Communications Security Establishment
Centre de la sécurité des télécommunications

IT Security Directive for the Control and Management of In-Process COMSEC Material

ITSD-08

April 2016

Canada

Foreword

The *IT Security Directive for the Control and Management of In-Process COMSEC Material* (ITSD-08) is an UNCLASSIFIED publication issued under the authority of the Chief, Communications Security Establishment in accordance with the Treasury Board of Canada Secretariat *Policy on Government Security*.

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

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

Effective Date

This directive takes effect on date of signature.

Original signed by

Scott Jones
Deputy Chief, IT Security

April 25, 2016

Reproduction and Distribution

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose

This directive provides Communications Security (COMSEC) practitioners with the minimum security requirements for the handling of COMSEC material where the normal accounting system is not possible because of board or component level integration activities. This situation requires a separate control and accounting system called an "In-Process (IP)" COMSEC accounting system. This COMSEC material will be hereinafter designated as IP COMSEC material.

For the purpose of this directive, COMSEC practitioners include departmental and private sector COMSEC authorities (sponsors and planners) as well as the custodial personnel appointed to manage and control IP COMSEC material within an IP COMSEC Account.

1.1.1 In-Process

IP is an international recognized term used in COMSEC channels to describe the detailed accounting methods and records, which enable contractors to control COMSEC material during development, manufacture, and assembly phases.

1.2 Authority

This directive is promulgated pursuant to the *Policy on Government Security* (PGS) that delegates the Communications Security Establishment (CSE) as the lead security agency and national authority for COMSEC. CSE is responsible for the development, approval and promulgation of COMSEC policy instruments and for the development of guidelines and tools related to Information Technology (IT) security.

The Deputy Chief, IT Security (DCITS), at CSE, is the promulgation authority for COMSEC policy instruments.

1.3 Scope

The methods used for controlling COMSEC material vary and are determined by the nature of the material itself. The scope of this directive includes:

- cryptographic key or cryptographic equipment (including Controlled Cryptographic Items [CCIs] and sensitive IP COMSEC parts, components and assemblies) which are being developed, manufactured, assembled, disassembled, destroyed, produced or reproduced before being controlled in the National COMSEC Material Control System (NCMCS) or a foreign national COMSEC system;
- cryptographic equipment (normally controlled in NCMCS) which is under a Repair and Maintenance (R&M) contract and includes the removal or insertion of accountable COMSEC parts, components or assemblies; and
- accountable COMSEC publications (normally controlled in NCMCS) and IP manuscripts being developed or under contract for translation or reproduction.

1.4 Context

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

- *IT Security Directive for the Control of COMSEC Material in the Government of Canada* (ITSD-03A);

- *Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material* (ITSD-05); and
- *IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector* (ITSD-06A).

1.5 Application

This directive applies to Government of Canada (GC) departments and private sector companies that are authorized to hold CSE-approved COMSEC material under sponsorship (i.e. GC contract procured through Public Services and Procurement Canada [PSPC] or other CSE-approved agreement) as well as the entities listed in Article 2 that support the deployment of Accountable COMSEC Material (ACM) and other IP COMSEC material to GC and private sector IP COMSEC Accounts.

For the purpose of this directive, the term:

- "GC department" includes any federal institution (e.g. Department, Agency, Organization [DAO]) subject to PGS and to Schedules I, I.1, II, IV and V of the *Financial Administration Act* (FAA);
- "Other Levels of Government" includes provincial, municipal and local government organizations (e.g. law enforcement agencies); and
- "private sector company" includes Canadian companies, organizations or individuals that do not fall under the FAA or are not subordinate to a provincial or municipal government. It also includes Canadian-based industries (or other non-government organizations) where security is administered by the Industrial Security Program (ISP) of PSPC.

1.6 Expected Results

Application of this directive will ensure that a minimum level of control, safeguard and accounting is maintained for CSE-approved COMSEC material provided to an IP COMSEC Account and for security of COMSEC material being developed or modified prior to being transitioned to NCMCS.

1.7 Compliance

Compliance with the minimum security requirements identified in this directive is the responsibility of the CSE Industrial COMSEC Account (CICA), sponsoring GC departments and sponsored private sector companies.

NOTE: Except when otherwise specifically identified, the term "responsible authority" will refer to the responsible GC department or COMSEC Client Services for GC COMSEC IP Accounts and to CICA or GC sponsor for private sector IP COMSEC Accounts.

Failure to comply with this directive may result in escalated administrative controls being placed on an IP COMSEC Account. In extreme circumstances, an IP COMSEC Account will be suspended or closed until an external audit is conducted by CSE and the IP COMSEC Account shortcomings are rectified.

1.8 Conflict Resolution

Any conflict encountered between this Information Technology Security Directive (ITSD) and any other national (e.g. other ITSDs, PGS, DDSM) or international (e.g. *International Traffic in Arms Regulations* [ITAR]) publications must be submitted to COMSEC Client Services for resolution.

1.9 Requests for Exception or Waiver

A request for an exception (substitution) or a waiver (temporary exemption from a specific requirement) must be submitted by the GC or CICA's Departmental COMSEC Authority (DCA) in writing, and with a justification, to COMSEC Client Services for approval.

NOTE: COMSEC Client Services periodically (annually, at a minimum) reviews exceptions for operational suitability and risk, and assesses progress towards the elimination of waivers.

1.10 Additional Regulations Affecting Acquisition of COMSEC Material

1.10.1 Foreign Ownership, Control or Influence

A private sector company will normally require a PSPC ISP Foreign Ownership, Control or Influence (FOCI) assessment before being provided access to ACM or other IP COMSEC material to fulfil a contract deliverable or in support of a CSE-approved requirement. This assessment is designed to ensure that there are no factors present in the private sector company's ownership and control arrangements that could allow unauthorized access to COMSEC material. A private sector company will be considered under FOCI when a reasonable basis exists, as determined by the FOCI assessment, to conclude that the nature and extent of foreign ownership, control or influence is such that control over the management or operations of the facility may result in the unauthorized access to COMSEC material by foreign parties or their agents.

NOTE: Requests for FOCI exemption must be submitted to COMSEC Client Services.

1.10.2 Canadian Controlled Goods Program

The Canadian Controlled Goods Program (CGP) is a domestic industrial security program within PSPC that is mandated under *Controlled Goods Regulations* to help strengthen Canada's defence trade controls and to prevent the proliferation of tactical and strategic assets. Acceptance of the control and management requirements of ACM detailed in this and other CSE directives – including Accountable COMSEC Material Control Agreements (ACMCAs), Memorandums of Understanding (MOUs), Memorandums of Agreements (MOAs), Non-Disclosure Agreements and Technical Assistance Agreements (TAAs) – does not exempt a private sector company from having to implement the requirements of the Canadian CGP.

1.10.3 United States International Traffic in Arms Regulations

The *International Traffic in Arms Regulations* (ITAR) is a set of United States (U.S.) government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML).

