Communications Security Establishment
Centre de la sécurité des télécommunications

IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector

ITSD-06A

Canada

Foreword

The *IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector* (ITSD-06A) 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*.

This publication supersedes the *Directive for the Control of COMSEC Material in the Canadian Private Sector* (ITSD-06), June 2013, and all previously distributed versions, which must be destroyed in accordance with departmental procedures for disposal of unclassified information.

General inquiries and suggestions for amendments are to be forwarded through departmental communications security channels to COMSEC Client Services (refer to Article 1.12).

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

Effective Date

This directive takes effect on date of signature.

Original signed on **June 15, 2016**
by Joseph Waddington, Director-General, Cyber Protection
on behalf of the Deputy Chief, IT Security

Reproduction and Distribution

Summary of Changes from ITSD-06 to ITSD-06A

Reference	Change
Previous Annex B	The In-Process Annex in ITSD-06 has been removed and integrated into a new and separate directive (i.e. ITSD-08).
Previous Annex D	Instructions for filling out the *COMSEC Material Report* (GC-223) have been removed and are now available at https://www.cse-cst.gc.ca/en/group-groupe/high-assurance-technologies.
Previous Annex E	Completing the new *COMSEC Material Control Register* is self-explanatory and the previous instructions for filling out the form have been removed and the form is now found at https://www.cse-cst.gc.ca/en/group-groupe/high-assurance-technologies.
Previous Annex F	Examples of common COMSEC incidents have been removed and added as Article 16.8.
Previous Annex G	Template for *COMSEC Incident Initial Report* has been removed and is now found at https://www.cse-cst.gc.ca/en/group-groupe/high-assurance-technologies.
Article 1.10	The *Requests for Exceptions and Waivers* section has been amended to add a requirement for annual review.
Article 1.12	Updated to include secure telephone and fax numbers.
Articles 2.3 and 2.3.1	Amended to show that the ISP has overall responsibility previously delegated to CISD and IISD. While CISD specific responsibility is detailed throughout this document, all references to IISD (Article 2.3.2) have been removed.
Articles 5.1 and 5.5	Updated to provide establishment and closure criteria for CICA COMSEC Sub-Account, including baseline security clearance requirements.
Article 5.1.1	Reworded to note that COMSEC Client Services is responsible to "confirm CGP registration" versus "CGP and ITAR compliance".
Article 5.2.3	Amended to include manual sub-systems and system back-up requirements.
Article 5.2.7	Amended to remove "reliability status" as criteria for access to ACM.
Article 5.3.2	Amended to remove the requirement for submission to CICA and to provide clarity on how to use the *COMSEC Signing Authority* form.
Article 6.2.5	Amended to add clarity to definitions of ALCs 1-7.
Article 7.3.1	Amended to define the difference between local accounting of ACM within NCMCS and local tracking of non-accountable COMSEC material outside of NCMCS.
Article 7.9	Additional responsibility has been added to tracer notices.

Reference	Change
Article 8.2.3	Amended to provide a requirement for COMSEC Briefing updates (every five years) for active COMSEC personnel.
Article 8.5	Amended to note that CICA representatives (e.g. auditors) do NOT require a visit clearance request. However, CICA visits must be coordinated between CICA and the COMSEC Sub-Account.
Article 9	Amended to provide additional clarity and mandatory criteria for establishing and protecting COMSEC facilities.
Article 9.3.4	Added new article “Incidents Involving Unattended Security Containers”.
Article 10.5	Added new article “Distributing Electronic Key on Magnetic or Optical Removable Storage Media”.
Article 11.1.2	Added new article on key states: RED (encrypted) and BLACK (unencrypted).
Article 11.1.5	Added new article on copying key.
Article 11.4.5	Added **NOTE** with a requirement to confirm completion of mandatory software upgrades.
Article 12.1	Amended to provide baseline security requirements for personnel handling the destruction of COMSEC material.
Article 13.2.1	Changed “Annual” inventory to “Periodic” inventory.
Article 14	Updated article on COMSEC Emergency Protection Planning.

NOTE: It is the responsibility of the user to apply all the security requirements identified in this ITSD.

Table of Contents

List of Tables

List of Figures

1 Introduction

The Government of Canada (GC) has established a program known as Communications Security (COMSEC) to assist in the protection of classified and PROTECTED C information. The COMSEC program involves the application of cryptographic security, transmission and emission security, physical security measures, and operational practices and controls. The objective of COMSEC is to deny unauthorized access to information and data derived from telecommunications and to ensure the authenticity of such telecommunications.

For the purpose of this directive, the term "GC department" includes any federal institution (e.g. Department, Agency or Organization) and enterprise services organizations subject to the *Policy on Government Security* (PGS) and to Schedules I, I.1, II, IV and V of the *Financial Administration Act* (FAA), unless excluded by specific acts, regulations or Orders in Council.

"COMSEC material" is designed to secure or authenticate telecommunications information. COMSEC material includes cryptographic key, devices, hardware, firmware or software that embodies or describes cryptographic logic. It also includes the documents that describe and support these items.

Applying this directive will help ensure that GC security controls are met when access to GC COMSEC material is provided to a Canadian private sector company.

1.1 Purpose

This directive provides COMSEC practitioners with the minimum security requirements for the control and management of COMSEC material authorized by the Communications Security Establishment (CSE) for use by a Canadian private sector company, (hereinafter referred to as "private sector company"), within Canada.

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 accountable COMSEC material within a COMSEC Account.

NOTE 1: For direction on the establishment of a private sector COMSEC Sub-Account outside of Canada, contact COMSEC Client Services.

NOTE 2: For the purpose of this directive, the term "private sector company" includes Canadian organizations, companies or individuals that do not fall under the FAA or are not subordinate to a provincial or municipal government.

1.2 Authority

This directive is promulgated pursuant to the PGS that delegates 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, at CSE is the promulgation authority for COMSEC policy instruments.

1.3 Scope

The methods for the control of COMSEC material vary and are determined by the nature of the material itself.

The scope of this directive includes:

- COMSEC material, which requires control and accountability within the National COMSEC Material Control System (NCMCS) or local tracking by a COMSEC Sub-Account Custodian through a CSE-approved manual or electronic tracking system outside of NCMCS; and
- COMSEC material requiring special handling stated in the United States (U.S.) *International Traffic in Arms Regulations* (ITAR) and the Canadian *Controlled Goods Regulations* (CGR) as managed within the Canadian Controlled Goods Program (CGP).

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 Application of Communications Security using CSE-Approved Solutions* (ITSD-01A), January 2014*;*
- *IT Security Directive for the Control of COMSEC Material in the Government of Canada* (ITSD-03A), March 2014;
- *IT Security Directive for the Control and Management of In-Process COMSEC Material* (ITSD-08), in development in 2016;
- *Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material* (ITSD-05), April 2012; and
- *Industrial Security Manual* (ISM).

1.5 Application

This directive applies to private sector companies that are authorized to handle, control and safeguard CSE-approved COMSEC material under sponsorship (i.e. a GC contract procured through Public Services and Procurement Canada [PSPC] or other CSE-approved agreement).

1.6 Expected Results

Application of this directive will help ensure the protection of GC classified and protected information and data. It will also ensure Canada's commitments to safeguard and control COMSEC material are aligned with the agreements and security requirements of its international partners.

1.7 Compliance

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

A sponsored private sector company must agree, through an Accountable COMSEC Material Control Agreement (ACMCA), to implement the controls and management requirements detailed in this directive as well as other controls and management requirements deemed necessary by CSE before it will be permitted to open a COMSEC Sub-Account.

1.8 Consequence of Non-Compliance

Failure to comply with this directive may result in escalated administrative controls being placed on a private sector company's COMSEC Sub-Account. As a final recourse after repeated non-compliance, a private sector company's COMSEC Sub-Account will be suspended or closed until an external audit is conducted by CICA, and the COMSEC shortcomings are rectified.

1.9 Conflict Resolution

This directive is intended to provide a comprehensive summary of the obligation related to control and handling of CSE–approved COMSEC material within the private sector. It should be read in conjunction with Public Services and Procurement Canada's *Industrial Security Manual* (ISM).

Any conflict between a requirement contained in this ITSD and any other national (e.g. PGS, DDSM, ISM and *Management of Information Technology Security* [MITS]) or international (e.g. ITAR) requirement must be submitted to COMSEC Client Services for resolution.

When a conflicting COMSEC directive (e.g. IT Security Directive [ITSD] series) is encountered, this directive will take precedence.

1.10 Request for Exception or Waiver

A request for an exception (substitution) or a waiver (temporary exemption from a specific requirement) must be submitted to COMSEC Client Services at CSE (hereinafter referred to as COMSEC Client Services) via CICA by the Company Security Officer (CSO). Requests must be submitted in writing, and with a justification. COMSEC Client Services will coordinate all exception or waiver requests with sponsoring organization(s) as appropriate.

NOTE: Exceptions and waivers are reviewed periodically by COMSEC Client Services.

1.11 Additional Regulations Affecting Acquisition of COMSEC Material

1.11.1 Foreign Ownership, Control or Influence

A private sector company will normally require a PSPC Industrial Security Program (ISP) Foreign Ownership, Control or Influence (FOCI) assessment before being provided access to Accountable COMSEC Material (ACM) 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 a private sector company's ownership and control arrangements that could allow unauthorized access to ACM.

A private sector company will be considered under FOCI when a reasonable basis exists, as determined by a PSPC 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 ACM by foreign parties or their agents.

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

1.11.2 Canadian Controlled Goods Program

The Canadian CGP is a domestic industrial security program within PSPC that is mandated under the CGR 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 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.

1.11.3 United States international Traffic in Arms Regulations

ITAR is a set of 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 ACM 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 ACM, contact COMSEC Client Services.

1.12 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 are attended from 8 a.m. to 4 p.m. Eastern Time, Monday to Friday.

Table 1 – Contact Information for COMSEC Offices

Office	Telephone Number	E-mail Address
CICA	Telephone: 613-991-7272 Secure Telephone: 613-991-7597 Secure Fax: 613-991-7593	cica-ccic@cse-cst.gc.ca
COMSEC Client Services	Telephone: 613-991-8495	comsecclientservices@cse-cst.gc.ca

1.13 Communications Security Establishment Website

COMSEC directives, forms, 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.

2 Roles and Responsibilities

2.1 General

This Article provides the major roles and responsibilities of CSE, GC departmental sponsors and private sector companies as they relate to COMSEC management in the private sector. It will also outline the security functions provided by the ISP of PSPC in the context of a GC contract.

NOTE: Annex D provides a quick reference guide for the roles and responsibilities identified in this directive.

2.2 Communications Security Establishment

CSE is Canada's national COMSEC authority. As such, CSE is responsible for approving the certification, acquisition and use of cryptographic equipment and key, as well as COMSEC-related policy instruments that protect classified and PROTECTED C information and data.

2.2.1 COMSEC Client Services

Under the direction of the Deputy Chief, Information Technology Security (DCITS), COMSEC Client Services is responsible to provide advice, guidance and direction to the GC and 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 Article 8.1.3);
- authorizing the establishment or closure of a COMSEC Sub-Account;
- validating private sector requirements to hold CSE-approved COMSEC solutions and material;
- confirming all security prerequisites and inspections are met by a private sector company prior to authorizing the release of ACM to its COMSEC Sub-Account, including:
  - *Facility Security Clearance* (FSC) or its equivalent;
  - *Document Safeguarding Capability* (DSC) inspection or its equivalent;
  - *COMSEC Safeguarding Inspection* (CSI);
  - production inspection (for In-Process [IP] requirements – refer to ITSD-08); and
  - FOCI assessment (refer to Article 1.11.1) or its exemption;
- coordinating the signing of ACMCAs, TAAs, Non-Disclosure Agreements and other agreements as required;
- validating Key Material Support Plans (KMSPs) (refer to the *Directive for the use of CSE-Approved COMSEC Equipment and Key on a Telecommunications Network* [ITSD-04]), as required;
- coordinating the provision of TEMPEST inspections; and
- coordinating cross-border shipments of ACM with other national security authorities.

2.2.2 CSE Industrial COMSEC Account Departmental COMSEC Authority

Under the direction of DCITS, the CICA Departmental COMSEC Authority (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.

2.2.3 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 COMSEC Sub-Accounts. CICA's responsibilities include:

- being the initial point of contact for issues pertaining to the management of COMSEC Sub-Accounts and IP COMSEC Accounts (including reporting of COMSEC incidents);
- opening and closing of private sector company COMSEC Sub-Accounts once approved by COMSEC Client Services;
- ensuring adherence to ACM management rules and providing support and guidance on the use of CSE-approved cryptographic equipment and key;

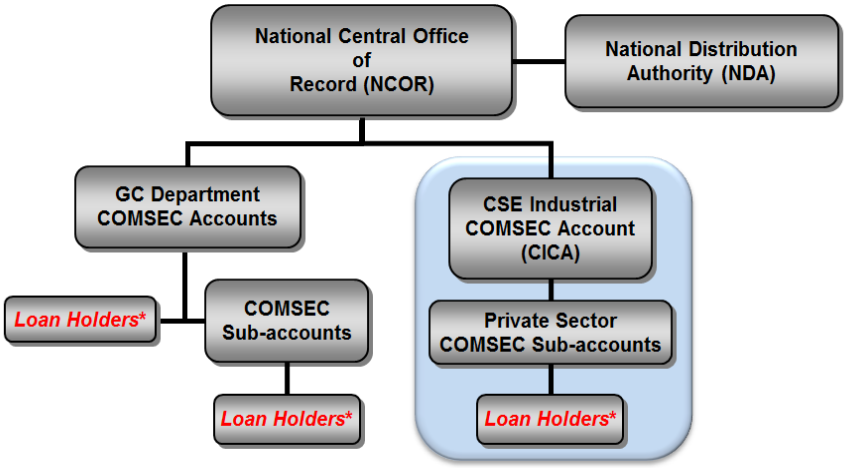
  NOTE: Throughout the remainder of this document (except in the glossary), the term "cryptographic key" will be referred to as "key". The term "key" will include all forms of physical or electronic key. The term "key" will also be used to refer to both singular and multiple quantities of key.

- performing annual inventory reconciliations with COMSEC Sub-Accounts;
- completing private sector COMSEC Sub-Account audits (refer to Article 15); and
- authorizing and coordinating the movement and distribution of ACM within Canada (providing courier certificates as required).

2.2.4 National COMSEC Material Control System

NCMCS is the CSE-approved national ACM logistics system that includes the personnel and procedures that enables GC departments and private sector companies to effectively handle and control ACM. NCMCS provides for the control of ACM through:

- National Central Office of Record (NCOR)
- National Distribution Authority (NDA)
- COMSEC Accounts
- COMSEC Sub-Accounts, and
- Loan Holders.



*New Terminology: Previously called Local Elements or Hand Receipt Holders.

Figure 1 – National COMSEC Material Controls System (as it relates to private sector companies)

2.2.5 National Central Office of Record

The NCOR is the entity at CSE responsible for overseeing the management and accounting of ACM produced in, or entrusted to, Canada. NCOR has three distinct roles: Registration Authority, COMSEC Account Manager and Key Processor (KP) Privilege Certificate Manager. These roles are administered by the Crypto Material Assistance Centre (CMAC).

2.2.6 National Distribution Authority

The NDA is the entity at CSE responsible for the receipt and distribution of ACM within and outside Canada.

