Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Technology Security Guidance

for

Purchasing CSEC-Approved Cryptographic Equipment from the United States Government

ITSG-26

January 2013

Canada

Foreword

The *Information Technology Security Guidance for Purchasing CSEC-Approved Cryptographic Equipment from the United States Government* (ITSG-26) is an UNCLASSIFIED publication issued under the authority of the Chief, Communications Security Establishment Canada in accordance with the Treasury Board of Canada Secretariat *Policy on Government Security*.

The Communications Security Establishment Canada will notify users of changes to this publication.

General inquiries and suggestions for amendments are to be forwarded through departmental communications security channels to COMSEC Client Services at the Communications Security Establishment Canada.

Effective Date

This directive takes effect on date of signature.

Originally signed by

Toni Moffa
Deputy Chief, IT Security

January 31, 2013
Date

Record of Amendments

Amendment No.	Date	Authority

Table of Contents

List of Figures

List of Abbreviations and Acronyms

AFU	Approval for Use
CCD	Canadian Cryptographic Doctrine
CEPAF	COMSEC Equipment Purchase Authorization Form
CERF	COMSEC Equipment Requirements Form
COMSEC	Communications Security
CSEC	Communications Security Establishment Canada
DCA	Departmental COMSEC Authority
DCS	Direct Commercial Sales (U.S.)
DDSM	*Directive on Departmental Security Management*
DoD	Department of Defense (U.S.)
DoS	Department of State (U.S.)
DS	Direct Sales
DSO	Departmental Security Officer
FMS	Foreign Military Sales (U.S.)
GC	Government of Canada
GOTS	Government off-the-shelf
IDIQ	Indefinite Delivery Indefinite Quantity (U.S.)
ISP	Industrial Security Program
ITAR	International Traffic in Arms Regulations (U.S.)
ITSC	Information Technology Security Coordinator
ITSD	Information Technology Security Directive
ITSG	Information Technology Security Guidance
LOA	Letter of Offer and Acceptance
LOR	Letter of Request
MITS	*Management of Information Technology Security*
NDA	National Distribution Authority
NMSO	National Master Standing Offer
NSA	National Security Agency
PA	Purchase Authorization
PGS	*Policy on Government Security*
PWGSC	Public Works and Government Services Canada
PWGSC(O)	Public Works and Government Services Canada – Ottawa
PWGCS(W)	Public Works and Government Services Canada – Washington
RFP	Request for Proposal
SFO	Senior Financial Officer
TBS	Treasury Board of Canada Secretariat
U.S.	United States
USG	United States Government

1 Introduction

1.1 Purpose

The *Information Technology Security Guidance for Purchasing CSEC-Approved Cryptographic Equipment from the United States Government* (ITSG-26) provides instructions and guidance on the purchase of Communications Security Establishment Canada (CSEC)-approved cryptographic equipment available from the United States (U.S.) via Foreign Military Sales (FMS) and Direct Sales (DS).

NOTE: The term Direct Sales as used in Canada is referred to as Direct Commercial Sales (DCS) in the U.S.

1.2 Authority

This document is promulgated pursuant to the *Policy on Government Security* (PGS) that delegates CSEC as the lead security agency and national authority for the development, approval and promulgation of Communications Security (COMSEC) policy instruments. These include directives, guidelines, doctrine, alerts and bulletins.

1.3 Scope

This document covers the purchasing process for U.S. Government off-the-shelf (GOTS) manufactured cryptographic equipment only. U.S. GOTS products are used to protect classified communications and data. These products are controlled under U.S. International Traffic in Arms Regulations (ITAR).

Governments other than the U.S. Government (USG), e.g. the Government of Canada (GC), must obtain approval from the USG prior to procurement. CSEC is the formal interface between the GC and the USG to obtain procurement approvals.

Cryptographic equipment includes equipment and systems designed to protect classified and PROTECTED C information and data for the GC. COMSEC equipment may also include crypto-ancillary equipment, crypto-production equipment and authentication equipment.