A significant amount of GC COMSEC material is of U.S. origin. Acceptance of the control and management requirements of COMSEC material detailed in this directive and other CSE directives – including ACMCAs, MOUs, MOAs and Non-Disclosure Agreements – does not exempt a private sector company from having to implement the requirements of ITAR. For advice and guidance on the movement of ITAR-controlled COMSEC material, contact COMSEC Client Services or CICA as appropriate.

1.11 Contact Information

The following table contains contact information for offices that provide COMSEC support to users.

NOTE: Unless otherwise specified, CSE's telephone and secure fax contact numbers listed in Table 1 are attended from 8 a.m. to 4 p.m. Eastern Time, Monday to Friday.

Table 1 – Contact Information for COMSEC Offices

COMSEC Client Services	
Telephone: 613-991-8495	**E-mail:** comsecclientservices@cse-cst.gc.ca
Secure Fax: 613-991-8565	
CSE Industrial COMSEC Account (CICA)	
Telephone: 613-991-7272	**E-mail:** cica-ccic@cse-cst.gc.ca
Fax/Secure Fax: 613-991-7593	
National COMSEC Incidents Office (NCIO)	
Telephone: 613-991-8175	**After office hours**
Fax: 613-991-7588	**Telephone:** 613-991-8762
Secure Fax: Call 613-991-8175 for set up	**Secure Fax:** 613-991-8766
E-mail: ncio@cse-cst.gc.ca	**E-mail:** cansoc@cse-cst.gc.ca

1.12 COMSEC User Portal

Authorized users may access the CSE COMSEC User Portal (CUP) at https://comsecportal.cse-cst.gc.ca. The CSE CUP provides COMSEC-related UNCLASSIFIED and PROTECTED A information, as well as Field Software Upgrades (FSUs) associated with CSE-approved high assurance products, systems and services. For information on becoming an authorized user of the CSE CUP, contact the CSE Crypto Material Assistance Centre (CMAC) at cmac-camc@cse-cst.gc.ca or via telephone at 613-991-8600.

1.13 Communications Security Establishment Website

COMSEC directives and information (UNCLASSIFIED only) associated with CSE-approved high assurance products, systems and services are available at https://www.cse-cst.gc.ca/en/group-groupe/high-assurance-technologies.

1.14 COMSEC Forms

COMSEC forms identified within this directive may be obtained on the CSE website.

1.15 Transmission of Information and Data about CSE-Approved COMSEC Systems and Services

Transmission of information and data, in part or in whole, about CSE-approved COMSEC systems and services controlled by the GC or by a GC-sponsored organization may be distributed electronically or physically.

NOTE: In all cases transmission of extracts must be labelled with the appropriate security classification.

1.15.1 Electronic Transmission

Information and data about CSE-approved COMSEC systems and services must be distributed electronically as follows:

- CONFIDENTIAL up to TOP SECRET, and PROTECTED C – disseminated electronically on GC networks using CSE-approved encryption capabilities. This includes secure telephony, facsimile and network services where the communications service must be accredited to a level commensurate with the classification of the information being processed;
- PROTECTED B – disseminated electronically on GC networks, including secure facsimile, or on a public network when protected minimally with GC Public Key Infrastructure (PKI) encryption; and
- PROTECTED A – disseminated electronically on GC networks or on a public network when protected minimally with GC PKI encryption, or a HyperText Transfer Protocol Secure (HTTPS) encrypted connection, or unclassified point-to-point facsimile that originates and terminates in an operations zone.

1.15.2 Physical Transmission

Physical (mail or courier) transmission of protected and classified information and data about CSE-approved COMSEC systems and services must be in accordance with the direction in ITSD-03A and ITSD-06A.

2 Roles and Responsibilities

2.1 Communications Security Establishment

CSE is Canada's national COMSEC authority. As such, CSE has the authority to release COMSEC material to the GC or private sector and is responsible for approving the certification, acquisition and use of cryptographic equipment and key, as well as developing COMSEC-related policy instruments, that protect classified and PROTECTED C information.

2.1.1 COMSEC Client Services

Under the direction of DCITS, COMSEC Client Services is responsible to provide advice, guidance and direction to the GC, as well as the private sector, for the handling of CSE-approved COMSEC solutions and material.

COMSEC Client Services' responsibilities, as they relate to the private sector, include:

- providing an assessment of suitability when there is an approved requirement to bid on a contract (e.g. Request for Proposal [RFP]) where the company has not previously established a COMSEC Sub-Account (refer to ITSD-06A);
- authorizing the establishment or closure of IP COMSEC Accounts;
- validating private sector requirements to hold CSE-approved COMSEC solutions and material;
- confirming all security prerequisites and inspections are met by a GC department or private sector company prior to authorizing the release of ACM or other COMSEC material to its IP COMSEC Account:
    - Facility Security Clearance (FSC) or its equivalent;
    - Document Safeguarding Capability (DSC) inspection or its equivalent;
    - COMSEC Safeguarding Inspection (CSI);
    - Production inspection (for IP requirements); and

- FOCI assessment (refer to Article 1.10.1);

- coordinating the signing of ACMCAs, TAAs, Non-Disclosure Agreements and other agreements as required;
- validating Key Material Support Plans (KMSPs) (refer to ITSD-04), as required;
- coordinating the provision of TEMPEST inspections; and
- coordinating cross-border shipments of IP COMSEC material with other national security authorities.

2.1.2 CSE Industrial COMSEC Account

Under the direction of the CICA DCA, CICA is responsible for the management and control of CSE-approved COMSEC solutions and material provided to private sector IP COMSEC Accounts. CICA's responsibilities include:

- being the initial point of contact for issues pertaining to the management of IP COMSEC Accounts (including reporting of COMSEC incidents);
- ensuring adherence to IP COMSEC material management rules and providing support and guidance on the use of CSE-approved cryptographic equipment and key;
- completing private sector IP COMSEC Account audits (refer to ITSD-06A); and
- authorizing and coordinating the movement and distribution of IP COMSEC material within Canada (providing courier certificates as required).

2.1.2.1 CSE Industrial COMSEC Account Departmental COMSEC Authority

Under the direction of the DCITS, the CICA DCA is responsible for developing, implementing, maintaining, coordinating and monitoring a private sector COMSEC program that is consistent with the PGS and its related policy instruments for the management of COMSEC. Additionally, the CICA DCA is responsible for the overall control of CSE-approved COMSEC material that has been charged to CICA.

2.2 Government of Canada Department

GC departments who have a requirement to establish a new GC COMSEC Account must follow ITSD-03A. However, to establish an IP COMSEC Account, GC departments must contact COMSEC Client Services (refer to Article 3.1).

2.3 Private Sector Company

Private sector companies who have a requirement to establish a new GC COMSEC Sub-Account must follow ITSD-06A. However, to establish an IP COMSEC Account, private sector companies must refer to Article 3 within this directive.