2.3 Public Services and Procurement Canada – COMSEC Security Services in Contracting

The Industrial Security Sector (ISS) of PSPC ensures the application of security safeguards through all phases of contracting with private sector companies within the scope of the ISP as per the PGS. The ISP enables the Canadian private sector to compete for domestic and international government contracts, protects public safety by safeguarding sensitive and controlled assets, and provides contract security services.

2.3.1 Industrial Security Program

For Canadian private sector companies that have a PSPC contract or sub-contract (national or international) and that have a requirement to access protected or classified government information or assets, the ISP provides the following services:

- personnel security screening services;
- site DSC, physical, production and IT security inspections;
- specific security-oriented terms and conditions to be written into contracts;

- completion of FSCs;
- FOCI assessments (refer to Article 1.11.1);
- screening of private sector companies and personnel for North Atlantic Treaty Organization (NATO) foreign contracting security requirements;
- transfer of non-COMSEC classified and protected information and assets between Canadian and foreign governments and the private sector through government-to-government channels;
- development of international Project Security Instructions (PSIs), including those that cover COMSEC requirements; and
- visit requests to ensure that visit security requirements are met (refer to Article 8.6 for COMSEC access requirements) for visits to government or private sector companies in Canada or abroad.

2.4 Communications Security Establishment – COMSEC Security Services without a Public Services and Procurement Canada–managed Contract

Where there is no PSPC-managed contract and a private sector company requires access to ACM (typically originated from a foreign nation), the security services, except for the FOCI and sponsorship requirements (refer to NOTE below), will be the same as detailed throughout this directive.

COMSEC Client Services will ensure that the Canadian private sector company has established a CICA COMSEC Sub-Account complete with FSC, DSC and CSI equivalent capability.

It is the responsibility of the foreign industrial partner to approach their own Department of State (DoS) authorities and request release of the ACM to a Canadian private sector company. Once COMSEC Client Services has received proof that the foreign DoS authority has received the request, COMSEC Client Services will coordinate the ACM release with both the foreign COMSEC and DoS authorities. Such a release must be in the form of an official written approval for release of the ACM to the Canadian private sector company.

The actual cross-border movement (export or import) of all ACM must be conducted through the Canadian NDA at CSE and the material will be handled within Canada under national COMSEC channels (e.g. NCMCS). Before the release of material, COMSEC Client Services will ensure that the Canadian private sector company has established a CICA COMSEC Sub-Account meeting FSC, DSC and CSI requirements.

NOTE: The official written release statement from the foreign COMSEC and DoS authorities will indicate that they are accepting the release without a Canadian FOCI assessment. Once release is established, COMSEC Client Services will exempt the Canadian GC sponsorship requirement as detailed in Article 2.5.

2.5 Government of Canada Departmental Sponsor – Private Sector Company

Prior to any ACM being provided, a private sector company must be sponsored by a GC department (hereinafter referred to as GC sponsor) that has a current COMSEC Account. The GC sponsor's DCA is responsible for:

- notifying COMSEC Client Services that a private sector company will require access to ACM;

  NOTE: This must be done as early as possible in the contracting and requirement process to ensure COMSEC management requirements are established to meet deadlines.

- signing the ACMCA as the sponsoring department;
- confirming that a private sector company is registered with the CGP before releasing ACM;
- ensuring COMSEC Client Services is in receipt of the approved contract Security Requirements Check List (SRCL), including amendments if applicable;
- providing FSC, DSC and IT equivalent inspections and FOCI assessments (as required by CSE) for a sponsored private sector company that does not hold a GC contract;
- providing additional supporting documentation (as required by CSE) for a sponsored private sector company that does not hold a GC contract;
- 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 a Controlling Authority (ConAuth) for authorized Cryptographic Networks (cryptonets), if required – refer to ITSD-04;
- coordinating the release of ACM to a private sector company with CICA once all prerequisites for the establishment of a COMSEC Sub-Account have been met (refer to Article 5.1); and
- coordinating the end-of-contract withdrawal of all ACM from the private sector company with CICA.

2.6 Private Sector Company

2.6.1 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 CSO. If the private sector company is seeking registration in the ISP, the procedures detailed in the ISM should be followed.

2.6.2 Company Security Officer

The CSO is responsible to the CEO for the overall company COMSEC security posture. CSO's COMSEC control and management responsibilities as they relate to ACM include:

- coordinating the signing of ACMCAs by a senior company official;
- ensuring the management of ACM assets as detailed in this directive, and as directed by CICA;
- ensuring ITAR (refer to Article 1.11.3), FOCI (refer to Article 1.11.1), and the Canadian CGP (refer to Article 1.11.2) requirements are met;
- appointing the company COMSEC Sub-Account Custodian and COMSEC Sub-Account Alternate Custodian, hereinafter referred to as the Alternate Custodian;
- ensuring a member of the COMSEC staff (Sub-Account Custodian or an Alternate Custodian) is available at all times to support its Sub-Account requirements;
- ensuring the COMSEC Sub-Account Custodian staff receive formal CSE COMSEC management training;
- ensuring COMSEC management requirements are reflected in company security orders;

- ensuring that there is an FSC or equivalent to the appropriate level and that IT, DSC, production inspections or their equivalent are completed prior to accepting ACM;
- ensuring COMSEC Briefings are provided to personnel requiring access to ACM;
- processing the requirement for COMSEC visits (i.e. visits that involve access to ACM) where there is a contract as detailed in the ISM and this directive. Visitor clearance requests must be submitted through the ISP. The ISP will then request COMSEC access authority through COMSEC Client Services;
- ensuring visit authorization is received from the ISP prior to permitting visitors access to ACM;
- developing a *COMSEC Emergency Plan* (refer to Article 14);
- reporting COMSEC incidents to CICA (refer to Article 16 and ITSD-05); and
- ensuring subcontractors meet the security requirements of the ISP or its equivalent and this directive prior to being provided access to ACM.

2.6.3 Separation of Duties

The CEO or CSO must not hold the position of company COMSEC Sub-Account Custodian or Alternate Custodian.

With the exception of an IP COMSEC Account, COMSEC Sub-Account Custodian or Alternate Custodian must not be assigned to concurrently manage more than one COMSEC Sub-Account.

2.6.4 COMSEC Sub-Account Custodian

The COMSEC Sub-Account Custodian is responsible for the receipt, custody, distribution, disposition, destruction and accounting of ACM entrusted to their COMSEC Sub-Account as detailed in this directive and as directed by CICA. Refer to Annex A for a detailed list of the COMSEC Sub-Account Custodian's duties.

2.6.5 COMSEC Sub-Account Alternate Custodian

An Alternate Custodian assists the COMSEC Sub-Account Custodian in the day-to-day activities of a COMSEC Sub-Account and performs the duties of the COMSEC Sub-Account Custodian during his or her temporary absence. Refer to Annex A for a detailed list of the Alternate Custodian's duties.

2.6.6 Loan Holder

A Loan Holder is an individual who is authorized to hold, store and use ACM. A Loan Holder is authorized to exchange ACM only with the COMSEC Sub-Account at which the Loan Holder is registered. A Loan Holder cannot be registered at more than one Sub-Account at a time. A Loan Holder is not authorized to re-loan ACM. Refer to Annex A for a detailed list of a Loan Holder's duties.

2.6.7 Shift Worker and Technical Staff

In certain instances, an individual such as a shift worker or technician (hereinafter referred to as an authorized user) may require short term (immediate) access to ACM (this is not considered a loan). Before allowing this access, the Sub-Account Custodian must ensure the intended authorized user meets the requirements of Article 8.1 and:

- is a company employee;

- has read and signed a *Loan Holder Responsibilities* form;
- signs for and maintains constant personal control of the ACM until it is returned;
- returns ACM for lock-up when not in use;
- does not transport the ACM to another work area or building without consent from the Sub-Account Custodian or Loan Holder; and
- understands what constitutes a COMSEC incident or potential COMSEC incident (refer to ITSD-05).

2.6.8 Witnessing Personnel

A company employee, other than the custodial staff, may be appointed as a witness to account transactions (e.g. for *Possession, Inventory* and *Destruction Reports*). A witness must have the prerequisites for access to ACM and a security status at least equal to the highest classification level of the ACM transaction being witnessed.

NOTE: Under no circumstances is a person permitted to sign as a witness without sighting the ACM that is identified on the form.

3 Selection of COMSEC Personnel

3.1 Selection of COMSEC Sub-Account Custodial Personnel

The CSO must carefully screen individuals who have been selected to become a COMSEC Sub-Account Custodian or Alternate Custodian to ensure that each proposed individual:

- is a Canadian citizen (including dual nationality);
- is a company employee;
- possesses a security clearance at least equal to the highest sensitivity of the ACM held in the COMSEC Sub-Account, but never less than SECRET;
- possesses a current COMSEC Briefing (refer to Article 8.2);
- is a responsible individual who is qualified to assume the duties and responsibilities of a COMSEC Sub-Account Custodian or Alternate Custodian;
- is in a position or at a 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 or Alternate Custodian duties for reasons of negligence or non-performance of duties; and
- has not been assigned duties that would interfere or conflict with the duties of the company COMSEC Sub-Account Custodian or Alternate Custodian.

3.2 Loan Holder

The COMSEC Sub-Account Custodian must ensure that Loan Holders are established for operational purposes that require access to or use ACM. In addition to the criteria in Article 2.6.6 and Annex A.3 must:

- be a Canadian citizen (including dual nationality);

- unless authorized by COMSEC Client Services, be an employee of the company to which the COMSEC Sub-Account is registered;
- not have previously been relieved of Loan Holder duties for reasons of negligence or non-performance of duties;
- possess a security clearance at least equal to the highest sensitivity of the ACM held; and
- be in a position or at a level of authority which would permit the individual to exercise proper jurisdiction in fulfilling the responsibilities of the position.

4 Training

4.1 General

COMSEC Sub-Account Custodians and Alternate Custodians require formal training. Prior to being appointed to the role of COMSEC Sub-Account Custodian or Alternate Custodian, or at least before administering COMSEC Sub-Account duties, individuals must complete CSE COMSEC Custodian training. Former COMSEC Sub-Account Custodians or Alternate Custodians who have not performed COMSEC related duties for more than two years must also attend formal COMSEC training.

NOTE: It is the responsibility of the COMSEC Sub-Account Custodian or Alternate Custodian to ensure that all Loan Holders and authorized users of ACM receive training that will ensure the proper control and management of ACM in their possession.

4.1.1 CSE COMSEC Training

The CSE COMSEC Custodian and related training schedule and registration information are available from the IT Security Learning Centre (ITSLC). Evidence of completed training must be provided to CICA.

NOTE: Personnel attending training requiring access to ACM will require a COMSEC Briefing.

4.1.2 COMSEC Accounting System Training

Before installing and using a CSE-approved automated accounting system/software package to manage ACM, if available, the COMSEC Sub-Account Custodian and Alternate Custodian must attend formal training provided by CSE.

4.2 Cryptographic Equipment Training

Before using CSE-approved cryptographic equipment and to the extent possible, a COMSEC Sub-Account Custodian and Alternate Custodian should attend CSE-approved training specific to the equipment held by the COMSEC Sub-Account.

4.2.1 Manufacturer Provided Training

Some manufacturers of CSE-approved cryptographic equipment provide training for their equipment. In order to attend this training, a visit clearance authorization must be requested through the ISP if there is a contract. If the training requires ACM access, COMSEC Client Services will have to provide COMSEC access authority (refer to Article 8.5).

4.3 Loan Holder Training

COMSEC Sub-Account Custodians are normally responsible for training Loan Holders. However, Loan Holders may attend the formal COMSEC Custodian training and cryptographic training courses provided by CSE, when space is available.

5 Management of COMSEC Sub-Accounts

5.1 Establishment of a COMSEC Sub-Account

5.1.1 General

A private sector company must establish a COMSEC Sub-Account before it will be permitted to receive ACM.

Once authorized by COMSEC Client Services, CICA is responsible for coordinating the setup and management of a private sector company COMSEC Sub-Account. A CICA representative must inspect the private sector COMSEC Sub-Account site before authorizing the release of ACM (refer to Article 9.2).

Normally, only one COMSEC Sub-Account is established at each private sector company. However, if sufficient justification exists, COMSEC Client Services may approve the establishment of additional COMSEC Sub-Account(s) within a private sector company.

The minimum COMSEC Sub-Account personnel requirements are:

- a CSO
- a COMSEC Sub-Account Custodian, and
- at least one Alternate COMSEC Custodian.

NOTE: For a COMSEC Sub-Account requiring Two-Person Integrity (TPI) or No-Lone Zone (NLZ) controls (refer to Articles 8.3 and 8.4), more than one Alternate COMSEC Custodian must be appointed.

Before COMSEC Client Services will authorize the establishment of a COMSEC Sub-Account and release ACM, the private sector company must have the following:

- a sponsorship through an authorized GC sponsor;
- a valid ACMCA;
- a FOCI assessment (refer to Article 1.11.1);
- for a GC or foreign contract procured through PSPC – a PSPC-approved FSC as well as a DSC, IT and production (if required) inspection;
- confirmation of CGP registration;
- a CSO-appointed COMSEC Sub-Account Custodian and Alternate Custodian (refer to Article 3);
- for private sector company without a GC contract procured through PSPC – a CSE-approved FSC, as well as DSC and IT equivalent inspections, as required by CSE;

- required documentation (e.g. Concept of Operations [CONOP], KMSP, PSI, IP plan) as deemed necessary by COMSEC Client Services; and
- if required by COMSEC Client Services, a MOA for the provision of ACM (less accountable cryptographic equipment) with the GC sponsor.

5.1.2 Documentation

The following documents must be submitted to CICA:

- an ACMCA and any supporting agreements stating that ACM support is required;
- a completed *Sub-Account Registration* form;
- a COMSEC Sub-Account Custodian or Alternate Custodian(s) *Appointment Certificate* for each person nominated;
- full shipping and mailing address for the COMSEC Sub-Account, along with telephone number, e-mail address and facsimile number for the COMSEC Sub-Account Custodian and Alternate Custodian (s); and
- after-hours points of contact, if available.

5.1.3 Loan Holder Registration

A COMSEC Sub-Account Custodian must register Loan Holders before authorizing access to or use of ACM. The registration of a Loan Holder must include, along with criteria listed in Article 3.2, the Loan Holder's full name, title or designator, location and telephone number. Loan Holder registration must be maintained locally by COMSEC Custodians.

5.2 Files and Records

5.2.1 Administration Files

The COMSEC Sub-Account Custodian must establish and maintain administration (manual [paper] or electronic) files that are appropriate for the accounting system being employed. These files, which must be approved by CICA, include:

- courier, mail and package receipts
- general correspondence
- IT Security Alerts (ITSAs)
- training (includes training certificates of staff, Loan Holders and authorized users)
- IT Security Bulletins (ITSBs)
- *COMSEC Incident Reports*
- Transaction Number Logs
- *COMSEC Signing Authority* form
- *Appointment Certificates*
- *COMSEC Briefing Certificates*
- ACMCAs
- *COMSEC Material Control Diary*
- *Audit and Inspection Reports* and *Statement of Action* forms
- *Security Screening Certificates*

5.2.2 Accounting Files

The COMSEC Sub-Account Custodian must establish and maintain accounting files (manual [paper] or electronic) that are appropriate for the accounting system being employed. These files, which must be approved by CICA, include:

- a copy of all accounting reports (refer to Article 7), records, registers and logs with appropriate physical or digital signatures; and
- a copy of all *Inventory Reports* (GC-223) (refer to Article 7).

5.2.3 Approved Accounting Sub-Systems

CSE has approved the use of several automated and manual accounting/management systems to accommodate the minimum security requirements of NCMCS. These systems employ terminology and procedures that are quite distinct from each other.