COMSEC Client Services should be consulted directly if devices of any other origin are being considered.

1.4 Context

This ITSG supports the PGS and the *Directive on Departmental Security Management* (DDSM). It should be read in conjunction with the following publications:

- *Directive for the Control of COMSEC Material in the Government of Canada* (ITSD-03), September, 2011; and

- *Directive for the use of CSEC-Approved COMSEC Equipment and Key on a Telecommunications Network* (ITSD-04), November 2011.

1.5 Application

This ITSG applies to any GC entity that wishes to purchase CSEC-approved cryptographic equipment that are of U.S. origin.

1.6 Audience

The audience includes Departmental Security Officers (DSOs) and representatives, Departmental COMSEC Authorities (DCAs), project authorities and all others who require COMSEC equipment or are involved in the COMSEC purchasing process.

1.7 Contact Information

COMSEC Client Services at CSEC is the primary point of contact for GC departments with respect to COMSEC equipment and product information:

Telephone: 613-991-8495

E-mail: comsecclientservices@cse-cst.gc.ca

2 Roles and Responsibilities

2.1 Communications Security Establishment Canada

In accordance with the PGS, CSEC is the national authority for COMSEC. This includes the Approval for Use (AFU) of specific devices to protect classified information. For the procurement of COMSEC devices, foreign governments will only deal through their respective national COMSEC agencies. CSEC then prepares the Canadian Cryptographic Doctrine (CCD) and authorizes the use of the equipment by Canada.

NOTE: Additional information about COMSEC authorities, roles and responsibilities can be found in ITSD-03.

2.1.1 COMSEC Client Services

COMSEC Client Services is the primary point of contact for GC departments with respect to CSEC-approved cryptographic equipment and product information.

COMSEC Client Services must approve all cryptographic equipment purchases on a case-by-case basis. In addition to approving purchases, COMSEC Client Services is responsible for the following:

- recommending CSEC-approved COMSEC solutions to GC departments and agencies in accordance with their requirements;
- seeking the release of COMSEC equipment from foreign countries;
- coordinating an initial evaluation of all COMSEC equipment types entering Canada;
- preparing and promulgating AFU documents for all CSEC-approved cryptographic equipment;
- advising on the purchasing vehicle (FMS or DS) to be used for COMSEC equipment;
- assigning the appropriate shipping address and COMSEC account to which the purchased materiel must be shipped to in Canada; and
- approving initial key orders on new equipment.

NOTE: In most cases, the account to which purchased material is shipped to in Canada is the National Distribution Authority (NDA) at CSEC.

2.2 Public Works and Government Services Canada

As the procurement authority for the GC, Public Works and Government Services Canada (PWGSC) must be involved with all cryptographic equipment purchases. According to the PGS, PWGSC ensures the application of security safeguards through all phases of the contracting process within the scope of the Industrial Security Program (ISP).

Specifically, the PWGSC office in Ottawa (PWGSC[O]) is responsible for the contractual arrangements with U.S. manufacturers for DS procurements, while the PWGSC office located in the Canadian Embassy in Washington (PWGSC[W]) is responsible for the contractual arrangements with the USG for FMS procurements. In addition, PWGSC is responsible for providing clients with the status of procurement orders.

NOTE: Private sector companies are responsible to PWGSC on matters of controlled goods and should be in contact with them to ensure participation in the Controlled Goods Program.

2.3 Government of Canada Department

Each GC department is responsible for their own personnel security, information security, physical security, customs broker (refer to Article 4.3), COMSEC requirements and COMSEC asset management.

2.3.1 Departmental Security Officer or Departmental COMSEC Authority

The DSO is appointed by the department Deputy Head. Among other duties, as listed in the PGS, the DSO is the requirements authority responsible for the process to authorize purchases of CSEC-approved cryptographic equipment. A DCA may be appointed by the DSO to act in his or her stead. The DSO or DCA is responsible to initiate and manage the department's purchase process for CSEC-approved cryptographic equipment.