2.3.1 Government of Canada Departmental Sponsor – Private Sector Company

A private sector company must be sponsored by a GC department (hereinafter referred to as GC sponsor) that has a current COMSEC Account prior to any ACM being provided. The GC sponsor's DCA must be actively engaged and provide continuing oversight in all aspects of the IP COMSEC Account, including:

- notifying COMSEC Client Services that a private sector company will require access to ACM;
- identifying ACM requirements and submitting a completed *COMSEC Equipment Requirements* (CER) and a *COMSEC Equipment Purchase Authorization* (CEPA) form (if required) to COMSEC Client Services;

- providing FSC, DSC and CSI equivalent inspections (as required by CSE) for a sponsored private sector company that does not hold a GC contract;
- confirming that a private sector company is CGP and ITAR compliant before releasing ACM;
- ensuring COMSEC Client Services is in receipt of the approved contract Security Requirements Check List (SRCL), including amendments if applicable;
- signing the ACMCA as the sponsoring department and identifying all extension criteria;
- providing a Controlling Authority for authorized Cryptographic Networks (cryptonets), if required (refer to ITSD-04); and
- coordinating with CICA the release of ACM to a private sector company once all prerequisites for the establishment of an IP COMSEC Account have been met (refer to Article 3) and coordinating the withdrawal of sponsor-provided material at end of contract.

2.3.2 Chief Executive Officer/Key Senior Official

The private sector company Chief Executive Officer (CEO) or Key Senior Official (KSO), hereinafter referred to as the CEO, is responsible for the appointment of a Company Security Officer (CSO). If the private sector company is seeking registration in the ISP, the procedures detailed in the PSPC Industrial Security Manual (ISM) should be followed.

2.3.3 Company Security Officer

The CSO is responsible to the CEO for the overall company COMSEC security posture. The private sector CSO responsibilities for COMSEC control and management as they relate to IP include:

- coordinating the signing of ACMCAs by a senior company official;
- ensuring the management of COMSEC material and other IP assets as detailed in this directive, and as directed by CICA;
- ensuring FOCI (refer to Article 1.10.1), Canadian CGP (refer to Article 1.10.2), and ITAR (refer to Article 1.10.3) requirements are met;
- appointing the company IP COMSEC Custodian and IP COMSEC Alternate Custodian(s);
- ensuring the IP COMSEC custodial staff receive formal CSE COMSEC management training;
- ensuring COMSEC management requirements are reflected in company security orders;
- ensuring that there is an FSC to the appropriate level and that CSI, DSC and Production inspections are completed prior to accepting IP COMSEC material;
- ensuring COMSEC briefings and *COMSEC Briefing Certificates* are provided to personnel requiring access to IP COMSEC material (copies of *COMSEC Briefing Certificates* must be provided to CICA);
- processing the requirement for COMSEC visits (i.e. visits that involve access to IP COMSEC material as detailed in the PSPC ISM and this directive). Visitor clearance requests must be submitted through the PSPC ISP. The ISP will then submit a COMSEC access authorization request through COMSEC Client Services;
- ensuring visit authorization is received from the ISP prior to permitting visitors access to IP COMSEC material;
- developing a COMSEC Emergency Plan (refer to ITSD-06A);

- reporting COMSEC incidents to CICA (refer to ITSD-05 and ITSD-06A); and
- ensuring sub-contractors meet the security requirements of the PSPC ISM and of this directive prior to being provided access to IP COMSEC material.

2.3.4 Separation of Duties

The CSO must not hold the position of company IP COMSEC Custodian or Alternate Custodian.

2.3.5 Multiple COMSEC Account Assignment

The CSO may assign the company COMSEC Sub-Account Custodian or Alternate Custodian to concurrently be the company IP COMSEC Custodian or Alternate Custodian.

2.3.6 In-Process COMSEC Custodian

The IP COMSEC Custodian is responsible for the receipt, custody, distribution, disposition or destruction, and accounting of IP COMSEC material charged to their IP COMSEC Account. Specifically these responsibilities include:

- protecting and controlling IP COMSEC material charged to the IP COMSEC Account;
- maintaining knowledge and record of the company's involvement in GC or foreign contracts and programs that require ACM support as it concerns IP COMSEC Account activity;
- retaining all copies of contract SRCLs, where applicable, as part of the custodial records and ensuring compliance with those requirements as they apply to COMSEC matters;
- ensuring the safeguarding and accounting for all IP COMSEC material issued to the company IP COMSEC Account, or produced within the facility;
- maintaining COMSEC accounting and related records as detailed in this directive;
- conducting an IP COMSEC inventory and submitting an *Inventory Report* (GC-223) to CICA when requested by CICA;
- disposing of IP COMSEC material only when directed and by means authorized by CICA;
- submitting *Inventory*, *Destruction*, and *Possession Reports* (GC-223s) when required;
- ensuring the prompt and accurate entry of all amendments to accountable COMSEC publications (refer to ITSD-06A);
- ensuring that required page checks are performed on all IP COMSEC material requiring page checks;
- being aware at all times of the location of every item of IP COMSEC material held by the facility and the general purpose for which it is held;
- establishing "in-house" procedures to ensure strict control of each item of IP COMSEC material whenever the material is outside of the IP COMSEC Account's secure storage facility;
- reporting immediately to the CSO all known or suspected COMSEC incidents;
- verifying the access to IP COMSEC material prior to granting access to such material or any records or files associated with the IP COMSEC Account;
- notifying, in writing, the local mail room or shipping/receiving department of the requirement to deliver all parcels or envelopes addressed to the IP COMSEC Custodian or marked "TO BE OPENED ONLY BY THE IP COMSEC CUSTODIAN" directly to the IP COMSEC Custodian without opening them

beforehand. Further, if the outer wrapper is inadvertently opened, the outer wrapper must be delivered to the IP COMSEC Custodian with the package;

- COMSEC briefing all personnel who require access to IP COMSEC material;
- ensuring IP COMSEC material issued in support of a specific contract is not used for another contract unless authorized by the GC sponsor and CICA is informed;
- reporting any issues or concerns regarding IP COMSEC material management to the CSO or CICA, as appropriate;
- ensuring the Alternate Custodian(s) maintain their knowledge of the IP COMSEC Account requirements at a level that will allow proper management of the IP COMSEC Account in the absence of the IP COMSEC Custodian;
- ensuring this directive is adhered to by all company personnel who handle or manage IP COMSEC material;
- verifying that there is a continued need for IP COMSEC material by Loan Holders/Users; and
- advising CICA of any changes that affect the management of the IP COMSEC Account.

2.3.7 In-Process COMSEC Alternate Custodian

The IP COMSEC Alternate Custodian duties include:

- keeping aware of and assisting in the day-to-day activities of the IP COMSEC Account in order to assume the duties of the IP COMSEC Custodian, whenever necessary and without undue interruption of operations;
- performing the duties of the IP COMSEC Custodian during a period of temporary absences not exceeding 60 calendar days; and
- in the event of the permanent departure or unauthorized absence (61 calendar days or more) of the IP COMSEC Custodian, performing the duties of the IP COMSEC Custodian until the appointment of a new IP COMSEC Custodian.