Each NCMCS-supporting system must be PROTECTED A, with additional appropriate classification to meet special inventory requirements and any other classified information stored on the system.

NOTE: Automated accounting/management systems must employ data and system back-up procedures to mitigate system failure.

Contact CICA for a list of CSE-approved automated and manual systems or to request approval of a new system.

5.2.4 Classification of Records and Files

COMSEC Sub-Account records and files must be marked PROTECTED A unless they contain:

- classified information (e.g. effective dates, classified long titles or remarks), in which case the file or record must be marked in accordance with the sensitivity of the content; or
- a list of COMSEC material that was provided by a United Kingdom (UK) source, in which case the list must be classified at least to the minimum standard that the UK is handling the material.

NOTE: Contact CICA if assistance is required to properly classify records, files and reports.

5.2.5 Retention and Disposition of Records and Files

Unless otherwise identified in Table 2, inactive or archived COMSEC Sub-Account records and files must be retained by the COMSEC Sub-Account Custodian (or CSO) for a period of no less than five years, after which they may be authorized by CICA to be destroyed or to be forwarded to CICA for retention.

Table 2 – Administration Files/Retention Requirements

File Type	Retention Requirements
ITSAs	Until superseded by COMSEC Client Services
ITSBs	Until superseded by COMSEC Client Services
COMSEC Material Control Register – Dormant files	Refer to Article 7.1.1
COMSEC Material Control Diary	Refer to Article 7.2
COMSEC Briefing Certificates	Refer to Article 8.2.2
Visitor Logs	Refer to Article 9.1.3

5.2.6 COMSEC Material Control Register

A *COMSEC Material Control Register* must be marked PROTECTED A except for the following requirements:

- **Classified or protected long titles** – if the *COMSEC Material Control Register* contains classified or protected long titles, it must be classified or protected commensurate with the highest level of sensitivity of the long titles listed;
- **Key** – if the *COMSEC Material Control Register* contains short or unclassified long titles along with effective dates of key, it must be classified at a minimum level of CONFIDENTIAL; and
- **TPI and NLZ material** – if the *COMSEC Material Control Register* (electronic or manual) contains short or unclassified long titles of TPI or NLZ material, it must be classified at a minimum level of CONFIDENTIAL.

5.2.7 Access to Records and Files

The COMSEC Sub-Account Custodian must limit access to COMSEC Sub-Account records and files to individuals who have a need-to-know, who meet the requirement to access COMSEC material and who possess the appropriate security clearance.

5.3 Changes to a COMSEC Sub-Account

5.3.1 Change of COMSEC Sub-Account Custodian or Alternate Custodian

Before the departure of the registered COMSEC Sub-Account Custodian or Alternate Custodian, the CSO must provide CICA with an *Appointment Certificate* for a new Sub-Account Custodian or Alternate Custodian, including:

- the new COMSEC Sub-Account personnel information section completed; and
- the "Termination of Appointment" section completed for the individual being replaced.

NOTE 1: The CSO must ensure the new appointee meets all the requirements for appointment to the position including COMSEC Custodian training and a COMSEC Briefing.

NOTE 2: For unexplained departure requirements, which include permanent departure, refer to Article 5.4.5 for guidance.

5.3.1.1 Scheduling a COMSEC Sub-Account Custodian Handover

The handover of the incoming COMSEC Sub-Account Custodian should be scheduled at least 90 calendar days in advance of the outgoing COMSEC Sub-Account Custodian's departure date.

5.3.1.2 Changeover Inventory

Once the new COMSEC Sub-Account Custodian appointment has been approved by CICA, the incoming and outgoing COMSEC Sub-Account Custodians must:

- conduct a physical (sight) inventory of all ACM held by the COMSEC Sub-Account. The change of COMSEC Sub-Account Custodian is effective the date the *Inventory Report* (GC-223) is signed; and

- prepare a *COMSEC Material Report* (GC-223) listing all ACM to be transferred to the incoming COMSEC Sub-Account Custodian, identify the report in Block 1 as an "Inventory" and check "Inventoried" in Block 14. The report must be addressed from the COMSEC Sub-Account to CICA. The incoming COMSEC Sub-Account Custodian must sign in Block 15 and the outgoing COMSEC Sub-Account Custodian must sign as the witness in Block 16.

The signed original (copy #1) must be forwarded to CICA and a signed duplicate (copy #2) must be retained in the COMSEC Sub-Account's file.

NOTE: The outgoing COMSEC Sub-Account Custodian is not relieved of responsibility for ACM which is involved in any unresolved discrepancy until an *Inventory Reconciliation Report* has been received from CICA.

5.3.2 Changes to a COMSEC Sub-Account Signing Authority

The *COMSEC Signing Authority* form is a **local** form used between a COMSEC Sub-Account and **its local shipping-receiving facility**. It must be signed by the DCA/ECA and contains the names, telephone numbers and signatures of COMSEC Account personnel and any additional departmental staff who are authorized to sign for shipments containing ACM. The completed form must be retained in the COMSEC Sub-Account’s chronological file.

5.3.3 Change to COMSEC Sub-Account Registration Information

The COMSEC Sub-Account Custodian must promptly submit changes to the COMSEC Sub-Account registration information (e.g. mailing and shipping addresses, telephone numbers) to CICA. The *Sub-Account Registration* form is to be used to submit these changes.

5.3.4 Change of Classification Level of a COMSEC Sub-Account

When the classification level of a COMSEC Sub-Account needs to be changed, the CSO must submit a written request to the contract authority (normally the GC sponsor). The contract authority will then submit an amended SRCL to the ISP. The ISP must then request authorization from COMSEC Client Services for a classification upgrade or downgrade to the COMSEC Sub-Account. The request must include a justification for the requirement (e.g. change in contract requirements) and indicate the new level of classification requested.

If there is no GC contract involved, the private sector company CSO must submit the change request to its GC sponsor. The GC sponsor will then submit the request to COMSEC Client Services.

NOTE: The FSC, as well as DSC, IT and production inspection requirements, or their equivalents, must be reviewed by the appropriate authority, as required.

5.4 Absence of COMSEC Custodial Staff

5.4.1 Temporary Absence of COMSEC Sub-Account Custodian

In the absence of the COMSEC Sub-Account Custodian for a period of 60 calendar days or less, the CSO must ensure the Alternate Custodian assumes the responsibilities and duties of the COMSEC Sub-Account Custodian.

5.4.2 Return of COMSEC Sub-Account Custodian

Upon return of a COMSEC Sub-Account Custodian from a temporary absence, the Alternate COMSEC Sub-Account Custodian must inform the COMSEC Sub-Account Custodian of all changes made to the account during his or her absence.

If ACM was received and receipt acknowledged by signature on a *Hand Receipt* (GC-223) or a *Possession Report* (GC-223) by the Alternate COMSEC Sub-Account Custodian, the COMSEC Sub-Account Custodian must conduct inventory of the ACM and countersign and date the front side of the COMSEC Sub-Account's copy of the report, accompanied by the remark "received from Alternate COMSEC Sub-Account Custodian". This action will relieve the Alternate COMSEC Sub-Account Custodian of subsequent accountability for the ACM.

In those cases where ACM was issued from the COMSEC Sub-Account or destroyed, the COMSEC Sub-Account Custodian must reconcile such action by comparing the applicable report with the *COMSEC Material Control Register* and annotating the front of the applicable report.

5.4.3 Temporary Absence of Alternate COMSEC Sub-Account Custodian

In the absence of the Alternate COMSEC Sub-Account Custodian for a period of 60 calendar days or less, the CSO must ensure the second Alternate COMSEC Sub-Account Custodian assumes the responsibilities and duties. Where no second Alternate COMSEC Sub-Account Custodian has been appointed, the CSO must appoint one.

5.4.4 Absence Longer than 60 Calendar Days

An absence of the COMSEC Sub-Account Custodian or Alternate COMSEC Sub-Account Custodian for longer than 60 calendar days must be treated as a permanent absence, and the CSO must appoint a new COMSEC Sub-Account Custodian or Alternate COMSEC Sub-Account Custodian, as applicable.

5.4.5 Unexplainable Departure of COMSEC Sub-Account Custodian or Alternate COMSEC Sub-Account Custodian

In the case of an unexplainable (not including death, serious illness or short-notice personnel transfer), sudden, indefinite or permanent departure of the COMSEC Sub-Account Custodian or Alternate COMSEC Sub-Account Custodian, the CSO must take the following steps:

1. immediately report the circumstances to CICA;
2. appoint a new COMSEC Sub-Account Custodian or Alternate COMSEC Sub-Account Custodian as required;
3. ensure the applicable passwords, as well as the combinations or the lock keys of containers and vaults, are changed;
4. ensure the new COMSEC Sub-Account Custodian or Alternate COMSEC Sub-Account Custodian immediately conducts an inventory with an appropriately cleared witness (refer to Article 2.6.8); and
5. ensure the COMSEC Sub-Account audit is conducted by a CICA-designated representative/auditor.

5.5 Closing a COMSEC Sub-Account

5.5.1 COMSEC Sub-Account Closure Request

When a COMSEC Sub-Account no longer has a requirement to hold ACM (e.g. completion of a contract requiring ACM), the CSO must provide COMSEC Client Services via CICA with a written request to close the COMSEC Sub-Account. COMSEC Client Services will coordinate all requests for COMSEC Sub-Account closure with sponsoring organization(s) as appropriate.

Once authorized by COMSEC Client Services to close the COMSEC Sub-Account, the CSO must:

- direct the COMSEC Sub-Account Custodian to return all ACM held to CICA;
- provide CICA with a *Termination Certificate* (refer to Block D of the *Appointment Certificate)* for all COMSEC Sub-Account personnel; and
- upon receiving confirmation of COMSEC Sub-Account closure from CICA, return all COMSEC Sub-Account files to CICA.

5.5.2 CSE-Required Closure

Under exceptional circumstances (e.g. failure to apply correct COMSEC procedures or maintain proper physical security, sale of the company, bankruptcy or cancellation of a contract), CSE may close a COMSEC Sub-Account. The company will be notified in writing of the intent to close the COMSEC Sub-Account.

5.5.3 Prerequisite for Closure

A COMSEC Sub-Account will be closed by CICA only when all of the following steps have been completed:

1. all ACM have been returned to CICA resulting in a "Zero Balance" COMSEC Sub-Account; and
2. the CSO has sent CICA COMSEC Custodian Staff *Termination Certificates* (refer to Block D of the *Appointment Certificate*), as well as all the Sub-Account records.

5.5.4 Closure Confirmation

Once CICA has confirmed that the closure prerequisites have been met, the CSO will be notified that the COMSEC Sub-Account has been closed and that the COMSEC Sub-Account Custodial personnel have been relieved of their responsibilities regarding the COMSEC Sub-Account. Until formal notification is received from CICA, the COMSEC Sub-Account Custodian and Alternate Custodian remain responsible for the COMSEC Sub-Account and any discrepancies involving associated ACM.

5.6 Retention of a Zero Balance COMSEC Sub-Account

A COMSEC Sub-Account that holds no ACM is known as a Zero Balance COMSEC Sub-Account. A request to maintain a Zero Balance Sub-Account must be submitted, with justification (e.g. new or extension of a contract), to COMSEC Client Services via CICA. COMSEC Client Services will coordinate all requests to maintain a Zero Balance COMSEC Sub-Account with sponsoring organization(s) as appropriate.

5.7 Suspension of a COMSEC Sub-Account

5.7.1 General

CICA may temporarily suspend a COMSEC Sub-Account due to an infraction or poor account management (refer to Article 1.8). A COMSEC Sub-Account may also be suspended if:

- the CSO fails to take action to correct serious deficiencies reported in the *COMSEC Sub-Account Audit Report* or fails to submit a *Statement of Action* (SOA) form showing that corrective action is underway; or
- the number of security violations or reporting and management practices at the COMSEC Sub-Account demonstrates a disregard for COMSEC policy and procedures.

NOTE: Any suspension, regardless of how temporary, may severely impact the COMSEC Sub-Account's activities.

5.7.2 Consequence of Suspension

CICA will cease to issue ACM to a suspended COMSEC Sub-Account. The custodial staff must remain in place to conduct all other normal activities within the account, including the corrective action that would lead to the lifting of the suspension.

NOTE: CICA will inform PSPC's Canadian Industrial Security Directorate (CISD), the CSO, the GC sponsor and the COMSEC Sub-Account Custodian that the issue of ACM to the account will be suspended. The notification will include a list of the discrepancies that caused the suspension, the corrective action needed to allow the lifting of the suspension and a target completion date.

5.7.3 Lifting Suspension

Upon receipt of the SOA form, which certifies that corrective action has been completed (or is underway), CICA may lift the suspension. Before lifting the suspension, CICA, or a CICA-designated representative/auditor, will conduct another audit of the account to ensure that conditions have been rectified.

Upon lifting the suspension, CICA will notify CISD, the CSO, the GC sponsor and the COMSEC Sub-Account Custodian that the issue of ACM to the COMSEC Sub-Account will resume.

6 Identification of Accountable COMSEC Material

6.1 General

ACM is COMSEC material that requires control and accountability within NCMCS in accordance with its Accounting Legend Code (ALC) and for which transfer or disclosure outside COMSEC channels could be detrimental to the national security of Canada and its allies.

6.2 Identification

6.2.1 Long Title

The long title provides a general description of the ACM. A long title is assigned to ACM at its point of origin or at CSE. Long titles are normally, but not always, UNCLASSIFIED.

6.2.2 Short Title

A short title is assigned to ACM at its point of origin, or at CSE, for accounting purposes. The short title is an identifying combination of letters and digits that consists of a maximum of 24 characters. For some CSE-approved automated accounting/management systems (e.g. Government of Canada Electronic Key Management System [GC EKMS]), special characters (e.g. /, -, * or #) are not permitted. For these systems, the special characters that may appear in ACM short titles, (including cryptographic equipment nameplates and COMSEC publications) are replaced with a space. Short titles are UNCLASSIFIED.

6.2.3 Edition

ACM editions may be identified by a unique alphabetic or numeric designator (e.g. A, AA, B). ACM editions are usually time sensitive and are superseded when the next edition becomes effective.

6.2.4 Accounting Numbers

6.2.4.1 Assignment of Accounting Numbers

ACM may be assigned a unique accounting serial or register number (e.g. 1234, Reg. 103) at the point of origin to facilitate accounting. A serial number is used with a Controlled Cryptographic Item (CCI) or cryptographic equipment, while a register number is used for any other material requiring an accounting number.

6.2.5 Accounting Legend Code

6.2.5.1 Description

The ALC is a numeric code assigned by the originator of the ACM to indicate its accounting and reporting requirements. The ALC is recorded on all *COMSEC Material Reports* but does not normally appear on the ACM itself. The ALC assigned by the originator must not be changed without authorization from CICA. CICA must request authorization from the originator (through COMSEC channels).

NOTE 1: If the accountability of the COMSEC material is in question, contact CICA.

NOTE 2: ALC 3 and ALC 5 are not in use.

6.2.5.2 Accounting Legend Code 1

ALC 1 is assigned to physical and electronic ACM that is subject to continuous accountability by serial and/or register number to NCOR within NCMCS. ALC 1 ACM includes:

- some unclassified and all classified physical key marked CRYPTO;
- all cryptographic equipment (including CCI) approved for classified processing;
- classified cryptographic software and firmware that are the functional equivalents of, or emulate, cryptographic equipment operations and cryptography; and
- classified full maintenance manuals and depot maintenance manuals (and their printed amendments), which contain cryptographic information.

