGINT Security Standards, 1 March 1995

"Second Parties" or "Second Party"

Second Party is the term used to describe the SIGINT organizations of Australia (DSD), New Zealand (GCSB), the UK (GCHQ) and the US (NSA).

Source: Procedures Summary (April 28, 1999)

"Second Parties"

A term used to describe the SIGINT organizations of Australia (DSD), New Zealand (GCSB), the UK (GCHQ), and the USA (NSA). See also Collaborating Countries.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Second Party"

Second Party refers to NSA, GCHQ, DSD and GCSB.

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

OPS-1-1 6 December 2002, Procedures for

"Security intelligence (SI)"

information relating to threats to the security of Canada.

Source: - June 30, 1999

Procedures, June 30, 1999

Source: Procedures, June 30, 1999

TOP SECRET COMINT
2003-03

Source: Procedures Summary (April 28, 1999)

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

Source: OPS-2-1, Procedures for
28 June 2001, Revised January 2002

Source: OPS-1-6 Procedures for 25 June 2002

s.15(1)
s.16(2)(c)

Source: OPS-3-3, Procedures, Revised 20 June 2002

"Senior Indoctrinated Official"

See SIO.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Sensitive Compartmented Information (SCI)"

SCI is a U.S. term which is defined as all information and material that requires special control for restricted handling under compartmented foreign intelligence systems. In the U.S., COMINT is a component of SCI.

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: - June 30, 1999

"Serious Crime"

Serious crime is explicitly defined to mean serious crime anywhere in the world,

Source: OPS-2-1, Procedures for
28 June 2001, Revised January 2002

Source: Canadian SIGINT Security Standards, 1 March 1995

"SIGINT"

Signals Intelligence (SIGINT) involves the intercept and analysis of foreign communications and non-communications signals. The term SIGINT comprises Communications Intelligence (COMINT), Electronic Intelligence (ELINT) and Foreign Instrumentation Signals Intelligence (FISINT).

Source: DGP/D-2116 - CSE SIGINT REPORTING PROCEDURES - June 18, 1999

"SIGINT"

Signals Intelligence. The term given to information gathered about foreign countries by intercepting and studying their radio, wire, radar and other electronic transmissions. SIGINT comprises Communications Intelligence (COMINT), Electronic Intelligence (ELINT) and Foreign Instrumentation Signals Intelligence (FISINT).

Source: CSSD-2101, June 6, 1995

"SIGINT"

Signals Intelligence. The term given to information gathered about foreign countries by intercepting and studying their radio, wire, radar and other electronic transmissions.

Source: Canadian SIGINT Security Standards, 1 March 1995

"SIGINT Community"

The term SIGINT Community refers to the five national SIGINT agencies (CSE, DSD, GCHQ,

GCSB, NSA).

Source: OPS-1-6 Procedures for 25 June 2002

Source: Canadian SIGINT Security Standards, 1 March 1995

"SIGINT Environment"

An approved, secure area where SIGINT, i.e. COMINT and/or ELINT and/or FISINT, is received, stored and worked on. A secure area approved only for the handling and storage of ELINT and/or FISINT classified in the national interest, although considered a SIGINT environment, is not automatically approved for COMINT and must be re-accredited by CSE prior to receiving and processing COMINT (*see* Authorized Organization).

Source: Canadian SIGINT Security Standards, 1 March 1995

"SIGINT Facility"

See SIGINT Secure Area.

Source: Canadian SIGINT Security Standards, 1 March 1995

s.15(1)
s.16(2)(c)

Source: CSSD-2101, June 6, 1995

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Canadian SIGINT Security Standards, 1 March 1995

"SIGINT Secure Area (SSA)"

A "high security zone" as defined in the Canadian SIGINT Security Standards (CSSS), Chapter 5 and associated annexes.

Source: Ops-2-3, (Undated)

"SIGINT Secure Area"

An area, e.g. a building, a room, a mobile platform, accredited by CSE to receive, process and store COMINT and COMINT-related information. A SIGINT Secure Area can be permanent or temporary. The term SIGINT facility is a generic term also used to describe a SIGINT Secure Area.

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

OPS-1-1 6 December 2002, Procedures

OPS-1-6 Procedures for 25 June 2002

"SIO"

The Senior Indoctrinated Official in an Authorized Organization has overall responsibility for SIGINT security.

Source: CSSD-2101, June 6, 1995

Canadian SIGINT Security Standards, 1 March 1995

"Special Material"

An unclassified term denoting COMINT and/or COMINT-related information, which is used on envelopes, wrappers and transmittal slips.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Special Operational Information"

Means information that the Government of Canada is taking measures to safeguard that 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 Government of Canada;
- the nature or content of plans of the Government of Canada for military operations in respect of a potential, imminent or present armed conflict;
- the means that the Government of Canada 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;

- 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 Government of Canada;
- 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 Government of Canada that is covert in nature;
- the means that the Government of Canada used, uses or intends to use, or is capable of using, to protect or exploit any information or intelligence referred to in any of 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 paragraphs (*a*) to (*f*) that is in relation to, or received from, a foreign entity or terrorist group.

Source: *Security of Information Act,* Section 8

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Canadian SIGINT Security Standards, 1 March 1995

"Sponsoring Authority"

The Senior Indoctrinated Official or another COMINT-indoctrinated official in an Authorized Organization responsible for certifying an individual's access to COMINT based on need to know.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Stand/Standing Alone"

Refers to use of a SIGINT term for reasons other than its security purposes, e.g. for administrative purposes, such as a memo listing available covernames; can apply also to rubber stamps, stamping of envelopes, paper stock, and cover sheets.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Sub-Category"

A sub-division within a COMINT Category to permit differentiation in processing, distribution, exchange or use.