3 Establishing or Closing an In-Process COMSEC Account

3.1 Establishing an In-Process COMSEC Account

COMSEC Client Services is the authority to release COMSEC material to the GC or private sector and for the establishment of an IP COMSEC Account within the GC or private sector. A GC department or private sector company that is involved in an In-Process contract must first establish a GC COMSEC Account or company COMSEC Sub-Account and then establish the IP COMSEC Account. An IP Plan (refer to Article 3.2) must be approved by COMSEC Client Services before an IP COMSEC Account can be established. COMSEC Client Services is the approving authority for establishing IP COMSEC Accounts (refer to Article 2.1.1). An IP COMSEC Account must meet the same requirements as for the establishment of a COMSEC Account or COMSEC Sub-Account as applicable (refer to ITSD-03A and ITSD-06A). The IP COMSEC Account must be registered to a security clearance at least equal to the highest sensitivity of the COMSEC material held in the IP COMSEC Account, but never less than SECRET.

The IP COMSEC Account must not be registered in NCMCS, but is reportable back to the appropriate responsible authority (refer to Article 1.7).

NOTE: A GC COMSEC Account Custodian or a private sector company COMSEC Sub-Account Custodian is permitted to hold the position of IP COMSEC Custodian if the two accounts are co-located.

3.1.1 COMSEC Custodial Personnel

The CSO must carefully screen individuals who have been selected to become an IP COMSEC Custodian or IP COMSEC Alternate Custodian to ensure that each proposed individual:

- is a Canadian citizen (including those of dual nationality);
- possesses a security clearance at least equal to the highest sensitivity of the COMSEC material held in the IP COMSEC Account, but must never be less than SECRET;
- possesses a current *COMSEC Briefing Certificate*;
- is a responsible individual who is qualified to assume the duties and responsibilities of IP COMSEC Custodian or IP COMSEC Alternate Custodian;
- is in a position or level of authority, which would permit the individual to exercise proper jurisdiction in fulfilling the responsibilities of the position;
- has not previously been relieved of COMSEC Sub-Account Custodian, Alternate COMSEC Sub-Account Custodian, IP COMSEC Custodian or IP COMSEC Alternate Custodian duties for reasons of negligence or non-performance of duties;
- will not be assigned duties that would interfere or conflict with the duties as IP COMSEC Custodian or IP COMSEC Alternate Custodian and will receive CSE-approved training before starting the role.

3.2 In-Process Plan

An IP Plan must be developed and submitted to COMSEC Client Services for approval prior to the establishment of an IP COMSEC Account. The IP Plan should be part of and include contractual Data Item Descriptions (DIDs) and Contract Data Requirements List (CDRLs).

3.2.1 Content of the In-Process Plan

The IP Plan must include the following:

- purpose of the IP Plan;
- references and definitions used in or to develop the IP Plan;
- name, address and account number of the IP COMSEC Account (if known);
- individual responsibilities and duties;
- list of contacts that includes minimally the names, phone numbers and e-mail addresses of the following:
  - Project Management Office (PMO),
  - GC sponsor (may also be the PMO) for private sector,
  - IP COMSEC Custodian/Alternate Custodian,
  - DCA or CSO as applicable,
  - CICA COMSEC Custodian (for private sector), and
  - COMSEC Client Services.
- access and storage requirements, including a floor plan if possible, and any No-Lone Zone (NLZ) and Two-Person Integrity (TPI) control requirements;

- list of the item(s) to be controlled and the point in the production process at which an item becomes IP COMSEC material, and becomes subject to IP accounting;

  NOTE: Assistance in identifying this point and in determining the level of security classification or protected level is available by contacting COMSEC Client Services.

- accounting records (with examples) that reflect an accurate accounting status of each individual IP item or portions thereof, at every stage of production at any given time;
- internal and external processes for the reconciliation of accounting records;
- procedures for the control of material during all aspects of its production as well as any form of drafts, extracts, waste, scrap, etc., applicable to that production;
- shipment methods for transfer or issue of IP COMSEC material;
- methods of disposal of breakage, waste and scrap, as well as authority and accounting procedures to reflect the disposal of the items;
- procedures for the entry of COMSEC material from NCMCS into the IP accounting system and transition of completed items into NCMCS;
- identity of sub-contractors, where applicable;
- COMSEC incident reporting procedures;
- an addendum to the plan for each contract where processing of IP COMSEC material is required, identifying the COMSEC material to be produced, modified or repaired under that contract and describing any procedures that are specific to that contract; and
- any special instructions.

3.2.2 Approval of an In-Process Plan

A COMSEC Client Services-approved IP Plan must be in place before the release or commencement of work on IP COMSEC material by a GC department contractor or a sub-contractor(s). The approval process for IP Plans (including sub-contracts) that involve COMSEC material subjected to IP controls is outlined in Tables 2 and 3.

3.2.3 Changes to an In-Process Plan

If changes to the planned development or production process are required, the IP Plan must be amended in accordance with the instructions in this section. Changes to an IP Plan must not be implemented before approval from COMSEC Client Services.

3.3 Closing an In-Process COMSEC Account

3.3.1 In-Process COMSEC Account Closure Request

When an IP COMSEC Account no longer has a requirement to hold COMSEC material (e.g. completion of a contract requiring ACM or other COMSEC material), the Departmental Security Officer (DSO) or CSO must provide COMSEC Client Services with a written request to close the IP COMSEC Account.

Once authorized by COMSEC Client Services to close the IP COMSEC Account, the DSO or CSO must:

- direct the IP COMSEC Custodian to return all COMSEC material held to the GC department COMSEC Account or CICA (for private sector);

- provide COMSEC Client Services or CICA with a *Termination Certificate* (refer to Block D of the *Appointment Certificate*) for all IP COMSEC Account personnel; and
- upon receiving confirmation of IP COMSEC Account closure from COMSEC Client Services or CICA, return all IP COMSEC Account files to the GC department COMSEC Account or CICA.

3.3.2 CSE-Required Closure

Under extenuating circumstances, CSE may close an IP COMSEC Account. The GC department or company will be notified in writing of the intent to close the IP COMSEC Account.

NOTE: Examples of extenuating circumstances are: failure to apply correct COMSEC procedures or maintain proper physical security, sale of the company, bankruptcy or cancellation of a contract.

3.3.3 Prerequisite for Closure

An IP COMSEC Account will be closed when the following steps have been completed:

- all COMSEC material has been returned to the GC department COMSEC Account or CICA resulting in a "Zero Balance" IP COMSEC Account; and
- the DSO or CSO has sent *Termination Certificates* (refer to Block D of the *Appointment Certificate*) as well as all the IP COMSEC Account records.

3.3.4 Closure Confirmation

Once CICA has confirmed that the closure prerequisites have been met, the DSO or CSO will be notified in writing that the IP COMSEC Account has been closed and that the IP COMSEC Account custodial personnel have been relieved of their responsibilities regarding the account.

Until formal notification is received from CICA or COMSEC Client Services, the IP COMSEC Custodian and Alternate COMSEC Custodian remain responsible for the IP COMSEC Account and any discrepancies involving associated COMSEC material.