6.2.5.3 Accounting Legend Code 2

ALC 2 is assigned to physical ACM that is subject to continuous accountability by quantity to NCOR within NCMCS. ALC 2 ACM includes:

- classified and CCI components (e.g. modular assemblies, Printed Wiring Assemblies [PWAs], Integrated Circuits [ICs], microcircuits, microchips, permuters) intended for installation (but not installed) in cryptographic equipment (refer to ITSD-08);
- specific COMSEC devices; and
- COMSEC publications.

6.2.5.4 Accounting Legend Code 4

ALC 4 is assigned to physical ACM and traditional key in electronic format that, following initial receipt, is locally accountable by serial or register number to the responsible COMSEC Account within NCMCS. ALC 4 ACM may include:

- unclassified or classified COMSEC publications dealing with a cryptographic subject (e.g. classified maintenance manuals);
- protected and unclassified key (e.g. test, maintenance and training key); and
- other unclassified or classified COMSEC material which, due to the nature of the COMSEC information it contains, requires accountability within NCMCS.

NOTE: ALC 4 ACM is accountable only to the COMSEC Account, and not to NCOR.

6.2.5.5 Accounting Legend Code 6

ALC 6 is assigned to electronic key that is subject to continuous accountability by register number(s) to NCOR within NCMCS. ALC 6 may be assigned to electronic key:

- intended to protect information having long-term intelligence value (e.g. TOP SECRET);
- used to protect other key (e.g. Key Encryption Key [KEK]);
- used for joint or combined interoperability;
- marked “CRYPTO”;
- used to generate other electronic key (e.g. key production key); and
- generated from ALC 1 physical key.

6.2.5.6 Accounting Legend Code 7

ALC 7 is assigned to electronic key that, following initial receipt, is subject to local accountability by register number(s) to the responsible COMSEC Account within NCMCS.

6.3 Entry of COMSEC Material into the National COMSEC Material Control System

Whenever ACM is assigned an ALC, it must be entered into NCMCS. This ACM must be controlled in NCMCS until it is authorized for destruction or other disposition, or the appropriate authority removes the accountability requirement. A *COMSEC Material Report* is used to enter COMSEC material into NCMCS as detailed in Article 7.4.

6.4 Types of Accountable COMSEC Material

NCMCS is approved to account for three types of ACM:

- cryptographic key
- cryptographic equipment, and
- COMSEC publications.

6.4.1 Cryptographic Key

The term key (also known as keying material or keymat in other documentation) refers to information used to setup and periodically change the operations performed in cryptographic equipment for the purpose of encrypting and decrypting electronic signals and digital signatures, determining electronic countermeasures patterns, or producing other key. Key is normally accounted for by its short title.

NOTE: As stated in Article 2.2.3, the term “key” is used throughout this document (except in the glossary) to mean “cryptographic key”.

6.4.2 Cryptographic Equipment

Cryptographic equipment (including CCI) is normally identified and accounted for by its short title, long title and serial number, rather than by its components or sub-assemblies. Whenever a component or sub-assembly that has been assigned an ALC is removed from its host equipment, it requires accountability within NCMCS and it must be identified separately by its individual short title. Refer to the Canadian Cryptographic Doctrine (CCD) series, available from CICA, for further information on specific cryptographic equipment.

NOTE: This may not always apply to IP accounting (refer to ITSD-08).

6.4.3 Controlled Cryptographic Item

The CCI marking indicates a type of cryptographic equipment that must always be accounted for and controlled within NCMCS. The term CCI applies to specific unclassified, secure communications and information handling equipment, as well as associated cryptographic components and assemblies.

In many cases, CCI will not be assigned a short title, but will instead bear a manufacturer’s commercial designator. This equipment will be marked “Controlled Cryptographic Item” or “CCI”, and will bear a government serial number label.

Since CCI and associated cryptographic components employ a classified cryptographic logic, it is only the hardware or firmware embodiment of that logic that is unclassified. The associated cryptographic engineering drawings, logic descriptions, theory of operation, computer programs, and related cryptographic information remain classified.

6.4.4 Publications

Publications may include:

- cryptographic maintenance manuals
- sensitive pages of a cryptographic maintenance manual
- cryptographic operating instructions
- classified full maintenance manuals
- classified depot maintenance manuals
- cryptographic logic descriptions
- drawings of cryptographic logics
- specifications describing a cryptographic logic
- other classified cryptographic and non-cryptographic operational publications
- replacement pages to the above and like publications, and
- extracts, supplements and addenda from accountable COMSEC publications.

6.5 Special Marking and Warning Caveats

6.5.1 CRYPTO

The “CRYPTO” caveat is used to indicate the unique sensitivity of the ACM on which it appears (or is otherwise identified). Items so marked, or identified by CSE as such, must always be accounted for within NCMCS. The CRYPTO marking will appear in bold letters on classified printed circuit boards, on the covers of printed key, on CD-ROMs, on individual key variables, and (as required) on equipment and tags or labels affixed to physical storage devices (e.g. Key Storage Devices [KSD-64s]) containing electronic key.

6.5.2 Eyes Only

Access to COMSEC material with an “Eyes Only” caveat (e.g. CAN/EYES ONLY, CAN/US/EYES ONLY, CAN/UK/EYES ONLY) is restricted only to those nationalities listed in the caveat. Access must meet the ACM access control requirements listed in Article 8.

6.6 Non-Accountable COMSEC Material

Associated COMSEC material, such as correspondence, logs and reports, may be categorized as non-accountable COMSEC material. Documents that contain classified COMSEC material but have not been assigned an ALC are also included in this category. This material must be handled through COMSEC channels, but it is excluded from accountability within NCMCS. CICA may determine that local tracking is required for non-accountable COMSEC material.

7 Accounting Registers, Forms, Reports and Notices

7.1 COMSEC Material Control Register

The *COMSEC Material Control Register* is the primary accounting tool for a private sector COMSEC Sub-Account not using an automated accounting tool. It is used to account for, and keep track of, all ACM generated or received by the COMSEC Sub-Account, from the time of its receipt or generation to its final disposition. The register is composed of individual register sheets (one per short title) for all ACM held in the COMSEC Sub-Account's inventory. The register is also used to record loans to Loan Holders (via hand receipt).

The register is divided into seven sections:

- section 1 – contains all ALC 1 items, less equipment
- section 2 – contains all ALC 2 items, less equipment
- section 3 – not used
- section 4 – contains all ALC 4 items, less equipment
- section 5 – ALC 1, 2 and 4 cryptographic equipment, including CCI
- section 6 – contains locally tracked (outside of NCMCS) CIKs, and
- section 7 – contains dormant files.

NOTE: The *COMSEC Material Control Register* is not to be used when providing ACM to authorized users since the *COMSEC Material Control Diary* (refer to Article 7.2) is used for this purpose.

7.1.1 Dormant Files

Section 7 of the *COMSEC Material Control Register* is to be used for dormant (dead) register sheets removed from the other sections. These register sheets will be inserted in Section 7 in chronological order according to the final disposition date on the sheet. Dormant files must be retained until the register sheets are authorized for destruction. Authority for destruction will be provided with the *COMSEC Inventory Reconciliation Report* following each annual inventory of a Sub-Account's holdings. Authorization from CICA must be given to destroy register sheets dated one year or more prior to the inventory date.

7.2 COMSEC Material Control Diary

The *COMSEC Material Control Diary* is used to record authorized user (refer to Article 2.6.7) access to ACM holdings of a COMSEC Sub-Account. Each diary sheet must be retained until authorized for destruction. Authorization is based on *COMSEC Inventory Reconciliation Reports* in the same manner as the *COMSEC Material Control Register*.

The *COMSEC Material Control Diary* must be completed as detailed in Table 3 hereafter.

ACM being accessed by an authorized user must be back in custody of the COMSEC Sub-Account Custodian, Alternate Custodian or Loan Holder prior to the end of the same working day on which access was granted.

Table 3 – Completion of the *COMSEC Material Control Diary*

Column	Enter
1	Date ACM was accessed or loaned.
2	Time ACM was accessed or loaned.
3	Short title, edition and, if applicable, the accounting number of the ACM.
4	Signature of the authorized user. The authorized user is signing for safeguarding the ACM while in his or her custody.
5	Signature of COMSEC Sub-Account Custodian, Alternate Custodian or Loan Holder upon access or loan of ACM.
6	Time ACM was returned or time access was removed.
7	Signature of COMSEC Sub-Account Custodian, Alternate Custodian or Loan Holder upon return of ACM or on access being removed.

7.3 Local Accounting Records and Logs

7.3.1 General

Local accounting records and logs may be used to manage the control and distribution of ACM.

NOTE: The term "local accounting" is not to be confused with "local tracking" which is used when managing COMSEC material that is **not** accountable within NCMCS.

7.3.2 Handling Instructions/Disposition Record Card

The *Handling Instructions/Disposition Record* (HI/DR) Card may be used to record the issue and destruction of individual segments of key. Before issuing a key, the COMSEC Sub-Account Custodian must enter the short title and its attributes on the HI/DR Card. The HI/DR Card is UNCLASSIFIED, but becomes CONFIDENTIAL once an entry is made. The individual and witness who perform the destruction of key segments must both initial or sign the HI/DR Card beside the entry corresponding to the segment that was destroyed.

The COMSEC Sub-Account Custodian must review each HI/DR Card to confirm the destruction of each key segment before using the record to prepare a *Consolidated Destruction Report* (GC-223).

7.3.3 Local Accounting Logs

When the distribution or re-distribution of ACM cannot be accounted for in a CSE-approved automated system, the COMSEC Sub-Account Custodian must establish a manual accounting system to locally control and account for the material. The *COMSEC Material Local Accounting Register* may be used for local control of redistributed material.

7.3.4 Transaction Number Logs

Incoming and outgoing *COMSEC Material Reports* (e.g. *Possession Reports*, *Destruction Reports* and *Hand Receipts*) require transaction numbers in Blocks 4 and 6 of the *COMSEC Material Report*. Transaction numbers must follow consecutively (without gaps in the numbers) from the date a COMSEC Sub-Account is opened until the date it is closed.

Individual sets of transaction numbers (in/out) must be used for each type of report (refer to Block 1 of the *COMSEC Material Report*). COMSEC Sub-Account Custodians may design and use any tracking method to ensure that transaction number requirements are met.

7.4 COMSEC Material Reports

The multipurpose *COMSEC Material Report* form (commonly referred to as the GC-223) is the primary form used for the control and accounting of ACM. This form is used to:

- report the change in the status of ACM (e.g. issue, possession, relief from accountability or destruction);
- report the inventory holdings of a COMSEC Sub-Account (i.e. *Inventory Report*); and
- provide notice of an action associated with ACM (e.g. *Tracer Notice*).

General instructions for the preparation of the various types of *COMSEC Material Reports* can be found on the back of the GC-223 form. The following articles list the specific requirements applicable to the preparation and distribution of each type of report.

7.4.1 Transfer Report

The distribution of ACM between two primary COMSEC Accounts is called a transfer. Except for IP COMSEC Account transactions (refer to ITSD-08), a private sector company COMSEC Sub-Account must always contact CICA if there is a requirement to move ACM outside its COMSEC Sub-Account to a primary account other than CICA or to a COMSEC Sub-Account outside the company.

7.4.2 Hand Receipt

7.4.2.1 General

The distribution of ACM from CICA to a COMSEC Sub-Account or from a COMSEC Sub-Account to a Loan Holder is called an issue. Issue of ACM is recorded and tracked using a *Hand Receipt* (GC-223). ACM being issued may be packaged as a shipment or hand delivered directly to an authorized recipient. Packages wrapped for shipment must be prepared as detailed in Article 10.

7.4.2.2 Distribution

When distributing ACM to a Loan Holder, the COMSEC Sub-Account Custodian must use a *Hand Receipt*.

The Loan Holder must sign the *Hand Receipt* to certify acceptance of the listed material, as well as an understanding of the handling requirements for the entrusted ACM. Before signing the *Hand Receipt*, the Loan Holder must inspect the ACM to verify the accuracy of the document and to establish the condition of the material (refer to Article 10).

Control and tracking responsibilities for issued material remains with the COMSEC Sub-Account Custodian; therefore, copies of *Hand Receipts* for material issued to Loan Holders are not sent to CICA.

NOTE: *Hand Receipts* for COMSEC material must be reviewed every six months by the COMSEC Sub-Account Custodian to ensure their accuracy and to verify the continued requirement for ACM by Loan Holders.

7.4.2.3 Accountability

Accountability for issued ACM resides with the issuing COMSEC Sub-Account and the Loan Holder. Upon signing the *Hand Receipt*, the Loan Holder assumes responsibility for the care and control of all ACM listed on the document; however, the Loan Holder's signature on a *Hand Receipt* does not relieve the issuing COMSEC Sub-Account Custodian from accountability for the issued ACM.

7.4.2.4 Confirmation before Issue

Before issuing ACM to a Loan Holder, the COMSEC Sub-Account Custodian must ensure the Loan Holder meets the requirements of Article 3.2 and Annex A, as well as:

- has the appropriate storage facilities for the material listed on the *Hand Receipt*;
- has been trained on the handling, storage, use and destruction (where authorized) of the ACM listed on the *Hand Receipt*;
- is aware of what constitutes a COMSEC incident;
- where necessary, has established a local accounting system that maintains strict control of each item of the ACM listed on the *Hand Receipt* whenever there is a requirement for an authorized user (refer to Article 2.6.7) to be given access to ACM; and
- signs the *Hand Receipt* acknowledging the receipt of the material and an understanding of the responsibilities associated with handling the ACM listed on the *Hand Receipt*.

7.4.2.5 Returning Accountable COMSEC Material

ACM that is listed to a COMSEC Sub-Account, but that is no longer required, must be returned to CICA, using a *COMSEC Material Report* (GC-223).

Upon receipt and verification of the returned material, CICA will sign the *COMSEC Material Report* (GC-223) and return it to the COMSEC Sub-Account, thereby relieving the COMSEC Sub-Account from accountability for the returned material.

Loan Holders must return ACM to the COMSEC Sub-Account Custodian when it is no longer required unless it has been authorized for local destruction by the COMSEC Sub-Account Custodian. The COMSEC Sub-Account Custodian must prepare a *Hand Receipt* for material being returned from the Loan Holder. The COMSEC Sub-Account Custodian must ensure that the *Hand Receipt*, which lists the material being returned from the Loan Holder, is addressed to the COMSEC Sub-Account. The COMSEC Sub-Account Custodian's signature on the *Hand Receipt* relieves the Loan Holder from accountability for the returned ACM.

7.4.3 Possession Report

7.4.3.1 General

Occasionally, circumstances dictate that ACM for which a current record of accountability within NCMCS does not exist must be taken on charge at a COMSEC Sub-Account.

A *Possession Report* (GC-223) is used to document the entry of ACM into NCMCS in the following circumstances:

- ACM under development or manufacturing has been accepted by the GC (refer to ITSD-08) after being received without an accompanying *Hand Receipt*;
- ACM previously declared lost and removed from accountability is subsequently found;
- an accountable COMSEC publication requiring control within NCMCS is reproduced (only with CICA authorization) in whole or in part;
- a magnetic or optical medium is used to issue electronic key;
- a non-automated COMSEC Sub-Account converts its inventory to an automated CSE-approved accounting system; and
- a COMSEC Sub-Account is in possession of ACM that is not listed on any COMSEC Account inventory.

NOTE: Some of the circumstances listed above may also require the COMSEC Sub-Account Custodian to initiate a COMSEC incident. If there is uncertainty as to whether a COMSEC incident has occurred, contact CICA for guidance.