NOTE 1: Depending on the organizational structure, the role of DSO is sometimes shared with that of the departmental Information Technology Security Coordinator (ITSC).

NOTE 2: The ITSC is authorized to sign the COMSEC Equipment Purchase Authorization Form (CEPAF) on behalf of the DSO.

2.3.2 Departmental Procurement Authority (Financial)

The departmental procurement authority is responsible for approving and authorizing procurements prior to contractual processing by PWGSC. Upon approving a given procurement, the departmental procurement authority will review and validate the required documentation as being complete and accurate and forwards it to the appropriate PWGSC procuring authority. The departmental procurement authority is also the main interface between the users and PWGSC.

3 Purchasing Methods

3.1 General

While the mechanics of the purchase process are normally transparent to the user (an order is placed and the client waits until the cryptographic equipment is delivered), the user may 'observe' some differences. For example, the method of payment for FMS requires payment prior to delivery, while DS contracts are paid after delivery and acceptance of the products.

This section describes the two purchase methods (FMS and DS) that apply to all GC departments and that are approved by the USG.

NOTE: Private sector companies are not permitted to purchase or own CSEC-approved cryptographic equipment.

3.2 Prerequisites for Procurement

In order for a GC department to acquire and account for CSEC-approved cryptographic equipment (e.g. U.S. GOTS products), it is required to, as a minimum:

- establish a COMSEC account with CSEC;
- designate a DCA and COMSEC custodial staff (custodian and alternate custodian); and
- ensure staff receive CSEC-approved COMSEC training.

NOTE: The GC department is also required to establish a customs broker to release goods from customs.

3.3 Foreign Military Sales

Purchasing CSEC-approved cryptographic equipment using FMS involves a government-to-government business association. PWGSC(W) is the only Canadian authorized point of contact for FMS contracts. Upon receipt of a funded requirement allocated by the PWGSC commodity management team at the PWGSC headquarters in Ottawa, PWGSC(W) will enter into a supporting government-to-government contract arrangement with the Department of Defense (DoD) for the specified materiel. This unique contract relationship is based on acceptance by PWGSC(W) of a formal USG Letter of Offer and Acceptance (LOA) that details general FMS terms and conditions the USG has in place with COMSEC product manufacturers as well as requirement specific notes. These contracts are also known as Indefinite Delivery Indefinite Quantity (IDIQ).

The FMS agreement is a contract. Attached to it is a list of terms and conditions that dictate the roles and responsibilities of both parties. Among these terms and conditions are the following:

- FMS pricing is normally non-negotiable;
- FMS pricing is subject to change at any time before or after delivery;

- there is a U.S. surcharge for recovery of USG costs;
- pricing may include, but is not limited to, the cost of item, non-recurring research and development and product costs, packaging and handling and administrative surcharges; and
- delivery timelines are not guaranteed and can change based on U.S. priorities.

NOTE: COMSEC Client Services may provide an explanation of USG costs when dealing with a GC client since this surcharge is subject to change.

3.4 Direct Sales

With the DS method, PWGSC negotiates directly with the approved U.S. manufacturer for the equipment being bought, all with the approval of the USG (in the case of cryptographic equipment, the National Security Agency [NSA] gives the approval through CSEC). Only PWGSC(O) is authorized to conduct the necessary contract negotiations for DS cryptographic equipment purchase requests for the GC, regardless of dollar value. The exception is the use of National Master Standing Offers (NMSO) that have been put in place, in which authorized departments may order directly provided the financial call-up (order) limitation identified in the NMSO is respected. These Standing Offers can be found by using the Standing Offer index at: http://soi.pwgsc.gc.ca/app/index.cfm?Fuseaction=sim.search&altlang=-e.