Table 2 – Approval Process for an In-Process Plan

Step	Action
1	The GC department or private sector company (in coordination with the GC sponsor) must submit a draft IP Plan to COMSEC Client Services 90 calendar days before the start date of the IP work – sooner if possible.
2	COMSEC Client Services will review the draft IP Plan and provide comments, if any, to the GC department or private sector company.
3	When the plan is acceptable to CSE, the GC department or private sector company (if required by contractual agreement) must submit the IP Plan formally to the GC client department's contract coordinating office or PMO, with a copy to the responsible authority (refer to Article 1.7).
4	CSE will issue formal approval to the GC department and the private sector company. IP Plan approval requires responsible authority signatures (refer to step 3).

Table 3 – Approval Process for a Sub-Contractor In-Process Plan

Step	Action
1	The primary contractor must ensure that the applicable requirements for IP Plan (as set forth in this section) are specified in the contract with the sub-contractor.
2	The primary contractor must ensure that the sub-contractor develops an IP Plan.
3	The primary contractor will review the draft IP Plan and provide comments, if any, to the sub-contractor.
4	In coordination with the GC sponsor, the primary contractor must submit a draft IP Plan to COMSEC Client Services on behalf of the sub-contractor 90 calendar days before the start date of the IP work – sooner if possible.
5	CSE will review the draft IP Plan and provide comments, if any, to the primary contractor.
6	When the plan is acceptable to CSE, the primary contractor must, if required by contractual agreement, submit the IP Plan formally to the GC department's contract coordinating office or PMO, with a copy to CICA and the sub-contractor.
7	CSE will issue formal approval to the GC department and the primary contractor.

4 Accounting for In-Process COMSEC Material

4.1 In-Process Accounting System

The IP COMSEC Custodian must use a CSE-approved IP accounting system to account for IP COMSEC material.

4.2 In-Process Accounting

IP accounting records must contain the following information for each item:

- the date that the item was introduced into the IP accounting system within the facility (including IP items being returned by a sub-contractor or the government, or being returned for rework);
- a brief, unclassified description of the items to be controlled, which may include one or a combination of the following elements:
  - North Atlantic Treaty Organization (NATO) Stock Number,
  - U.S. Federal Stock Number,
  - CSE or vendor part number,
  - short title (if applicable),
  - sensitivity (classification or protected level, or CCI – refer to Article 6.2),
  - Accounting Legend Code (ALC), if required,
  - quantity (when accounting by quantity is approved) or serial number (if individual item accounting is required); and

- disposition:
  - incorporated into a higher assembly (identify the higher assembly), or otherwise made a part of another item of IP COMSEC material,
  - transferred or issued within IP accounting procedures,
  - entered into NCMCS as an individual accountable item,
  - destroyed or declassified,
  - re-entered into the IP accounting for rework, or
  - any other disposition not covered above.

4.3 Reconciliation of In-Process Accounting

The IP COMSEC Custodian and an appropriately cleared and COMSEC-briefed witness must conduct reconciliation of IP accounting records semi-annually and at final delivery of the COMSEC material. The reconciliation must determine that every item brought into the IP accounting system or produced within the IP process is accounted for by physically sighting the COMSEC material to ensure that it:

- is still in the IP process or has been integrated or destroyed;
- is in IP COMSEC material storage;
- has been transferred out as a delivery of completed COMSEC material; or
- has been transferred or issued to a contractor, sub-contractor or the GC client department.

Any item that cannot be accounted for must be immediately reported as a **COMSEC incident** as detailed in ITSD-05.

NOTE: Requirements for conducting reconciliation at irregular intervals may be requested by COMSEC Client Services or CICA.

5 In-Process Accounting Reports

5.1 General

The following articles describe reports that track the flow of IP COMSEC material in varying circumstances.

5.2 Movement of In-Process Material

An IP COMSEC Custodian must transfer IP COMSEC material from one IP COMSEC Account to another IP COMSEC Account using a *Transfer Report* (GC-223) with an IP transaction number. The *Transfer Report* must state that the COMSEC material is IP COMSEC material and the reason for the transfer, such as "PROVIDED TO SUPPORT CONTRACT (insert number)". The IP accounting records must be annotated to reflect the transfer quoting the IP transaction number of the *Transfer Report*.

5.3 In-Process Transfer Report Receipt

A COMSEC Custodian who receives IP COMSEC material from another account must sign both copies of the *Transfer Report* that the sending COMSEC Custodian sent with the IP COMSEC material to confirm the material and integrity of IP COMSEC material received. He or she must also assign an incoming IP transaction number to it for tracking purposes, keep one copy and send the other back to the sending COMSEC Custodian for his or her records. The IP accounting records must then be annotated to reflect the receipt of the material.

5.4 In-Process Hand Receipt

When IP COMSEC material is issued to a Loan Holder before GC acceptance of the final product, the IP COMSEC Custodian must issue the material on a *Hand Receipt* (GC-223). The *Hand Receipt* must be assigned an outgoing IP transaction number and contain the information in Figure 1. The loan period should not exceed 90 calendar days without renewal. The IP accounting records must be annotated to reflect the issue. The IP COMSEC material must be shipped directly to the Loan Holder. The Loan Holder must sign and return one of the copies.

5.5 Transfer Following Government of Canada Acceptance

Following GC acceptance and purchase, the IP COMSEC Custodian must transfer the IP COMSEC material from the IP COMSEC Account to either the GC sponsor's COMSEC Account or the company's COMSEC Sub-Account for entry into NCMCS. The *Transfer Report* must be annotated in the remarks column with "NEW COMSEC MATERIAL".

For entry into the company's COMSEC Sub-Account, the COMSEC Sub-Account Custodian must complete a *Possession Report* (GC-223) to enter the COMSEC material into NCMCS. The material must then be sent to the responsible authority (refer to Article 1.7), which will in turn coordinate the transfer of the COMSEC material to the GC sponsor.

5.6 Temporary Release to Government of Canada

If for some reason it is necessary to temporarily release IP COMSEC material to the GC, a copy of the *Hand Receipt* (GC-223) must be provided to the COMSEC Account at which the receiving Loan Holder is registered (or to the DSO if the GC department does not have a COMSEC Account). The IP COMSEC material must not be entered into NCMCS.

NOTE: The IP COMSEC Custodian must contact the COMSEC Custodian or the DSO to ensure the Loan Holder has the appropriate security clearance, has been COMSEC briefed and has the appropriate storage for the IP COMSEC material.

5.7 Hand Receipt Renewal

The IP COMSEC Custodian must review *Hand Receipts* minimally every 90 calendar days to ensure IP COMSEC material is returned before its due date. If the *Hand Receipt* needs to be renewed, the IP COMSEC Custodian must prepare a new *Hand Receipt* with a new IP transaction number and a reference to the previous *Hand Receipt* transaction number. The *Hand Receipt* for the renewal must include the additional information provided in Figure 1. The Loan Holder must sign the new *Hand Receipt* each time it is renewed.

5.8 Return of In-Process COMSEC Material

When the IP COMSEC material is to be returned to the IP COMSEC Account, the IP COMSEC Custodian must prepare a *Hand Receipt* for the Loan Holder. The Loan Holder must include this *Hand Receipt* with the shipment. Upon receipt of the material, the IP COMSEC Custodian will sign the *Hand Receipt* and return a copy to the Loan Holder. The *Hand Receipt* must include the additional information provided in Figure 2.