7.4.3.2 Preparation

Except as detailed in Article 11.3.2.5 and in ITSD-08, authorization from CICA must be given prior to a COMSEC Sub-Account initiating a *Possession Report*. The following applies to the preparation and distribution of a *Possession Report*:

- a brief description of why the item is being possessed must be included in either the remarks column or after the “NOTHING FOLLOWS” line; and
- if the report lists COMSEC material accountable to NCOR, a copy must be sent to CICA within five working days following the creation of the report. *Possession Reports* listing only ALC 4 or ALC 7 COMSEC material must be retained locally.

7.4.3.3 Distribution

A *Possession Report* must be distributed as follows:

- send the original signed copy to CICA;
- retain copy on files; and
- if reporting ACM received without a *COMSEC Material Report* and the source of the material is known, send a copy to the source.

7.4.4 Relief from Accountability

A *Relief from Accountability Report* (GC-223) is used to document the removal of ACM from a COMSEC Sub-Account inventory.

COMSEC Sub-Account Custodians may seek relief from accountability for ACM that has been irretrievably lost.

7.4.5 Destruction Report

Under normal circumstances a private sector company will only be permitted to destroy accountable COMSEC key when supported by a status letter (refer to Article 12.2) from CICA. A *Destruction Report* (GC-223) is used to document the physical destruction or electronic zeroization of ACM, whether by authorized means or by accident and serves to report items removed from accountability (refer to Article 12).

7.4.5.1 Preparation and Distribution

The following applies to the preparation and distribution of a *Destruction Report*:

- list, in alphanumerical order, all key that is scheduled for destruction;
- enter the reason for the destruction (e.g. zeroized, superseded);
- if the *Destruction Report* lists ALC 1, ALC 2, ALC 4, ALC 6 or ALC 7 key, send a signed copy to CICA; and
- retain a signed copy of the *Destruction Report* on file.

7.4.6 Consolidated Destruction Report

A *Consolidated Destruction Report* (GC-223) must only be originated when it can be based on other destruction documentation (e.g. HI/DR Card). Prior to originating a *Consolidated Destruction Report* that lists a complete edition of key, the custodial staff must confirm that all key segments of that edition have been destroyed.

In such cases, the appropriate destruction documents, duly signed and witnessed, must be forwarded to CICA.

7.4.6.1 Preparation and Distribution

The following applies to the preparation and distribution of *Consolidated Destruction Reports*:

- review local destruction records (e.g. HI/DR Card) for accuracy, appropriate authorizations and required signatures;
- list the key that was destroyed (and reported as destroyed on local accounting records) during the month;
- annotate the report with "*Consolidated Destruction Report*";
- if the report contains ALC 1, ALC 2, ALC 4, ALC 6 or ALC 7 key, submit the report to CICA no later than the 16th of the month following destruction of the key; and
- retain a copy of all *Consolidated Destruction Reports* on file.

7.5 Seed Key Conversion Report

The Canadian Central Facility (CCF) generates a monthly *Seed Key Conversion Report* (SKCR) for Secure Communication Interoperability Protocol (SCIP) equipment that lists the Key Material Identifier (KMID) of key that has been converted from seed key to operational key.

When a Loan Holder initiates a secure call from authorized SCIP equipment to the Secure Data Network System (SDNS) Public Switched Telephone Network (PSTN)-Integrated Services Digital Network (ISDN) Rekey Subsystem (SPIRS), operational key is sent to that Loan Holder's SCIP equipment.

Once the operation is completed, the Loan Holder can use his or her equipment to place secure calls to other SCIP users. A copy of the SKCR will be sent to the COMSEC Sub-Account Custodian by CICA on a monthly basis or upon request. The COMSEC Sub-Account Custodian must verify to CICA that a *Destruction Report* has been completed for all KMIDs listed on the report.

7.6 Operational Rekey Report

The CCF generates a monthly *Operational Rekey Report* (ORR) that lists the KMIDs for SCIP equipment used to place a secure call to the SPIRS. Upon initiation of a secure call to the SPIRS, a new operational key is downloaded to the SCIP equipment along with a *Compromised Key List* (CKL). A copy of the ORR will be sent the COMSEC Sub-Account Custodian by CICA on a monthly basis or upon request. This report must be used to verify that end users conduct quarterly rekey calls to the SPIRS and ensure that they have the latest CKL. CICA must use the ORR to verify that a *Destruction Report* has been completed for all KMIDs listed on the report.

7.7 Inventory Report

COMSEC Sub-Account Custodians are responsible for conducting inventories. During the inventory process, the ACM held at the COMSEC Sub-Account is physically sighted and the actual holdings are compared to the accounting records. The inventory process is very important as it is sometimes the only means of discovering the loss of ACM. For detailed information on *Inventory Reports*, refer to Article 13.

7.8 Tracer Notices

7.8.1 Hand Receipts

If CICA has not received a signed *Hand Receipt* within 20 working days of the date on which the receipt was sent, CICA will send a *Tracer Notice* to the delinquent COMSEC Sub-Account.

7.8.2 Inventory Reports

Missing *Inventory Reports* will result in an inability to reconcile a COMSEC Sub-Account's inventory. CICA will originate tracer action for the missing *COMSEC Material Reports*.

7.9 Failure to Respond to Tracer Notices

Failure to respond to a *Tracer Notice* could result in an immediate audit of the COMSEC Sub-Account by a CICA-designated representative/auditor.

If initial tracer action and CICA assistance fails to resolve the issue, secondary *Tracer Notices* must be sent to the CSO for action (including investigation into potential COMSEC incident reporting).

8 Access to Accountable COMSEC Material

8.1 Prerequisite for Access to Accountable COMSEC Material

8.1.1 Access by Private Sector Company Employees

Access to ACM may be granted to Canadian citizens (including those of dual nationality) who:

- possess a valid security clearance commensurate with the security classification of the material and information they will access;

  NOTE: Refer to Article 3.1 for security clearance requirements for COMSEC Sub-Account Custodians and Alternate Custodians.

- have a need-to-know;
- have been given a COMSEC Briefing;
- have signed a *COMSEC Briefing Certificate*;
- are familiar with applicable COMSEC material control procedures; and
- are designated as a COMSEC Sub-Account Custodian, IP COMSEC Account Custodian, Alternate Custodian, Loan Holder or an authorized user who is required to use ACM in the performance of his or her duties and who is responsible for safeguarding that ACM.

8.1.2 Access by Foreign Nationals

Access to ACM may be granted to foreign nationals (i.e. non-Canadian citizens) upon approval from COMSEC Client Services on a case-by-case basis. Requests for such access must be submitted in writing to COMSEC Client Services by the requesting DCA.

8.1.3 Requirements for Participation in a Government of Canada Request for Proposal

A private sector company will not be excluded from seeking to bid on a GC RFP that requires access to ACM solely on the basis of not having an established COMSEC Sub-Account prior to submitting its bid. A private sector company that wishes to bid on a RFP, but that does not hold a COMSEC Sub-Account must contact COMSEC Client Services to request an assessment of suitability for the establishment of a COMSEC Sub-Account should it be awarded the contract. The private sector company must then be able to meet the prerequisites for the establishment of a COMSEC Sub-Account detailed in this directive prior to any ACM being made available.

NOTE 1: The ISP must also complete an assessment of suitability for an FSC, IT processing, DSC and FOCI.

NOTE 2: The CGP requirements (refer to Article 1.11.2) must be met.

8.2 COMSEC Briefing and COMSEC Briefing Certificate

8.2.1 Requirements

CICA will administer an initial COMSEC Briefing to the COMSEC Sub-Account Custodian who must then ensure that all individuals requiring access to ACM receive a COMSEC Briefing and sign a *COMSEC Briefing Certificate*.

NOTE: Any individual being re-appointed at the same or at a different COMSEC Sub-Account as a COMSEC Sub-Account Custodian, Alternate Custodian or Loan Holder must be given a new COMSEC Briefing and sign a new *COMSEC Briefing Certificate*.

A COMSEC Briefing is required for individuals (including COMSEC Sub-Account personnel, Loan Holders, individuals attending CSE and international COMSEC training and COMSEC forums, and individuals who need "user access" or "maintainer access" during installation, troubleshooting, repair, or physical keying of equipment) who require access to:

- ACM;
- cryptographic information which embodies, describes or implements a classified cryptographic logic;
- cryptographic information including, but not limited to full maintenance manuals, cryptographic computer software (must be a continuing requirement);
- classified IP ACM or CCI and components at any phase during its production or development; and
- cryptographic key or logic during its production or development.

8.2.2 Retention of COMSEC Briefing Certificates

A *COMSEC Briefing Certificate* for those having access to COMSEC Sub-Account ACM must be kept on file for at least two years after authorized access to ACM has ended.

8.2.3 COMSEC Debriefings and Updates

COMSEC debriefings are not required when access to ACM is no longer required. COMSEC Briefing updates are required every five years for active COMSEC Sub-Account Custodians, Alternate Custodians, Loan Holders or authorized users.

8.3 Two-Person Integrity

TPI is a security measure designed to prevent any one person from having solitary access to specified ACM (e.g. TOP SECRET key). Each individual having TPI access must be capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. TPI-regulated storage and handling require the use of security devices protected by two approved locks (refer to the Royal Canadian Mounted Police [RCMP] *Security Equipment Guide* [G1-001]), Personal Identification Numbers (PINs) or passwords, with no one person having access to both sets of combinations, lock keys, PINs or passwords.

NOTE: Access to the G1-001 can be obtained by contacting COMSEC Client Services.

8.4 No-Lone Zone

Certain areas in a COMSEC facility may be designated as a NLZ. A minimum of two authorized individuals must be in visual contact with each other at all times within a NLZ. If the departure of one individual would leave a single occupant, then both individuals must leave and secure the NLZ.

The CSO will establish a NLZ for a COMSEC Sub-Account where:

- TOP SECRET key is received, stored, handled, used and destroyed;
- physical key is produced; or
- cryptographic equipment is designed, developed, manufactured or maintained.

8.5 Access Control – COMSEC Visits

It is the responsibility of the CSO to ensure that all visits to the company that involve access to ACM, classified and protected COMSEC information, or material related to ACM are authorized by the ISP if there is a GC contract.

A private sector company that has a requirement to access ACM, classified and protected COMSEC information, or material related to ACM outside its own company must submit a visit clearance request through the ISP. The ISP will then submit a COMSEC access authorization request to COMSEC Client Services. COMSEC Client Services will inform the CICA manager of the visit request and authorization or refusal.

The following visit requirements that involve the access to ACM, classified and protected COMSEC information, or material related to ACM must be authorized by COMSEC Client Services:

- GC department to a Canadian private sector company;
- Canadian private sector company to a GC department;
- Canadian private sector company to a Canadian or foreign private sector company; and
- Canadian private sector company to a foreign government agency.

NOTE 1: Private sector companies under contract must ensure that all visitors, including GC departments that require access to ACM, are approved by the ISP.

NOTE 2: ISM requirements at Article 2.6.2 notwithstanding, a CICA representative does **not** require COMSEC visit clearance authority from the ISP; however, the ISP must provide visitor information to the CSO as detailed in Article 8.6.

8.6 COMSEC Visit Request

For GC contracts, the ISP will submit a COMSEC access authorization request for a Canadian visit to a foreign government organization or private sector company (including foreign company) that requires access to ACM, classified and protected COMSEC information, or material related to ACM to COMSEC Client Services a minimum of 45 calendar days prior to the anticipated visit.

The COMSEC Visit Request must include:

- surname of the visitor
- all given names of the visitor

- date of birth (DD/MM/YYYY) of the visitor
- place of birth of the visitor
- citizenship (including dual nationality) of the visitor
- clearance level (verified by security staff) of the visitor
- copy of signed *COMSEC Briefing Certificate*
- contract or sub-contract number associated with visit requirement
- reason for visit (COMSEC access required)
- name, telephone, fax, e-mail address of security point of contact at destination
- name, telephone, fax, e-mail address of point of contact or office of primary interest at destination, and
- full address of company or agency to be visited.

Once COMSEC Client Services authorize the COMSEC access and the ISP authorizes the visit, it is the responsibility of the requester, prior to the visit, to ensure that the visit clearance and COMSEC access authorization are in place at final destination. This should be done at a minimum of five working days prior to the visit to ensure any discrepancies can be resolved.

NOTE: For visits outside Canada, include passport number and expiry date.

9 Physical Security

9.1 COMSEC Facilities

9.1.1 Requirement

A COMSEC facility must be established wherever ACM is generated, stored, repaired, used or warranted by operations (e.g. COMSEC Sub-Account Custodian work area). A COMSEC facility is either fixed or mobile. The facility must provide the maximum possible protection from theft, compromise, damage and deterioration of COMSEC material, and ensure that access and accounting integrity is maintained.

COMSEC Sub-Account Custodian work areas that are outside of established COMSEC facilities (e.g. temporary structures, mobile vehicles) that are not considered COMSEC facilities must be authorized by COMSEC Client Services.

NOTE: An office environment where only user-level cryptographic equipment and BLACK (encrypted – refer to Article 11.1.2) key is available for individual use is not considered a COMSEC facility; however the office area must be protected, at a minimum, to the highest classification of the equipment when keyed.

9.1.2 Planning and Establishing a Fixed COMSEC Facility

When planning and establishing a fixed COMSEC facility, the CSO must:

- consult COMSEC Client Services to accommodate the direction in Article 3 of this directive;

- ensure a *Threat and Risk Assessment* (TRA) is conducted before initial activation (where practical) and periodically thereafter based on threat, physical modifications, sensitivity of operations and *COMSEC Incident Reports* of a serious nature;
- establish the COMSEC facility in an area which provides positive control over access using a hierarchy of zones (refer to Article 6.2 of the Treasury Board of Canada Secretariat [TBS] *Operational Security Standard on Physical Security* and the RCMP *Guide to the Applications of Physical Security Zones* (G1-026). Contact the ISP or COMSEC Client Services for additional guidance;
- construct the COMSEC facility according to the *Operational Security Standard on Physical Security* and the G1-026; and
- produce a standard operating procedure (in conjunction with the *COMSEC Emergency Plan*) containing provisions for securely conducting facility operations.

9.1.3 Access Controls and Restrictions

The COMSEC Sub-Account Custodian must:

- establish an access list of authorized individuals who have regular duty assignments in the COMSEC facility;
- limit unescorted access to individuals who are Canadian citizens (including dual nationality), whose duties require such access and who meet the access requirements of Article 8;
- ensure all visitors (including cleaning staff) are recorded in a visitor log and that the log is retained for at least one year after the date of the last entry. The visitor log must contain, at a minimum:
  - the date/time of arrival and departure of the visitor
  - the visitor's name, printed
  - the visitor's signature
  - the purpose of visit, and
  - the signature, including printed name, of the authorized individual admitting the visitor;
- ensure visitors are continuously escorted by the authorized individual whose name is on the access list;
- prohibit non–CSE-approved devices and equipment capable of receiving and recording intelligible images, sound recording devices and equipment, radio transmitting and receiving equipment, microphones, and television receivers from the COMSEC facility;
- post a sign to identify the area as a RESTRICTED ACCESS area;
- establish and document a daily security check procedure to ensure that ACM is properly safeguarded and that approved physical security protection devices (e.g. door locks, alarm system) are functioning properly; and
- ensure unmanned facilities in areas posing a high risk of compromise employ an electronic intrusion detection system that meets the *Underwriters Laboratories of Canada (ULC) Standard* ULC-S306-03. Physical checks must also be conducted at least once every 24 hours to ensure that all doors to the facility are locked and that there have been no attempts at forceful entry.