It is important to note that once DS is authorized, the USG is no longer responsible for the transport and condition of the material being purchased. Any problems that arise with respect to the purchase must be resolved by means of negotiations between Canada (PWGSC) and the manufacturer.

4 Purchasing Process

4.1 General

The following sections describe in detail the GC departmental purchasing process of cryptographic equipment from the U.S.

4.2 Requirement Identification

A requirement for a quantity of COMSEC equipment is identified and developed within a GC department. The requirement may be to replace existing inventory or it may be to purchase a new requirement.

NOTE: It is recommended that GC departments involve COMSEC Client Services early in the requirements process to minimize potential delays and to ensure the selection of best fit.

Assuming that the necessary funds are available, or have been committed, the person responsible for the user organization typically identifies the requirement and contacts the appropriate authority (DSO, ITSC, or DCA) for the purpose of COMSEC purchases for that department. In addition to any department-specific approvals that may be required, two forms must be completed and submitted to CSEC. The COMSEC Equipment Requirements Form (CERF) and the CEPAF, when completed and signed by the appropriate authority(ies), contain all the information and authorizations required by CSEC, the USG and the appropriate purchasing authority to initiate the COMSEC equipment purchasing.

NOTE: The CERF is to stay with the client department and CSEC. It is not shared with the USG or PWGSC.

4.3 Staffing

This section describes the two purchase processes (FMS and DS) that apply to all GC departments and that are approved by the USG.

Personnel representing a GC department adhere to the following procedure:

- complete the CERF;
- complete the CEPAF;
- submit the completed CERF and CEPAF forms to COMSEC Client Services;
- once authorized, CSEC will return the CEPAF, complete with a CSEC Purchase Authorization number, to the originating GC department, as described in Step 1 below;
- the originating GC department may then forward a requisition, with the signed and approved CEPAF attached, to PWGSC for procurement (contract) action; and

- shipping direction will be provided as part of the CEPAF (contact COMSEC Client Services for CSEC COMSEC mailing address).

When a GC department places an order for CSEC-approved cryptographic equipment, the U.S. vendor prepares the shipment and sends it to the NDA at CSEC. This shipment will arrive at the Canadian border and must be cleared by the customs agent of the purchasing GC department. The department must identify which customs broker represents their account, typically in the early stages of the purchasing process, to prevent clearance delays. For more information on brokerage firms, contact COMSEC Client Services.

NOTE: The NDA at CSEC is the distribution authority for all CSEC-approved cryptographic equipment in Canada and cannot clear shipments on behalf of other GC departments. Advising your broker and the NDA of incoming shipments will help minimize delays.

4.4 Approval Process

COMSEC Client Services reviews and confirms the requirement, as stated in the CEPAF. If the requirements have been met as detailed in the CERF and CEPAF, COMSEC Client Services assigns a Purchase Authorization (PA) number to the CEPAF. This number is used at CSEC for internal tracking of the purchase.

4.5 Direct Sales

This article is only applicable to DS. If this does not apply, refer to Article 4.6. There are two types of PWGCS contracts: sole source and Request for Proposal (RFP) process. PWGSC is responsible to negotiate the terms and conditions of the contract as well as the price of the material. The DS process is outlined in Steps 1 through 10 below.

Sole Source:

Sole source contracting can only be initiated through PWGSC if there is only a single manufacturer that meets the requirements of the GC department.

Request for Proposal:

If more than one manufacturer can meet the requirements of the GC department, CSEC-approved cryptographic equipment must be purchased through the RFP process.

NOTE 1: Contact PWGSC for detailed information on the Sole source and RFP requirement.

NOTE 2: COMSEC Client Services will provide advice as to the availability of equipment from various manufacturers.

Step 1 – Approval

COMSEC Client Services determines if the USG has provided prior approval for a specific quantity of the particular cryptographic equipment requested by the GC department. This approval is provided to CSEC in the form of a letter of authorization, described in detail in Step 2 below.