5.9 In-Process Destruction Report

The IP COMSEC Custodian must prepare a *Destruction Report* (GC-223) to report the destruction of COMSEC material from the IP accounting system. The *Destruction Report* must be signed by the IP COMSEC Custodian and the witness who performed the destruction. The remarks column of the *Destruction Report* must be annotated with the reason for destruction (e.g. breakage, waste, scrap).

NOTE: Personnel carrying out the destruction process must possess a security clearance at least equal to the highest sensitivity of the COMSEC material being destroyed, but never less than SECRET.

The above listed IP COMSEC material has not been accepted by the Government of Canada and is the property of:

_____.
(Name)

This IP COMSEC material is being issued (on a Hand Receipt) for 90 calendar days for:

_____.
(Reason for Loan)

Should the length of the loan exceed 90 calendar days, the recipient must sign a new Hand Receipt provided by:

_____.
(Name)

THIS IP COMSEC MATERIAL MUST NOT BE ENTERED INTO THE NATIONAL COMSEC MATERIAL CONTROL SYSTEM (NCMCS).

Figure 1 – In-Process Hand Receipt Required Information

The above listed IP COMSEC material has not been accepted by the Government of Canada and is the property of:

_____.
(Contractor Name)

This IP COMSEC material is being returned to the originator.

THIS IP COMSEC MATERIAL MUST **NOT** BE ENTERED INTO THE NATIONAL COMSEC MATERIAL CONTROL SYSTEM (NCMCS).

Figure 2 – Return of Issued In-Process COMSEC Material

6 Control of In-Process Cryptographic Equipment

6.1 Integrated Circuits

6.1.1 Individual Items

Individual classified or protected IP wafers, masks, masters, test samples, pattern generation tapes, etc., must be controlled on a continuous receipt system from one manufacturing process to another, and from one IP COMSEC Account to another. The accounting and control record must show the receipt or fabrication of each IP item, the description and quantity of the COMSEC material and the disposition of the item, and must bear the signatures of the responsible individuals (e.g. production supervisor, Loan Holder) for each phase of fabrication.

6.1.2 Partial Items

Less than a full wafer must be controlled as individual dies, as detailed in Article 6.1.1, unless the wafer is reconstructed on an adhesive base. In that case, accountability resumes by wafer count, and the record must show the number of dies removed. An attempt should be made to determine the number of possible full dies in a wafer before dicing the wafer.

If this cannot be accomplished, the number of full dies must be established immediately after dicing the wafer. Less than a full die must be considered classified or protected scrap and controlled accordingly.

6.1.3 Broken Items

Any area in which the breakage of an IP wafer, mask, reticule or die has occurred must be immediately safeguarded. Every effort must be made to reconstruct the broken item onto an adhesive base. If any chip or portion thereof cannot be accounted for, a *COMSEC Incident Initial Report* must be completed as detailed in ITSD-05. If a portion is missing or the entire wafer, mask, reticule or die has fragmented to such a degree that reconstruction is impossible, the IP COMSEC Custodian must:

1. remove all particles from the breakage area by vacuuming;
2. mark the vacuum bag containing the residue of the item with the wafer, mask or reticule number and its sensitivity (or, where applicable, with the identification of the chip or portion thereof belonging to the wafer, mask or reticule number);
3. ensure the vacuum cleaner bag is initialled by two properly cleared individuals; and
4. control the vacuum bag as protected or classified COMSEC material, as required, until its contents can be destroyed using a CSE-approved destruction method, or transported to CICA (in the case of a private sector IP COMSEC Account).

6.2 Controlled Cryptographic Items

6.2.1 Development

The development, manufacture or assembly of IP CCI equipment may begin with either:

- an IP design that goes through transition during development to become an IP CCI component or assembly, which the contractor further processes into IP CCI equipment; or
- a CCI component or assembly that the contractor receives from an authorized source and further processes into IP CCI equipment.

6.2.2 Protection of In-Process COMSEC Functions

Microcircuit chips used in hardware or firmware embodiments must be protectively coated by a CSE-approved process that will resist attempts to:

- recover IP design information by reverse engineering;
- defeat the security features; or
- otherwise recover information in memory (e.g. by external probing) unless, as verified by the GC sponsor through COMSEC Client Services, one of the following applies:
  - the protective coating is incompatible with the microcircuit chip, such that the reduced effectiveness inherent with the use of the coating is unacceptable, or
  - other equally protective measures have been adopted in order to resist the above mentioned threats.

NOTE 1: Unless not technically feasible to do so, hardware embodiments of IP COMSEC functions must be in custom microcircuit form (i.e. embodiments that are composed of discrete components or standard microcircuits are not permitted).

NOTE 2: Firmware embodiments of IP COMSEC functions must be in microcircuit form (custom or standard). They must employ an irreversible security feature that prevents both readout and modification, of the programmed information in the on board memory from external, physically accessible pins.

6.2.3 Transition from In-Process Design Status to In-Process Controlled Cryptographic Items – Hardware Embodiments

For hardware embodiments, the transition from IP design status to IP CCI occurs at the microcircuit photomask stage. Design automation by products leading to, and including, the reticule for each layer of the microcircuit must be handled at the same classification or protected level as the engineering drawings from which they were derived. The photomasks ultimately used as tooling in the actual production process, as well as the resulting semiconductor wafers and their subsequent forms (e.g. individual chips) leading to sealed devices, must be controlled as IP CCI material, as detailed in Article 6.2.5.

6.2.4 Transition from In-Process Design Status to In-Process Controlled Cryptographic Items – Firmware Embodiments

For firmware embodiments, the transition from IP design status to IP CCI occurs after the IP design information has been entered into the microcircuit memory, and the security feature described in Article 6.2.2 has been set. Thereafter, the microcircuits must be controlled as IP CCI material, as detailed in Article 6.2.6. Software source data for firmware embodiments of IP design information remain IP and must be safeguarded as detailed in this directive.

6.2.5 Control of In-Process Microcircuit Devices

Following the transition from IP design status to IP CCI, the microcircuit devices must be controlled throughout the remainder of the manufacturing and assembly process as follows:

- **photomasks and wafers must:**
  - be clearly marked “CONTROLLED CRYPTOGRAPHIC ITEM” or “CCI”;
  - bear a serial number and be accounted for by that serial number (until the photomasks are securely destroyed and the wafers are diced); and

- be accounted for by quantity after a wafer is diced;

- when a microcircuit is completely fabricated, purchased, accepted and transferred to the government, accountability must be in accordance with NCMCS accounting procedures;
- when a microcircuit is completely fabricated, purchased, accepted and shipped to another private sector company for use in a manufacturing process, accountability must be in accordance with the IP accounting procedures; and
- when the microcircuit is stored for future sale or stored for contractual obligations or is moved to the next level of assembly, the microcircuit must be maintained in the contractor's IP accounting system.