9.2 COMSEC Facility Approval

Every new, remodeled or relocated facility for the COMSEC Sub-Account Custodian work area must be approved by CICA before a private sector company is authorized to receive ACM. Following a visit by CICA staff, an authorization will be granted if the facility meets the requirements for safeguarding ACM, as detailed in this directive.

NOTE: This requirement is in addition to the FSC, DSC, IT inspections or their equivalent CSI requirements.

9.3 Secure Storage

9.3.1 Security Containers

ACM must be stored in security containers (e.g. vaults, safes, file cabinets, etc.) that are approved for the classification or protected level of the ACM and which meet the requirements of the RCMP G1-001.

Security containers used for the storage of ACM must be located in a security zone appropriate for the level of classification of the ACM. For further guidance on the use and procurement of secure containers, contact the ISP or COMSEC Client Services.

NOTE 1: Briefcases are not considered storage containers and must not be used as such.

NOTE 2: Access to the RCMP G1-001 can be obtained by contacting COMSEC Client Services.

9.3.2 Segregation of COMSEC Material in Storage

The rules for the minimum segregation of ACM in physical storage are:

- effective editions, reserve editions and superseded key awaiting destruction must be stored separately from each other in approved security containers (refer to the RCMP's G1-001); and

  NOTE: Access to the RCMP G1-001 can be obtained by contacting COMSEC Client Services.

- key or Cryptographic Ignition Keys (CIKs) must not be stored in the same security container as the equipment with which they may be used.

  NOTE: In situations where space is at a premium, segregation may be accomplished using a locked strongbox housed within a single security container.

9.3.3 Opening of Security Containers in Emergency Situations

When the COMSEC Sub-Account Custodian and Alternate Custodian(s) are not available to open a security container in an emergency, the CSO (or other designated authority) may direct the opening of the security container, under the following conditions:

- at least two individuals must be present to gain access to the combination and to open the security container;
- the individuals who opened the security container must prepare a written report (containing an inventory of the contents and the circumstances surrounding the access requirement) to the individual(s) in charge of the security container, after the emergency opening; and
- the individual(s) responsible for the security container must conduct a full inventory of the ACM and change the combination(s), immediately upon their return.

In the event of an emergency where access is required to ACM that has been previously issued to a Loan Holder who is not available, the individual requiring immediate access must contact either the COMSEC Sub-Account Custodian or Alternate Custodian.

9.3.4 Incidents Involving Unattended Security Containers

In the event of a security incident (e.g. if a container or vault is found open and unattended during or after normal working hours), the individual discovering the incident must notify the COMSEC Sub-Account Custodian or Alternate Custodian. If the COMSEC Sub-Account Custodian or Alternate Custodian cannot be located, another individual on the list of individuals having knowledge of the combinations or keys to the container must be contacted. The COMSEC Sub-Account Custodian and Alternate Custodian must conduct a full inventory of the container's contents and then secure the container (e.g. provide a new key lock or change the combination).

In the event of an incident relating to ACM that has been issued to a Loan Holder, the individual discovering the incident must contact either the COMSEC Sub-Account Custodian or the Alternate Custodian.

9.4 Protecting Lock Combinations and Lock Keys

9.4.1 General

Any sign of tampering with or suspicion of compromise of a lock or its associated combinations (or lock keys) must be immediately reported to CICA.

9.4.2 Change of Combinations

The COMSEC Sub-Account Custodian must ensure that combinations for locks used for the secure storage of ACM are changed by a CSO–authorized person when:

- the lock is first put into use by the COMSEC Sub-Account Custodian (i.e. the manufacturer's pre-set combination must not be used);
- an individual knowing the combination ceases to have authorized access to the storage facility or the security container;
- an unauthorized individual has had access to the written record of the combination;
- the combination is known or suspected to have been compromised;
- the lock has been repaired, serviced or inspected by a person not having authorized access to the storage facility or security container;
- the combination has not been changed in the last 12 months; or
- the lock is temporarily or permanently taken out of use.

9.4.3 Selection of Combinations

Each lock must have a combination composed of randomly selected numbers based on the manufacturer's specifications. The combination must not be a duplicate of another lock combination within the facility. It is further recommended that combination numbers:

- do not include dates of birth, room numbers, civic addresses, etc.;
- be separated as follows:
  - on cabinets with integrated locks – the dial numbers are separated into two groups: Low numbers (L) 0-49 and High numbers (H) 50-99; and
  - on combination padlocks – the dial numbers are also separated into two groups (L) 0-24 and (H) 25-49;
- be separated by at least 10 numbers; and
- do not include numbers between 90 and 10 on cabinets with integrated locks, nor the third number be between 90 and 20.

9.4.4 Classification of Combinations

Lock or vault combinations must be classified commensurate with the highest sensitivity level of the information or material protected by the combination.

9.4.5 Change of Key–Operated Locks

The COMSEC Sub-Account Custodian must ensure that key-operated locks used to secure ACM are replaced and not re-used to secure ACM when:

- an individual ceases to have authorized access to the security container;
- an unauthorized individual has had access to a lock key;
- the lock key or lock is known or suspected to have been compromised;
- the lock has been repaired, serviced or inspected by a person not having authorized access to the security container; or
- the lock has not been changed in the last 12 months.

9.4.6 Protection of Combinations and Spare Lock Keys

When a combination lock or key–operated lock is changed by the individual responsible for the security container, the COMSEC Sub-Account Custodian must ensure that the responsible individual has:

1. sealed the combination numbers (or spare lock keys) in an opaque envelope in such a manner that tampering with the envelope is evident;
2. marked the envelope with the highest classification or protected level of the ACM that the combinations (or lock keys) protect and listed the name and telephone number of the individual(s) authorized access to the combinations (or lock keys); and

3. given the envelope to the COMSEC Sub-Account Custodian for secure storage in a storage container that meets or exceeds the classification or protected level of the material being protected by the combinations (or lock keys).

9.4.7 Record of Combinations and Lock Keys

The COMSEC Sub-Account Custodian must keep a record of the name and telephone number of individuals having knowledge of the combinations or hold lock keys to containers in which ACM is stored. Normally, the containers will be under the direct control of the COMSEC Sub-Account Custodian and the Alternate Custodian(s).

9.4.8 Access to and Knowledge of Combinations or Lock Keys

The COMSEC Sub-Account Custodian must ensure that only appropriately cleared and authorized personnel have access to, or knowledge of, combinations or lock keys that protect the ACM for which they are accountable. Personnel with knowledge of combinations must not record and carry the combinations or store the records of such combinations in electronic form. Lock keys must not be stored in key press cabinets that are accessible to any personnel other than the COMSEC Sub-Account Custodian or Alternate Custodian(s).

9.4.9 Combinations for Two-Person Integrity Containers and No-Lone Zones

The COMSEC Sub-Account Custodian must ensure that no one person may change both combinations or be allowed access to or have knowledge of both combinations to a security container used to store COMSEC material requiring TPI control or to an area used as a NLZ.

NOTE: Lock combinations must be classified and safeguarded at the highest classification of the material they protect.

9.5 Storage of Cryptographic Key

9.5.1 Physical Key Storage Requirements

Key not under the direct continuous control of a cleared and authorized individual (or individuals where applicable) must be stored in a locked, approved security container (refer to the RCMP G1-001), in an area protected by security guards or by an intrusion detection system (i.e. Security Zone, High Security Zone). Refer to Table 4 – Storage of Physical Key for specific requirements for the storage of physical key.

Table 4 – Storage of Physical Key

Key	Storage Requirements
TOP SECRET key and other key requiring TPI control	TOP SECRET key must be stored under TPI controls in containers meeting the RCMP G1-001. TOP SECRET key that is held within a work area for intermittent use throughout the day may be kept under one lock in a NLZ. Knowledge of the combination or access to the key used to secure the lock must be restricted to the supervisor on duty. TOP SECRET key in tactical environments may be: • stored in a standard, approved field safe; • stored in a similar container secured by a combination lock meeting the RCMP G1-001; or • kept under personal custody if adequate storage facilities are not available.
SECRET, CONFIDENTIAL and PROTECTED C key	SECRET, CONFIDENTIAL and PROTECTED C key must be stored: • in any manner approved for TOP SECRET key; or • in a container approved for SECRET, CONFIDENTIAL or PROTECTED C material, as applicable, with an approved combination lock.
PROTECTED A and PROTECTED B key	PROTECTED A and PROTECTED B key must be stored in any manner approved for classified key.
UNCLASSIFIED key	UNCLASSIFIED key must be stored by the most secure means available provided that it will reasonably preclude theft, sabotage, tampering or use by unauthorized individuals.
Foreign key	Foreign key must be stored in accordance with the instructions for Canadian COMSEC material of equivalent sensitivity. UNCLASSIFIED, RESTRICTED and UNCLASSIFIED/For Official Use Only (U/FOUO) foreign key marked “CRYPTO” must be stored as PROTECTED A (or higher) COMSEC material.
Open storage	Any storage of classified national security information outside of approved containers. This includes classified information that is resident on information systems media and outside of an approved storage container, regardless of whether or not that media is in use (i.e. unattended operations). Open storage of classified cryptographic material and equipment must be done within an approved COMSEC facility, vault, or secure room when authorized personnel are not present. Except when storing TOP SECRET key, TPI and NLZ controls are NOT required.

9.5.2 Key Held in Reserve

The amount of key to be held in reserve varies with the supersession rate of the key. Table 5 – Key Held in Reserve provides a guide to the amount that may be held in reserve. For a requirement to hold more than what is listed in Table 5 – Key Held in Reserve, contact CICA.

Table 5 – Key Held in Reserve

Supersession Rate	Held in Reserve
Key superseded daily, ten times monthly, semi-monthly and monthly.	Editions effective during the current month, plus three months reserve.
Key superseded every two months or quarterly.	Effective edition plus two editions reserve.
Key superseded semi-annually, annually and irregularly.	Effective edition plus one edition reserve.
SDNS seed key (five year retention factor).	One seed key may be held in reserve.

9.5.3 Storage of Electronic Key

Electronic key must be stored according to equipment-specific doctrine.

9.6 Storage of Cryptographic Equipment

9.6.1 General

All cryptographic equipment must be stored in a manner consistent with its classification or protected level and security markings (e.g. CRYPTO, CCI) when not under the direct and continuous control of appropriately cleared and authorized personnel. Cryptographic equipment may require special storage procedures or storage facilities. Refer to equipment–specific doctrine for detailed information on storage of cryptographic equipment, or contact CICA.

NOTE: UNCLASSIFIED cryptographic equipment and unkeyed CCI require storage that provides reasonable protection from compromise, theft, tampering and damage.

9.6.2 Preparation for Storage

Accountable cryptographic equipment must never be stored in a keyed state, unless:

- operational requirements mandate it and no practical alternative exists; or

  NOTE: CICA authorization is required.

- it cannot be zeroized due to malfunction or damage.

When cryptographic equipment is stored in a keyed state, it must be stored in accordance with the highest classification of key loaded in the equipment.

NOTE 1: CCIs that use a CIK are considered unlocked whenever the CIK is inserted and locked with the CIK removed and not accessible for use by unauthorized persons.

NOTE 2: CCIs that use only a PIN to unlock the secure mode are considered unlocked whenever the PIN is entered.

NOTE 3: CCIs that use a CIK and password/PIN combination are considered unlocked whenever the CIK is inserted and the proper password/PIN authenticated.

9.6.3 Spare or Standby Cryptographic Equipment

Spare or standby cryptographic equipment that is located within a secure work area is considered installed for operation. The storage requirements in the previous articles are not applicable to such equipment.

9.7 Storage of Accountable COMSEC Publications

Accountable COMSEC publications must be stored in accordance with their security classification and any caveat(s) or other security marking(s).

10 Distribution and Receipt of Accountable COMSEC Material

10.1 General

CICA is the authority for the movement of ACM outside a COMSEC Sub-Account.

10.2 Transfer To or From a Foreign Interest

Transfer of ACM to or from a foreign interest (government or private sector established COMSEC Accounts) must only be completed via government-to-government NDAs. CICA must authorize in coordination with COMSEC Client Services the transfer via the responsible NDAs.

10.3 Transmission of Key via Telecommunications Systems

Except when using cryptographic systems specifically designed and authorized for remote rekeying, operational keying variables must only be transmitted via telecommunications means in emergency circumstances and only under the following conditions:

- the approval from CICA must be obtained prior transmission of operational keying variables;
- a cryptographic system that provides end-to-end encryption must be employed (i.e. the key setting will not appear in plain text anywhere in the communications path); and
- the transmitting system must be keyed with a setting that is classified or protected equal to, or higher than, that of the key being transmitted.

10.4 Distributing Accountable COMSEC Material Outside of a Sub-Account

It is a COMSEC Sub-Account Custodian’s responsibility, in coordination with CICA, to ensure that individual shipments of ACM are kept to the minimum required to support contractual requirements.

When preparing ACM for distribution, the COMSEC Sub-Account Custodian must:

- ensure the receiver meets the requirements for storage of ACM (refer to Article 9.3), perform page checks, equipment checks and inspection of protective packaging immediately (no earlier than 48 hours) before packaging;
- zeroize or remove CIKs from all CCI before transportation (or, when circumstances warrant, keyed devices may be hand-carried by authorized private sector company couriers);
- package operational and seed key separately from its associated cryptographic equipment (including CCI) and transport in different vehicles on different days, unless:
  - the application or design of the equipment is such that the corresponding key cannot be physically separated from it;
  - the key is an UNCLASSIFIED maintenance key (which may be shipped in the same container as its associated cryptographic equipment); or
  - there are no other means available to effect delivery to support an immediate requirement;

    NOTE 1: When cryptographic equipment must be shipped in a keyed state or with its associated key, ship the package in accordance with the classification of the key or the cryptographic equipment, whichever is higher.

    NOTE 2: A private sector company must not ship cryptographic equipment in a keyed condition without authority from CICA.
- send the list of effective dates of editions of key separately, and on different days, from the key;
- package each Traffic Encryption Key (TEK) separately from its associated KEK;
- package components which comprise a cryptographic system (i.e. cryptographic equipment, ancillaries, associated documentation and key variables) separately and transport in different shipments;
- apply TPI controls to TOP SECRET key during its transit unless it is enclosed in manufacturer's protective packaging and is double-wrapped, in which case only one courier is required;
- ensure that electronic key is transmitted in accordance with the applicable system or equipment doctrine; and
- prepare a *COMSEC Material Report* as detailed in Article 7.

10.5 Distributing Electronic Key on Magnetic or Optical Removable Storage Media

In addition to the criteria specified in Article 10.4, when electronic key is distributed (i.e. transferred or issued) on magnetic or optical Removable Storage Media (RSM), the RSM must be controlled as a separate COMSEC item within NCMCS as ALC 4. The COMSEC Sub-Account Custodian must affix a label to the RSM similar to the example label depicted in Figure 2 – Example of a Magnetic or Optical Removable Storage Media Label. The accounting number is taken from a "next in sequence" number log maintained by the COMSEC Sub-Account Custodian to record the sequential serial numbers of the RSM. The originating COMSEC Sub-Account Custodian must prepare and process a *Possession Report* (GC-223) in accordance with Article 7 to enter the new ACM into NCMCS before distributing the RSM (containing the electronic key).

A *Transfer Report* (GC-223) is required to account for the physical transport of RSM and another *Transfer Report* is required to account for the transfer of the electronic key that is being transported by the RSM. Both reports must be signed and returned to the originating COMSEC Account.