If there is no NSA authorization letter on file at CSEC for the requested equipment, or if the quantity required by the GC department results in a situation whereby the NSA authorized quantity is exceeded, CSEC must request an authorization from NSA for an increase of number of DS purchases of the particular product from the manufacturer. If NSA approves the request, another authorization letter is forwarded to the manufacturer and a copy is provided to CSEC. If NSA denies the request, then CSEC informs the client. Typically, the GC department would then choose the FMS route at which time the FMS process would begin.

Step 2 – Sales Authorization

When CSEC requests authorization from NSA for the purchase of a type of cryptographic equipment using DS, and NSA approves the request, a letter of authorization is provided to the manufacturer and CSEC. This letter indicates that NSA has authorized the GC to purchase up to a specific quantity of pieces of that equipment using DS. The letter includes an NSA reference number generated by NSA, which CSEC inserts on the CEPAF, and is used by the manufacturer as authorization to proceed with responding to the PWGSC procurement contract. This contract is linked to the CEPAF, and thus will refer to NSA's reference number, providing the manufacturer with the necessary authorization.

Step 3 – CSEC Notification

An electronic copy of the letter of authorization is forwarded from NSA to CSEC to be retained on file.

Step 4 – National Distribution Authority – Shipping Notification

COMSEC Client Services forwards a copy of the CEPAF to the NDA at CSEC for their files. This step ensures that once the shipment has arrived, NDA personnel will know who is expecting the equipment and who to contact once it is received at the NDA.

Step 5 – Return of Approved CEPAF

Once CSEC has obtained all the information necessary for the procurement to proceed, the CEPAF is signed-off and returned to the CEPAF signing authority of the purchasing department.

Step 6 – Initiation of Purchasing Process

The CSEC-approved CEPAF, along with any other required departmental purchasing documentation (such as funding authorization), is forwarded to the DSO, ITSC or DCA who will forward it to the departmental procurement authority.

Step 7 – Departmental Purchasing Processing

The departmental procurement authority conducts its own authorization process and prepares the necessary purchasing documentation based on the information on the CEPAF and any other attached information, for procurement action through PWGSC(O). PWGSC(W) is not involved in DS purchasing.

Step 8 – PWGSC and NSA Processing

In this part of the acquisition process, PWGSC(O) validates the requisition by confirming all the necessary information has been provided by the requesting GC department, including necessary signatures, purchasing details and the necessary funding control numbers.

Step 9 – Cryptographic Equipment Manufacture and Transport

Once the manufacturer has a valid contract in hand from NSA, the manufacturing of the required cryptographic equipment can begin. Once the order can be filled, it is packaged up and transported to Canada. Export of controlled goods such as COMSEC equipment is subject to stringent U.S. Department of State (DoS) regulations.

In accordance with these regulations, the procured equipment is transported via a courier or freight service authorized to carry controlled goods to the Canada Customs office closest to Ottawa. At that point, a customs broker representing the purchasing GC department arranges for the goods to be released from customs and shipped to the NDA at CSEC. The NDA holds a U.S. COMSEC account, and when GC-bound COMSEC equipment is exported to Canada, it is received into this account.

Step 10 – Delivery of the Cryptographic Equipment to the User

The NDA at CSEC receives the shipment and performs the necessary inspections of the equipment, validating and confirming the order against the records on file associated with this shipment (obtained in step 3). The applicable COMSEC accounting documents are completed and signed and the COMSEC Custodian is informed that the shipment is ready for delivery.

4.6 Foreign Military Sales

This article is only applicable to FMS. For DS, refer to Article 4.5. The FMS process is outlined in Steps 1 through 8 below.

Step 1 – PWGSC Form

PWGSC(O) will complete a form called a 1062 Supply Component (re-allocation), retain a copy of the procurement documentation for record purposes and then forward the original to PWGSC(W). Subsequently, PWGSC(O) has no further formal action with regards to an FMS procurement.