6.2.6 Control of Printed Wiring Assemblies

The Printed Wiring Assemblies (PWAs) assume IP CCI status as soon as a CCI microcircuit is installed upon it. Following this transition, the PWA must be controlled throughout the remainder of the manufacturing and assembly process as follows:

- at the point of transition, accountability for the microcircuit ceases, and accountability for the PWA begins;

  NOTE: This disposition of the microcircuit, and the subsequent accountability for the PWA, must be reflected in the IP accounting records.

- completely fabricated PWAs are accountable by quantity when they fit the definition of "CCI component" and by serial number when they fit the definition of "CCI assembly";
- during further assembly, PWAs must be accounted for by quantity;
- when a PWA is completely fabricated, purchased, accepted and transferred to the government, accountability must be in accordance with NCMCS accounting procedures;
- when a PWA is completely fabricated, purchased and shipped to another private sector company for use in a manufacturing process, accountability must be in accordance with the IP accounting procedures; and
- when the PWA is stored for future sale or stored for contractual obligations or it is moved to the next level of assembly, it must be maintained in the contractor's IP accounting system.

6.2.7 Labelling Controlled Cryptographic Item Components, Assemblies and Equipment

CCI components, assemblies and equipment must be labelled, "CONTROLLED CRYPTOGRAPHIC ITEM" or "CCI" depending on the labelling space available, in accordance with standard drawings available from COMSEC Client Services and with the information provided in Table 4.

Table 4 – Labelling CCI

CCI	Labelling and Control Requirements
Components	• Each CCI component (CCI microcircuit device) must be labelled "CCI" at the same time as other part-specific nomenclature is applied.
Assemblies	• Each CCI assembly (printed wiring assembly) must bear a government serial number for accounting purposes, in accordance with criteria which will be provided by COMSEC Client Services. • Labelling may be applied at any stage of the assembly process before the end of the assembly process. • CCI status is assigned to CCI assemblies as soon as the CCI component (CCI microcircuit) is installed on it (refer to Article 6.2.6).

CCI	Labelling and Control Requirements
Equipment	• Each item of CCI equipment must be labelled "CONTROLLED CRYPTOGRAPHIC ITEM" in a conspicuous, external location. • Each item of CCI equipment must also bear a government serial number for accounting purposes, in accordance with criteria provided by COMSEC Client Services. • Labelling may be applied at any stage of the assembly process before the end of the assembly process. • CCI status is assigned to equipment as soon as the CCI component (CCI microcircuit) or CCI assembly (printed wiring assembly) is installed.

6.3 Breakage, Waste and Scrap In-Process COMSEC Material

IP COMSEC material leaving the development, production, manufacturing or assembly process due to failure, breakage or normal waste (e.g. broken wafer, partial die, broken or faulty PWAs or microcircuit devices) must be controlled until its approved destruction can be performed. When authorized methods of destruction are not available, contact COMSEC Client Services or CICA for disposal guidance.

6.4 Loss of In-Process COMSEC Material

An extensive search must be made for any lost IP COMSEC material. Loss of such material must be documented in the IP COMSEC Account records and immediately reported as a **COMSEC incident** as detailed in ITSD-05.

7 Cryptographic Equipment under Repair and Maintenance Contract

7.1 Transfer to/from the Contractor

The COMSEC Custodian for the GC department must transfer cryptographic equipment requiring R&M to the contractors COMSEC Sub-Account through CICA, unless a direct transfer has been pre-approved by CICA. The COMSEC Sub-Account Custodian will transfer the cryptographic equipment to the IP COMSEC Account and annotate the *Hand Receipt* (GC-223) appropriately. When the item is ready to be returned to the GC department, the process will be reversed.

7.2 Accountability within the Repair and Maintenance In-Process Facility

Special attention must be given to ensure that the IP accounting procedures record the removal, insertion, disposal, destruction (if authorized) and conversion (if required) of all COMSEC parts, components and assemblies used in the R&M process as well as the continuous accountability of the cryptographic equipment being serviced by the contractor or maintenance depot.

7.3 Source of Spare COMSEC Parts, Components and Assemblies

7.3.1 In-House Sources

If the R&M contractor is the same contractor who built the cryptographic equipment, the required COMSEC parts, components and assemblies require an in-house *Transfer Report* (GC-223) from the manufacturing IP accounting system to the R&M IP accounting system.

7.3.2 Government Sources

The COMSEC Custodian must transfer the COMSEC parts, components and assemblies to CICA who will, in turn, issue the material as Government Furnished Equipment (GFE) to a private sector COMSEC Sub-Account.

7.3.3 Sub-Contracting

COMSEC parts, components and assemblies that originate from another contractor, whether by purchase or by contractual agreement, should be transferred from the manufacturer's IP accounting system to the R&M contractor's IP accounting system using an *IP Transfer Report*.

7.4 Non-Serviceable In-Process Parts, Components and Assemblies

Any COMSEC part, component or assembly removed from a GC cryptographic equipment and replaced with IP COMSEC material (part, component or assembly) automatically becomes non-serviceable IP COMSEC material for disposal. Unless otherwise authorized by COMSEC Client Services, these non-serviceable items must be transferred to CSE through COMSEC channels, for disposition. The IP disposition records must show the disposition, and if required, replacement of non-serviceable COMSEC parts, components and assemblies. IP disposition must be detailed in the IP Plan.

7.5 Non-Repairable Cryptographic Equipment

Non-repairable cryptographic equipment under an R&M contract must be returned to the GC department through CICA for disposal. The R&M contractor may only dispose of a GC department's cryptographic equipment by returning it to that GC department. The GC department is responsible for the disposition of its cryptographic equipment as detailed in the ITSD-03A.

8 Development of Accountable COMSEC Publications

GC departments may have a requirement to develop COMSEC publications that will be accounted for, controlled and managed in NCMCS. GC departments preparing to develop accountable COMSEC publications must contact COMSEC Client Services for approval and direction.

9 Reproduction or Translation of Accountable COMSEC Publications

GC departments may have a requirement to reproduce or translate COMSEC publications that are accounted for, controlled and managed in NCMCS. GC departments reproducing or translating accountable COMSEC publications must contact COMSEC Client Services for approval and direction.