If RED (unencrypted – refer to Article 11.1.2) key is being transported on a magnetic or optical RSM, the label must also display the CRYPTO marking and the highest classification of key being transported (minimum SECRET).

Classification:	SECRET (CRYPTO if applicable)
Accounting Legend Code:	ALC 4
Short Title:	CAKAE 4005 (+ COMSEC Account Number)
Accounting Number:	(Unique next in sequence number)

Figure 2 – Example of a Magnetic or Optical Removable Storage Media Label

10.6 Tracking the Shipment of Accountable COMSEC Material

The COMSEC Sub-Account Custodian must:

- notify the recipient, within 24 hours of shipment, of the details of the shipment and the estimated time of delivery;
- ensure the telephone numbers of both the shipping and the receiving COMSEC Sub-Accounts are listed on the waybill when ACM is shipped by commercial carrier or Canada Post Priority Courier;
- keep a local record of the shipment; and
- follow-up to ensure the ACM is delivered to the authorized recipient according to schedule, and
  - if a shipment is not received within 48 hours of expected delivery, initiate shipment tracer action with the carrier to determine the last known location of the shipment; and
  - if the location cannot be determined and the shipment is not recovered within 24 hours of the shipment tracer initiation, assume that the shipment is lost in transit and immediately report the loss as a **COMSEC incident** as detailed in Article 16.

10.7 Packaging Accountable COMSEC Material

10.7.1 Overview

Packaging used for the distribution of physical ACM will depend upon the material's size, weight, shape and intended method of transport. All ACM must be double-wrapped or otherwise encased in two opaque containers and securely sealed (including seams) before its transportation.

NOTE: Windowed envelopes or any other form of transparent wrapping such as plastic-sealed packaging is not considered as one of the two required covers.

10.7.2 Inner Wrapping

The inner wrapping must:

- be secure enough to detect tampering;
- guard against damage; and
- be marked as follows:
  - full addresses of both the shipping and receiving COMSEC Accounts,
  - highest classification or protected level of the contents,
  - caveat “CRYPTO” if any of the contents are so marked, and
  - notation “TO BE OPENED ONLY BY THE COMSEC CUSTODIAL STAFF”.

The sealed envelope containing the copies of the *COMSEC Material Report* may be enclosed inside the package or affixed to the external surface of the inner wrapping of the package. When more than one package is required, the envelope may be enclosed or affixed to the first package of the series.

NOTE: Protective packaging (e.g. key canisters) is not considered an inner wrapping when preparing items for shipment (refer to Article 11.1.4).

10.7.3 Outer Wrapping

The outer wrapping must:

- be secure enough to prevent damage to the contents or inadvertent or accidental unwrapping;
- not bear any indication that the package contains classified or protected ACM;
- be marked as follows:
  - full addresses of both the shipping and receiving COMSEC Accounts,
  - shipment number or authorized courier number, and
  - package number, followed by a forward slash (/), followed by the total number of the packages in the shipment (e.g. 1/3, 2/3, 3/3); and
- have all required customs documentation clearly identified and affixed to the wrapping.

10.7.4 Types of Packaging

10.7.4.1 Envelopes

Official double envelopes may be used for the shipment of ACM by mail or by courier. If the inner envelope contains cryptographic material (of any classification) or ACM classified SECRET or above, both the inner and outer envelope flap must be sealed with reinforced or tamper evident tape, in addition to the envelope gum seal.

If the inner envelope contains ACM classified CONFIDENTIAL or below, both the inner and outer envelopes require gum sealing only. However, envelopes should be sealed with reinforced or tamper evident tape if, in the opinion of the COMSEC Sub-Account Custodian, the envelopes may tear during transit.

10.7.4.2 Parcels

Good quality brown wrapping paper and fibre-reinforced paper tape should be used when preparing COMSEC parcels. Parcels must be packaged and bound as follows:

- all seams of the inner wrapping must be bound with fibre-reinforced paper tape;
- sharp corners must be reinforced or bound with cardboard to prevent damage to the inner wrapping while in transit; and
- outer wrapping must consist of paper and fibre-reinforced tape heavy enough to ensure a suitably sturdy parcel.

10.7.4.3 Cardboard Boxes

Cardboard boxes may be used as the inner or outer container for a shipment. Used boxes must be in good condition, with all previous markings obliterated. Additional packing must be used within the boxes to prevent movement of the contents. Fibre-reinforced paper tape must be used to seal all seams and to reinforce edges and corners.

10.7.4.4 Wooden Crates or Transit Cases

Wooden crates or transit cases should normally be used only as outer wrapping for shipments, except when specially designed and authorized to be used as inner wraps. The outer crate or case must be strapped with a minimum of one strap lengthwise and one widthwise, both centred. The clamp securing the strap running lengthwise must be positioned above the strap running widthwise.

10.7.4.5 Canvas Bags

A canvas bag may be used as the outer wrapping of a parcel. The bag must be sealed with a lever lock and a Plik seal. The identification number on each Plik seal is a tamper evident security control that must be used to detect unauthorized access to the bag.

The user must take note of the Plik seal's unique Identifier (ID) when using the Plik seal to secure the bag. Later, when the bag is to be opened, the user must verify that the Plik seal ID on the bag has not changed. This verification of the ID confirms that the bag has not been opened by anyone and then re-sealed using a different Plik seal. The seams of the bag must be on the inside. Damaged or repaired bags must not be used.

10.7.4.6 Briefcases

Within Canada, a briefcase with a GC-approved lock is an appropriate outer wrapper for ACM carried by authorized private sector company couriers. Refer to the RCMP G1-001 for details.

10.7.5 Controlled Cryptographic Items

CCIs must be prepared and packaged as follows:

- Unkeyed CCIs must be packaged for shipment in any manner that:
  - provides sufficient protection from damage, and
  - provides evidence of any attempt to penetrate the package while the material is in transit.

- In order to conceal the sensitive nature of the shipment, packages containing CCIs must not be externally marked as “CCI” or show the item description (nomenclature) of the equipment being shipped. For exterior container documentation purposes, CCIs are considered controlled and sensitive items.
- CCIs must only be shipped to authorized destinations. Packages must be addressed in a manner that will ensure delivery of the material to an organization with an individual designated to accept custody for it at the recipient destination. An individual’s name should not be used in the address; rather a functional designator should be used (e.g. an office symbol or an NCMCS COMSEC Account number).

10.8 Authorized Modes of Transportation

10.8.1 General

The approved modes of transportation for Canadian ACM are listed in Table 6.

10.8.2 North Atlantic Treaty Organization and Foreign Accountable COMSEC Material

The approved modes of transportation listed in this article do not apply to NATO or foreign classified ACM or unclassified key marked CRYPTO. This ACM must be transported in accordance with NATO and foreign national requirements.

NOTE: Contact CICA if there is a requirement to ship ACM to NATO or foreign entities.

10.8.3 UNCLASSIFIED, RESTRICTED and U/FOUO NATO and Foreign Accountable COMSEC Material (Other than Key Marked CRYPTO)

UNCLASSIFIED, RESTRICTED and U/FOUO NATO and foreign ACM (other than key marked CRYPTO) must be shipped by the modes listed in Table 6 as approved for PROTECTED A ACM of the same type. CCI, whether of foreign or national origin, must always be shipped by the approved modes listed in Table 6.

10.9 Segregation Requirements

10.9.1 General

To reduce the potential to compromise communication systems and cryptographic equipment, some types of ACM are never packaged or transmitted together. Separate packages in the same shipment (multiple package shipments) are not considered adequate segregation. ACM must be packed separately and sent in separate shipments unless specifically authorized by CICA. COMSEC Sub-Account Custodians must adhere to the following segregation regulations when packaging and transmitting ACM.

10.9.2 Key

Key **must not** be packaged or shipped with its associated cryptographic equipment, except for requirements identified in Article 10.4.

10.9.3 Keyed Cryptographic Equipment

Cryptographic equipment **must not** be packaged/shipped in a keyed state (key loaded into the equipment [with or without associated CIKs and PINs]) without authorization from CICA.

10.9.4 Documentation or Key Status Notifications

Documentation or key status notifications that reveal the effective date and time, and other pertinent information regarding key, must be packaged and shipped separate from other forms of ACM or correspondence.

10.9.5 Non-Accountable COMSEC Material

Non-accountable COMSEC material must be shipped by approved means commensurate with its classification.

When accountable and non-accountable COMSEC material is shipped in the same package, care must be taken to separately identify one from the other. Only ACM is to be listed on the enclosed *COMSEC Material Report*. A separate receipt must be included for the non-accountable COMSEC material.

10.10 Authorized Couriers of Accountable COMSEC Material

10.10.1 Private Sector Company Authorized Couriers

Appropriately cleared company personnel who have been authorized by CICA may be employed as couriers. Contact CICA for details on the requirements that must be met by personnel appointed as company couriers.

10.10.2 COMSEC Courier Certificate

The *COMSEC Courier Certificate* attests to all concerned individuals (e.g. air carrier security agents, customs officials) that the sealed container or package transported by the courier holds only official matter. Presentation of the *COMSEC Courier Certificate* should extend immunity from search or examination of the official material carried or escorted by the courier. When further verification is needed regarding the authenticity of a *COMSEC Courier Certificate*, the courier must direct the concerned individual to contact CICA.

10.10.3 Courier Instructions

The CSO must brief the courier and provide written instructions regarding his or her responsibilities to personally safeguard the ACM until the package has been delivered to, and signed for by, the authorized recipient. The courier instructions must accommodate, at a minimum, the following actions:

- before the start of the trip – contact with airline security or customs officials to make arrangements for clearance without inspection;
- during the pre-boarding security screening or customs inspection – ensure that the ACM is not compromised or damaged (e.g. requirement to show the *COMSEC Courier Certificate* when requested to do so by appropriate authorities);
- for alternate storage arrangements – who to contact in the event of emergency situations, lengthy delays or stopovers *en route*; and
- in the event of loss, compromise or possible compromise of ACM – who to contact in such a case.

10.11 Customs and Pre-Boarding Inspections

In cases where customs officials request or demand to view the contents of a COMSEC shipment, the authorized courier, or the COMSEC Sub-Account Custodian if called, must request an interview with the Chief of Customs or Air Transport Security Authority. The courier may agree to limited inspection as a means of assuring customs officials that the shipment contains nothing other than what is described on the documentation. Whenever COMSEC packages are subjected to increased scrutiny, the authorized courier will request that the inspection:

- take place in a private location;
- be conducted by duly authorized individuals in the presence of the authorized courier; and
- be restricted only to the external viewing of the ACM.

The courier may be obliged to discontinue the courier run and return to the point of departure with the ACM if an arrangement regarding the extent of customs clearance examination required cannot be reached.

NOTE: X-ray is authorized if requested or demanded.

10.12 Commercial Carriers

A commercial carrier service (including Canada Post Priority Courier Service) may be used as a courier service for ACM (at the levels specified in Table 6) provided the carrier can ensure a continuous chain of accountability and custody for the material while in transit.

The courier must offer speed of service (e.g. overnight delivery), physical protection and track-and-trace capabilities.

A commercial carrier may be used, if authorized by CICA, to transport CCI providing the carrier warrants, in writing, that the carrier:

- provides door-to-door service and guarantees delivery within a reasonable number of days based on the distance to be travelled;
- possesses a means of tracking individual packages within its system (i.e. manual or electronic) to the extent that should a package become lost, the carrier can, within 24 hours following notification, provide information regarding the last known location of the package(s);
- guarantees the integrity of package contents, including protection against damage, tampering and theft;
- has the capability to store in-transit COMSEC packages in a securely locked facility (e.g. security cage) that is accessible solely to authorized carrier personnel should it become necessary for the carrier to make a prolonged stop at a carrier terminal (during overnight stopovers);
- obtains manual or electronic signatures whenever a shipment changes hands within the carrier company; and
- obtains date-timed signatures upon pickup and delivery.

10.13 Receiving Accountable COMSEC Material

A shipment of ACM should arrive at the recipient, addressed by name, to the COMSEC Sub-Account Custodian and delivered unopened to that individual. If the outer wrapper/cover is inadvertently opened by company mail room personnel, but the inner wrapper/cover remains intact and there is no sign of tampering, it is not considered a COMSEC incident or security violation. However, the inadvertently opened outer wrapper/cover must be delivered to the COMSEC Sub-Account Custodian along with the parcel. Refer to Annex B for detailed instructions on the receipt of ACM.

Table 6 – Authorized Modes of Transportation for Accountable COMSEC Material

Destination	Classification or Protected Level of ACM (refer to the COMSEC Material Legend)				
	1, 2	3, 4, 5	6, 7	8	9
Within Canada	A, B, C (Notes I, II, IV)	A, B, C, D (Notes I, II, IV)	A, B, C, D, E, F (Notes I, II, IV)	A, B, D, E, F	A, B, C, D, E, F (Notes I, II)
Between Canadian addressees outside of Canada (see Note V)	A, B, C (Notes I, II, IV)	A, B, C, D (Notes I, II, IV)	A, B, C, D (Notes I, II, IV)	A, B, D, E, F	A, B, C, D, E, F (Notes I, II)
To or from Non-Canadian addressees (see Note VI)	A, B, C (Notes I, II, IV)	A, B, C, D (Notes I, II, III, IV)	A, B, C, D (Notes I, II, III, IV)	A, B, D, E	A, B, C, D (Notes I, II, III)

UNCLASSIFIED ACM may be shipped by any means intended to assure safe arrival at its destination.
UNCLASSIFIED ACM material marked with "CRYPTO" caveat must be shipped as per PROTECTED A (Note IV).

COMSEC Material Legend:	
1	All TOP SECRET and PROTECTED C ACM
2	All key not in protective packaging
3	Classified cryptographic information (not TOP SECRET)
4	Classified cryptographic equipment
5	SECRET key in protective packaging
6	PROTECTED B, CONFIDENTIAL and SECRET COMSEC information
7	CONFIDENTIAL and PROTECTED B key in protective packaging
8	UNCLASSIFIED CCI and UNCLASSIFIED cryptographic material
9	PROTECTED A ACM

Authorized Mode Legend:	
A	Canadian Government Diplomatic Courier Service
B	Authorized Departmental Couriers
C	Electronic transfer
D	Private sector company authorized couriers
E	Authorized commercial carriers
F	Canada Post Priority Courier Service

Notes:	
I	Systems for electronic transfer of ACM are authorized by CICA on a case-by-case basis.
II	Electronic transfer of key when authorized by CICA and in accordance with system operational doctrine.
III	Departmental and private sector company couriers authorized by CICA for urgent requirements only.
IV	NATO and foreign ACM (including cryptographic key) may require additional considerations – Contact CICA for instructions.
V	Refers to those addressees outside of Canada where mail and shipment of material, once delivered, are handled and opened by Canadian citizens (including dual nationality), e.g. Canadian Forces bases, Canadian embassies, consular offices – Contact CICA for instructions.
VI	Refers to any other foreign addressee not covered in Note V – Contact CICA for instructions.

Instructions: Locate the correct classification/protected level of the ACM from the COMSEC Material Legend. Find the destination in the upper left hand column. The authorized modes of transportation are indicated by letters, which correspond to letters listed in the Authorized Mode Legend. Refer to the notes for additional information.

11 Handling and Use of Accountable COMSEC Material

11.1 Cryptographic Key

11.1.1 Purpose and Use

Key must be used only for its intended purpose and only in the cryptographic equipment for which it was produced, unless otherwise directed by the Controlling Authority (CA) through CICA.