Prior to PWGSC(W) approving and accepting an FMS case, Treasury Board of Canada Secretariat (TBS) policy requires the department's Senior Financial Officer's (SFO's) approval either for each individual FMS transaction (amendments and new contracts), or a blanket approval for the FMS program (preferred approach).

NOTE: Refer to Annex A of the Contracting Policy Notice for Non-Competitive Contracting at http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/ContPolNotices/2007/0920-eng.asp.

Step 2 – Letter of Request

With SFO approval in hand, PWGSC(W) drafts a Letter of Request (LOR), which contains the details of the FMS procurement request based on information in the 1062 form and the CEPAF. This letter is signed and forwarded to NSA.

Upon receipt of the LOR, NSA opens an FMS case file and an FMS Case number is generated for the file. This number will be used as the reference as long as the file remains open.

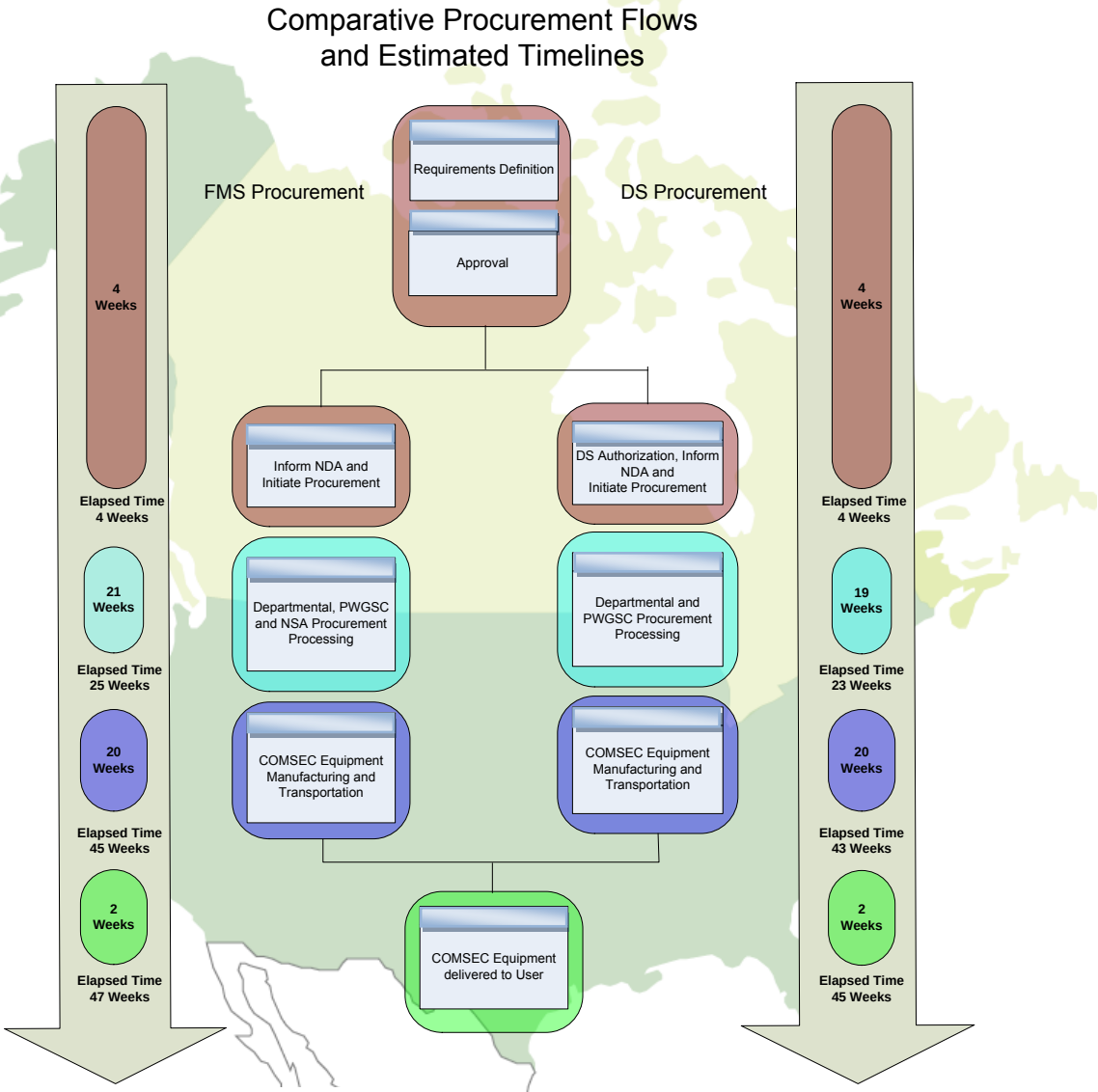
Step 3 – National Distribution Authority – Shipping Notification