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Directive, DGP/D-2102, March 27, 1998, (Directive supersedes and amalgamates DGP/D-2101, Policy of 9 October 1990, and DGP/D-2102, Policy of 1 March 1991)

s.15(1)

TOP SECRET COMINT
2003-03

Source: OPS-1-1 6 December 2002, Procedures for

Source: Safeguarding the Privacy of Canadians, Annual Report for the period January – December 2000, April 2002

T

Source: Ops-2-3, (Undated)

Source: Canadian SIGINT Security Standards, 1 March 1995

"Targeting"

To single out for collection or acquisition purposes

Source: OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, Revised 20 June 2002, (Supersedes CPP-2010, Safeguarding the Privacy of Canadians)

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)

"Technical Information"

Source: Canadian SIGINT Security Standards, 1 March 1995

"Telecommunications"

As defined in the *Interpretation Act*, Chapter I-21 of the *Revised Statutes of Canada*, any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by wire, radio, visual, or other electromagnetic systems. This includes telephone. telegraph, teletype, facsimile, data transmissions, closed circuit television and remote dictation systems.

Source: Canadian SIGINT Security Standards, 1 March 1995

"TEMPEST"

See Emission Security.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Terrorism-related"

For the purpose of this procedure, "terrorism-related" primarily refers to any foreign-originated threat of violence

Source: , OPS-1-4 October 25, 2001

"Threat Assessment"

An evaluation of the nature, likelihood and consequence of acts or events that could cause a security threat to materialize.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Threats"

Threats include unauthorized disclosure, destruction, removal, modification or interruption of SIGINT, as well as compromise, due to penetration by hostile intelligence services; by otherwise legitimate users who gain access to data or processes for which they are not authorized; or as a result of inadequate security design, implementation or operation.

Source: Canadian SIGINT Security Standards, 1 March 1995

"TRA"

Threat and Risk Assessment. See individual entries.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Traffic"

Communications/messages intercepted for SIGINT purposes.

Source: Canadian SIGINT Security Standards, 1 March 1995

"Traffic Analysis"

Source: Canadian SIGINT Security Standards, 1 March 1995

Source: Canadian SIGINT Security Standards, 1 March 1995

TREASURY BOARD DEFINITIONS - Policy on use of Electronic Networks

"Access"

means gaining entry to an electronic network that the federal government has provided to authorized individuals. Access to such networks may be from inside or outside government premises. Access may support telework and remote access situations or where authorized individuals are using electronic networks provided by the federal government on their own time for personal use.

"Authorized individuals"

include employees of the federal government as well as contractors and other persons who have been authorized by the deputy head to access electronic networks.

"Electronic networks"

are groups of computers and computer systems that can communicate with each other. Without restricting the generality of the foregoing, these networks include the Internet, networks internal to an institution and public and private networks external to an institution.

"Monitoring of electronic networks"

means any action that involves the recording and subsequent analysis of activity on, or use of, a system or electronic network. Examples include recording user accounts, user activities, sites visited, information downloaded and computer resources used to perform a routine analysis of traffic flow on networks, use patterns and sites that certain work groups or individuals have visited. The information recorded and subjected to analysis does not normally involve the contents of individual electronic mail, files and transmissions.

"Unacceptable activity"

is any activity that violates institutional or Treasury Board policy (for examples of Treasury Board policy, see Appendix B), or that violates the limitations on personal use set out in Appendix C to this policy.

"Unlawful activity"

includes criminal offences, contraventions of non-criminal regulatory federal and provincial statutes, and actions that make an authorized individual or an institution liable to a civil lawsuit.

U

Source: OPS-2-1
28 June 2001, Revised January 2002

"UK Person"

A "*UK person*" is defined as a person, organization or other entity (including ships and aircraft) who is either a national of, resident or registered in the UK/British Dependent Territories (For a full list, see Appendix I). Ownership is immaterial, be it of a company, joint venture, aircraft or vessel: if it is resident or registered in the UK, it is considered to be a "UK person".

Source: Procedures Summary (April 28, 1999)

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)

"US Person"

A "*US person*" or entity is

- a US citizen;
- a permanent resident alien (green card holder);
- a corporation incorporated in the US, unless it is openly acknowledged by a foreign government to be directed and controlled by that government;
- an unincorporated association organized in the US or headquartered in the US;
- an unincorporated association with headquarters outside the US, if a substantial number of its members are US citizens or aliens lawfully admitted for permanent residence; or
- a US-flagged non-governmental aircraft or vessel.

Source: Procedures Summary (April 28, 1999)

s.15(1)
s.16(2)(c)

DRAFT WORKING DOCUMENT (Revised: 6 July 2001)

V

"Violation of Security"

Any act or omission that contravenes any provision of the Government Security Policy.

Source: Canadian SIGINT Security Standards, 1 March 1995

"VRK Control System"

Very Restricted Knowledge Control System. The VRK Control System is a system within the COMINT Control System whereby especially sensitive COMINT and COMINT-related information is subject to more restrictive handling and dissemination controls.

Source: Canadian SIGINT Security Standards, 1 March 1995

W

Source: OPS-5-3 1 Procedures - Revised 8 November 2001

X

Y

Z

March 26, 2003