10 References

10.1 Abbreviations and Acronyms

ACM	Accountable COMSEC Material
ACMCA	Accountable COMSEC Material Control Agreement
ALC	Accounting Legend Code
CCI	Controlled Cryptographic Item
CDRL	Contract Data Requirements List
CEO	Chief Executive Officer
CEPA	COMSEC Equipment Purchase Authorization
CER	COMSEC Equipment Requirements
CGP	Controlled Goods Program
CICA	CSE Industrial COMSEC Account
CMAC	Crypto Material Assistance Centre
COMSEC	Communications Security
COR	Central Office of Record
Cryptonet	Cryptographic Network
CSI	COMSEC Safeguarding Inspection
CSE	Communications Security Establishment
CSO	Company Security Officer
CUP	COMSEC User Portal
DAO	Department, Agency, Organization
DCA	Departmental COMSEC Authority
DCITS	Deputy Chief, Information Technology Security
DDSM	*Directive on Departmental Security Management*
DID	Data Item Description
DSC	Document Safeguarding Capability
DSO	Departmental Security Officer
FAA	*Financial Administration Act*
FOCI	Foreign Ownership, Control or Influence
FSC	Facility Security Clearance
FSU	Field Software Upgrade
GC	Government of Canada
GFE	Government Furnished Equipment
IP	In-Process
ISM	*Industrial Security Manual*
ISP	Industrial Security Program
IT	Information Technology
ITAR	*International Traffic In Arms Regulations*
ITSD	Information Technology Security Directive
KMSP	Key Material Support Plan
KSO	Key Senior Official
LOA	Letter of Agreement
MOA	Memorandum of Agreement

MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCIO	National COMSEC Incidents Office
NCMCS	National COMSEC Material Control System
NCOR	National Central Office of Record
NLZ	No-Lone Zone
PGS	*Policy on Government Security*
PMO	Project Management Office
PSPC	Public Services and Procurement Canada
PWA	Printed Wiring Assembly
R&M	Repair and Maintenance
RFP	Request for Proposal
SRCL	Security Requirements Check List
TAA	Technical Assistance Agreement
TPI	Two-Person Integrity
U.S.	United States
USML	United States Munitions List

11 Glossary

This glossary contains terms and definitions related to the COMSEC material identified within this directive.

UNCLASSIFIED	
Access	The capability and opportunity to gain knowledge or possession of, or to alter, information or material.
Accountability	The responsibility of an individual for the safeguard and control of COMSEC material which has been entrusted to his or her custody.
Accounting Legend Code (ALC)	A numeric code used to indicate the minimum accounting controls for COMSEC material within NCMCS.
Audit	The process of conducting an independent review and examination of system records and activities in order to test the adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any changes in controls, policy, or procedures.
Communications Security (COMSEC)	The application of cryptographic, transmission, emission and physical security measures, and operational practices and controls, to deny unauthorized access to information derived from telecommunications and to ensure the authenticity of such telecommunications.
Company Security Officer (CSO)	The private sector company's official point of contact with the ISP responsible for monitoring the private sector company's security profile, addressing security issues, and accountable to the ISP and to the private sector company's designated KSO on all industrial security matters.

UNCLASSIFIED	
COMSEC Client Services	An entity within CSE responsible to provide advice, guidance and direction to the Government of Canada and sponsored Canadian private sector, for the planning, acquisition and operation of high assurance products, COMSEC material and services.
COMSEC Incident	Any occurrence that jeopardizes or potentially jeopardizes the security of classified or protected Government of Canada information while it is being stored, processed, transmitted or received.
COMSEC Material	An item designed to secure or authenticate telecommunications information. COMSEC material includes, but is not limited to, cryptographic key, equipment, modules, devices, documents, hardware, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.
Controlled Cryptographic Item (CCI)	An unclassified secure telecommunications or information system, or associated cryptographic component, that is governed by a special set of control requirements within NCMCS and marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI".
Crypto Material Assistance Centre (CMAC)	The entity within CSE 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.
CSE Industrial COMSEC Account (CICA)	The entity at CSE responsible for developing, implementing, maintaining, coordinating and monitoring a private sector communications security program that is consistent with the *Policy on Government Security* and its related policy instruments for the management of accountable COMSEC material.
Departmental COMSEC Authority (DCA)	The individual designated by, and responsible to, the departmental security officer for developing, implementing, maintaining, coordinating and monitoring a departmental communications security 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.
Firmware	Programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
Foreign Ownership, Control or Influence (FOCI)	A situation whereby a third party individual, firm or government is assumed to possess dominance of, or authority over, a Canadian facility to such a degree that a third party individual, firm or government could gain unauthorized access to information technology security information. An administrative determination of the nature and extent of foreign dominance over the contractor's management and/or operations is required. Foreign Ownership, Control or Influence may also be referred to as Foreign Ownership or Dominance.

UNCLASSIFIED	
Government of Canada (GC) Department	Any federal department, organization, agency or institution subject to the *Policy on Government Security*.
Government of Canada (GC) Sponsor	A Government of Canada department that has agreed to sponsor a private sector company to have access to or receive (for use), manufacture, reproduce or repair accountable COMSEC material.
Hand Receipt	An accounting document (GC-223) that records the issue of and acceptance of responsibility for COMSEC material.
Information Technology Security (IT Security)	Safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.
In-Process (IP) COMSEC Material	COMSEC material being developed, produced, manufactured or repaired. See COMSEC Material.
Loan Holder	An individual registered at a COMSEC Account or COMSEC Sub-Account who is authorized to receive COMSEC material from that account.
National Central Office of Record (NCOR)	The entity at CSE responsible for overseeing the management and accounting of all accountable COMSEC material, produced in, or entrusted to, Canada.
National COMSEC Audit Team (NCAT)	The entity at CSE responsible for conducting COMSEC audits of the COMSEC Accounts within NCMCS.
National COMSEC Incidents Office (NCIO)	The entity at CSE responsible for managing communications security incidents through registration, investigation, assessment, evaluation and closure.
National COMSEC Material Control System (NCMCS)	A centralized system, which includes personnel, training and procedures, that enables Government of Canada departments to effectively control and handle accountable COMSEC material.
No-Lone Zone (NLZ)	An area, room, or space to which no one person is permitted to have unaccompanied access, and that when occupied must have two or more appropriately cleared individuals within, who must remain within sight of each other.
Photomask	A film or glass negative that has many high-resolution images, used in the production of semiconductor devices and integrated circuits.
Physical Security	The use of physical safeguards to prevent and delay unauthorized access to assets, to detect attempted and actual unauthorized access and to activate appropriate response.
Private Sector	Canadian organizations, companies or individuals that do not fall under the *Financial Administration Act* or is not subordinate to a provincial or municipal government.

UNCLASSIFIED	
Reticule	A disk, or the like, with a pattern of opaque and transparent portions which can be rotated in the path of a beam of light or other radiation so as to modulate it.
Tier 3 Management Device (T3MD)	Cryptographic equipment that securely stores, transports and transfers (electronically) cryptographic key and that is programmable to support modern mission systems.
Two-Person Integrity (TPI)	A control procedure whereby TOP SECRET key and other specified key must not be handled by or made available to one individual only.
Wafer	A thin slice of semiconductor material, such as a silicon crystal, used in the fabrication of integrated circuits and other microdevices.

12 Bibliography

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

- **Communications Security Establishment:**
  - *Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material* (ITSD-05), April 2012.
  - *Directive for the Use of CSEC-Approved COMSEC Equipment and Key on a Telecommunications Network* (ITSD-04), November 2011.
  - *IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector* (ITSD-06A), 2016.
  - *IT Security Directive for the Control of COMSEC Material in the Government of Canada* (ITSD-03A), March 2014.
- **Department of Justice:**
  - *Financial Administration Act* (FAA), 1985.
- **Public Works and Government Services Canada:**
  - *Industrial Security Manual* (ISM), October 2014.
- **Treasury Board of Canada Secretariat:**
  - *Directive on Departmental Security Management* (DDSM), July 2009.
  - *Policy on Government Security* (PGS), July 2009.