COMSEC Client Services forwards a copy of the CEPAF to the NDA at CSEC for their files. This step ensures that once the shipment has arrived, NDA personnel will know who is expecting the equipment and who to contact once it is received at the NDA.

Steps 4 through 8

Same as DS Steps 6 through 10.

A comparative view of the FMS and DS purchasing process and estimated timelines is presented in Figure 1.



Note that FMS Procurement total elapse time from Steps 1 to 8 can range from 24 to 47 weeks (excluding any delays within the purchasing department or delays in obtaining equipment certification from the USG).

Note that DS Procurement total elapse time from Steps 1 to 10 can range from 25 to 45 weeks (excluding any delays within the purchasing department or delays in obtaining equipment certification from the USG).

Figure 1 – FMS and DS Comparative View

5 Glossary

Canadian Cryptographic Doctrine (CCD)	The minimum security standards for the safeguard, control and use of Communications Security Establishment Canada-approved cryptographic equipment and systems.
Communications Security (COMSEC)	The application of cryptographic security, transmission and emission security, physical security measures, operational practices and controls to deny unauthorized access to information derived from telecommunications and that ensure the authenticity of such telecommunications.
COMSEC Custodian	The individual designated by the departmental COMSEC authority to be responsible for the receipt, storage, access, distribution, accounting, disposal and destruction of all COMSEC material that has been charged to the departmental COMSEC Account.
COMSEC Material	Material designed to secure or authenticate telecommunications information. COMSEC material includes, but is not limited to key, equipment, modules, devices, documents, hardware, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.
Crypto Material Assistance Centre (CMAC)	The entity within the Communications Security Establishment Canada responsible for all aspects of key ordering including privilege management, the management of the National Central Office of Record and the administration of the Assistance Centre.
Departmental COMSEC Authority (DCA)	The individual designated by, and responsible to, the Departmental Security Officer for developing, implementing, maintaining, coordinating and monitoring a departmental COMSEC program which is consistent with the *Policy on Government Security* and its standards.
Departmental Security Officer (DSO)	The individual responsible for developing, implementing, maintaining, coordinating and monitoring a departmental security program consistent with the *Policy on Government Security* and its standards.

6 Bibliography

The following source documents were used in the development of this ITSG:

- **Communications Security Establishment Canada:**
  - *Directive for the Control of COMSEC Material in the Government of Canada* (ITSD-03), October 2011.
  - *Directive for the use of CSEC-Approved COMSEC Equipment and Key on a Telecommunications Network* (ITSD-04), November 2011.
- **Public Works and Government Services Canada:**
  - *Supply Manual*, Version 08-2, December 12, 2008.
- **Treasury Board of Canada Secretariat:**
  - *Directive on Departmental Security Management* (DDSM), July 2009.
  - *Management of Information Technology Security* (MITS), May 2004.
  - *Policy on Government Security* (PGS), July 2009.