11.1.2 Key States (RED and BLACK)

Key is developed, distributed and handled in one of two states: RED (unencrypted) or BLACK (encrypted). RED key is accounted for in NCMCS and BLACK key is tracked outside of NCMCS.

11.1.3 Labels

Except for the labels affixed to protective packaging at a production facility, no other labels may be affixed to the protective packaging of any key unless authorized by COMSEC Client Services.

11.1.4 Protective Packaging

Some key are protectively packaged at the time of production and will not, in most cases, be opened until issued to a Loan Holder or authorized user. The protective packaging must be inspected for signs of tampering upon initial receipt, during inventory, before issue and before destruction of the sealed key.

NOTE 1: Protective packaging applied to individual TOP SECRET key must be removed under TPI controls.

NOTE 2: Protective packaging (e.g. key canisters) is not considered an inner wrapping (refer to Article 10.7.2).

11.1.4.1 Electronic Key on Magnetic or Optical Removable Storage Media

The COMSEC Sub-Account Custodian must ensure that the protective packaging of magnetic or optical RSM used for the distribution of electronic key is not opened until required for use.

11.1.4.2 Electronic Key on a Key Storage Device

The COMSEC Sub-Account Custodian must ensure that the protective packaging of electronic seed or operational key received on KSD is not opened until required for use. The label, normally attached to a KSD, bears information to identify the electronic key. The labelled KSD will be sealed in a plastic bag or in thermoplastic film.

11.1.5 Copies of Key

11.1.5.1 Operational Symmetric Key

Operational key may be copied, in whole or in part, as authorized by the CA and in accordance with equipment doctrine. The following rules apply:

- retain the short title of the key being copied;
- safeguard the copies according to their classification and CRYPTO caveat (if applicable);

- do not retain the copies beyond the destruction date for the key from which they were made (they may be destroyed before this date);
- destroy the copies before destroying the original key from which the copies were made; and
- locally account for the copies using a manual tracking system when equipment or system audit trails are not available.

11.1.5.2 Test Symmetric Key

Test key may be copied and accounted for within a COMSEC Account as ALC 4 or ALC 7. If the test key is transferred to another COMSEC Account, all copies must be destroyed.

11.1.5.3 Asymmetric Key

Copying of any asymmetric key is not permitted.

11.2 Cryptographic Equipment

11.2.1 Sight Verification

The COMSEC Sub-Account Custodian must verify the completeness of cryptographic equipment (classified or unclassified and CCI) upon initial receipt, during inventory and before issue.

11.2.2 Equipment Labels

The only approved labels that may be attached to cryptographic equipment or to its protective packaging are:

- a manufacturer label;
- an equipment nomenclature plate;
- a CCI label;
- one or more tamper-evident labels; and
- any other CSE-authorized labels.

An approved label must not be removed or covered by another label unless specifically authorized by CSE. Visible signs of label tampering must be reported as detailed in Article 16. If there is uncertainty as to whether a COMSEC incident has occurred, contact CICA for assistance.

11.2.3 Modification

Modification of any kind (includes labelling) to cryptographic equipment may only be made upon approval by CICA. Approved modifications to cryptographic equipment must be done by authorized and qualified personnel.

11.2.4 Cryptographic Equipment Installed for Operational Use

The COMSEC Sub-Account Custodian must ensure that:

- all users of the equipment have read and understood the equipment-specific doctrine;
- the equipment installed for operational use is protected based on the classification of the equipment or the key, whichever is higher; and

- authorized procedures have been put in place to prevent unauthorized use of the equipment or extraction of its key.

11.2.5 Classified Cryptographic Equipment – Keyed and Unattended

Keyed classified cryptographic equipment, in operation and unattended, may only be operated within a High Security Zone with the same supplemental controls as TOP SECRET key. TPI and NLZ controls are not required except when using TOP SECRET key.

11.2.6 Controlled Cryptographic Items

11.2.6.1 General

CCIs are by definition unclassified, but controlled. When keyed, a CCI takes on the classification of the key being used. Unless authorized by CICA (refer to Article 9.6.2), CCIs must be zeroized prior to storage or shipping.

Minimum controls for CCIs are prescribed under three different conditions:

- unkeyed
- installed and keyed with unclassified key, and
- keyed with classified or protected key.

The provisions below apply to CCIs that are installed for operational use. For detailed security instructions for CCIs, refer to the equipment-specific doctrine or contact CICA.

11.2.6.2 Unkeyed

The private sector company holding a CCI is responsible for providing procedural and physical controls adequately to prevent unauthorized removal of the CCI or its CCI components.

11.2.6.3 Installed and Keyed with Unclassified Key

- **Attended** – The private sector company is responsible for preventing access to CCIs by unauthorized personnel through the use of physical controls or monitoring access with authorized personnel; and
- **Unattended** – At a minimum, CCIs require operating from an Operation Zone. The private sector company is responsible for preventing access to the CCIs by unauthorized personnel through the use of adequate physical controls (e.g. locked rooms, alarms, or random checks).

11.2.6.4 Installed and Keyed with Classified or Protected Key

- **Attended** – Keyed CCIs must be under the continuous positive control of company personnel who possess a security clearance at least equal to the classification level of the key in use. If the key is TOP SECRET, the NLZ controls must be instituted unless the key is resident in the equipment in BLACK electronic form (e.g. SCIP devices) or where the equipment has been modified to preclude access by a lone individual to the key contained therein.
- **Unattended** – Keyed CCIs may only be operated from a High Security Zone with the same supplemental controls as for TOP SECRET keying. TPI and NLZ controls are not required except when using TOP SECRET key.

11.2.7 Key Storage and Fill Equipment Containing Key

11.2.7.1 Common Fill Devices Containing RED Key

Common Fill Devices (e.g. KYK-13) that store key in the RED state and provide no record of transactions must not be used for long term storage of key. Key may be held in this device no longer than 12 hours after the end of the applicable cryptoperiod. This type of device must be marked to show the highest classification of the key contained and must be kept under TPI controls whenever it holds TOP SECRET key.

11.2.7.2 Tier 3 Management Devices Containing BLACK Key

Tier 3 Management Devices (T3MDs) that store key in the BLACK state must be used as detailed in equipment-specific doctrine.

11.2.7.3 Magnetic or Optical Removable Storage Media Containing Key

Magnetic or optical RSM containing RED key must be returned to secure storage after the key or associated data has been loaded into the End Cryptographic Unit (ECU). RSM holding RED key must be marked to show the highest classification of the key held and, where applicable, must display the CRYPTO marking.

NOTE: RSMs includes CD-ROMs, DVDs and all other optical media, Universal Serial Bus (USB) flash drives, memory storage cards and all other magnetic media.

11.2.7.4 Re-Use of Non-Accountable Magnetic and Optical Removable Storage Media

A non-accountable RSM used in the transfer of BLACK key may be re-used once the BLACK key has been removed and once the RSM has been appropriately sanitized (refer to *Clearing and Declassifying Electronic Data Storage Device* [ITSG-06] for details on RSM declassifying and sanitization).

11.2.8 Equipment Audit Trails

11.2.8.1 Responsibility for Reviewing

Except for T3MD audit trails, which must be uploaded to CICA for review and retention, it is the responsibility of the COMSEC Sub-Account Custodian to ensure audit trails for CSE-approved cryptographic equipment are reviewed as specified in equipment-specific doctrine and as directed by CICA.

11.2.8.2 Reviewing Audit Trails

The individual authorized to review the audit trail data must:

- not be the primary cryptographic equipment user;
- meet the COMSEC access requirements discussed in Article 8.1;
- have sufficient knowledge about the use of the applicable cryptographic equipment and the key stored or filled in the cryptographic equipment;
- confirm that only authorized copies of key are made;
- be able to detect any anomalies in the audit trail data; and
- send a record of the outcome of the audit trail review to the COMSEC Sub-Account Custodian, who in turn must send a copy to CICA.

11.2.8.3 Retention of Audit Logs

Audit logs must be retained as detailed in Article 5.2.5, as detailed in the applicable equipment-specific doctrine if different from this directive, or as directed by CICA.

11.2.8.4 Retention of Records and Audit Trails

The COMSEC Sub-Account Custodian must retain a record of the completion of audit trail reviews until the COMSEC Sub-Account receives a *Periodic Inventory Reconciliation Notification* letter attesting that the account inventory has been reconciled.

11.3 COMSEC Publications

11.3.1 Reproduction

Accountable COMSEC publications must not be reproduced unless reproduction is authorized under a private sector contract procured through PSPC or by CICA. Refer to ITSD-08 for more information.

11.3.2 Page Checks

11.3.2.1 Requirement

The COMSEC Sub-Account Custodian (or other authorized individual) must conduct a page check of unsealed accountable COMSEC publications to ensure the presence of all required pages. To conduct the page check, the presence of each page must be verified against the "List of Effective Pages" or the "Handling Instructions", as appropriate.

NOTE: A page check must be completed on initial receipt of an Accountable COMSEC publication (this includes receipt by a Loan Holder and the COMSEC Sub-Account Custodian on return of a publication).

11.3.2.2 Frequency

Accountable COMSEC publications and amendments to accountable COMSEC publications must be page-checked:

- during each COMSEC Sub-Account inventory;
- upon receipt;
- before transfer and issue;
- before routine destruction;
- when an outgoing COMSEC Sub-Account Custodian is not available to complete an *Inventory Report*;

  NOTE: The incoming COMSEC Sub-Account Custodian and a witness must conduct a page check of all accountable COMSEC publications.

- at the time of the sight inventory and prior to the *Possession Report* being signed; and
- after posting any amendment (includes removal of pages or replacement of pages).

11.3.2.3 No Missing Pages

If there are no missing pages, the "Record of Page Checks" page must be signed and dated. If the accountable COMSEC publication has no "Record of Page Checks" page, the notation must be placed on the cover.

11.3.2.4 Missing Pages

If any pages are missing, the "Record of Page Checks" page must be annotated accordingly and a *COMSEC Incident Report* must be submitted as detailed in Article 16. When pages are missing upon initial receipt of an accountable COMSEC publication from a production facility, the COMSEC Sub-Account Custodian must notify the issuing authority and request disposition instructions (e.g. transfer back for replacement, destroy, use with missing page).

11.3.2.5 Duplicate Pages

In the case of duplicate pages, the COMSEC Sub-Account Custodian must prepare a *Possession Report* (GC-223) as detailed in Article 7 and notify CICA for disposition instructions of the duplicate page(s). The *Possession Report* must list the page number as part of the short title (e.g. AMSG 600, page 3) and list the accounting number assigned to the material. A notation of the duplicate page(s) and the resultant disposition of the duplicate page(s) must be entered on the "Record of Page Checks" page.

11.3.3 Amendments

11.3.3.1 Printed Amendments

The COMSEC Sub-Account Custodian must account for the printed amendment as an accountable COMSEC publication in accordance with its respective ALC until the printed amendment has been posted and the replaced information destroyed. Care should be taken when preparing the *Destruction Report* (GC-223) to ensure that the short title, edition and accounting number of the amendment are reported (rather than that of the publication). Printed amendments must be entered in sequence. If one is received and the previous amendment(s) have not been entered, they must be entered (or acquired and entered) before processing the latest amendment.

11.3.3.2 Posting Amendments

The following applies to the posting of amendments:

- the COMSEC Sub-Account Custodian (or other authorized individual) must post the amendment as soon as possible after its receipt (or effective date);
- personnel who are authorized to post amendments must be appropriately trained;
- specific instructions contained in the letter of promulgation or handling instructions must be read and understood before posting amendments;
- entire amendments must be posted at one time, and not extended over a period of time;
- if replacement pages are included in an amendment, page checks of both the publication and the information to be replaced must be made before destruction of the replaced pages. Inadvertent destruction of the effective portions of publications must be reported as a **COMSEC incident** as detailed in Article 16;
- personnel posting amendments must annotate the posting of the amendment on the "Record of Amendments". If pages were added to or removed from the publication, date and sign the "Record of Page Checks" page;

- personnel, other than the COMSEC Sub-Account Custodian, posting amendments must return all removed and/or replaced pages to the COMSEC Sub-Account Custodian for destruction;
- removed and/or replaced pages must be placed in a sealed envelope marked with the short title, accounting number and classification of the amendment;
- removed and/or replaced pages must be destroyed within five working days after entry of the amendment; and
- after an amendment has been completed, the publication must be page-checked by a member of the custodial staff other than the person who entered the amendment.

11.4 Local Tracking of Non-Accountable COMSEC Material

11.4.1 Local Tracking System

Certain material (e.g. CIKs, PINs, passwords, configuration disks) associated with cryptographic equipment that cannot be controlled within NCMCS must be controlled by the COMSEC Sub-Account Custodian through a local tracking and control system. Control and handling of this material must be as detailed in this directive, unless otherwise specified by the equipment-specific doctrine, the originating authority or CICA.

11.4.2 Cryptographic Ignition Keys

The COMSEC Sub-Account Custodian must locally track CIKs using a procedure that will minimize any potential for compromise associated with their use. Local tracking procedures for CIKs must include:

- maintaining a record of each CIK created, including the serial number of the CIK (if possible), the serial number of the associated equipment, location of the equipment, the date equipment was keyed, and the name of each Loan Holder authorized to use the CIK;
- ensuring each CIK is signed for and held by the Loan Holder to whom it has been issued and verifying, at least annually, that all Loan Holders still hold their CIK;
- shipping CIKs (separately from their associated equipment) in a COMSEC channel approved by CICA;
- providing adequate storage for a CIK when it is not held under the personal control of the Loan Holder;
- zeroizing or destroying CIKs that are no longer required; and
- developing procedures for detecting potential compromises.

11.4.3 Personal Identification Numbers and Passwords

When a written record or master list of PINs or passwords is required, the COMSEC Sub-Account Custodian must ensure:

- the record contains the name and telephone number of individual(s) having knowledge of the PIN or password, the serial number of the associated equipment, the location of the equipment, and the date the PIN or password was changed;
- the record of PINs or passwords is safeguarded as directed by its classification or the classification of the associated equipment, whichever is higher;
- access to individual PINs or passwords is restricted to the individual to whom it is assigned, unless an emergency situation dictates otherwise; and

- the record of PINs and passwords, or individual PINs and passwords, are distributed via COMSEC channels or via approved methods for classified material.

11.4.3.1 Personal Identification Numbers and Passwords Changes

The COMSEC Sub-Account Custodian must ensure that PINs and passwords for cryptographic equipment are changed as detailed in the equipment-specific doctrine. Where direction is not otherwise provided, the PIN or password must be changed when:

- the equipment is first put into use by the COMSEC Sub-Account Custodian;
- an individual knowing the PIN or password ceases to have authorized access to the equipment;
- an unauthorized individual has had access to the written record of the PIN or password;
- the PIN or password is known or suspected to have been compromised; and
- the PIN or password has not been changed in the last six months.

11.4.3.2 Personal Identification Numbers and Passwords Storage

When records of PINs or passwords, or a list of PINs and passwords, need to be maintained, they must be safeguarded and managed by an appropriate authority (CICA DCA or CICA COMSEC Custodian) who must mark and protect the list in accordance with the highest classification of the material being protected by the PIN or password.

11.4.4 Configuration Disks

The COMSEC Sub-Account Custodian must ensure the label on the equipment configuration disk identifies the equipment to which it belongs, the date it was created, and its classification. Local tracking must be established and include the recording of information on the label, the name of the individual responsible for the control of the disk and the location of the associated equipment.

11.4.5 Software Upgrades

All software upgrades must be approved by CICA. The COMSEC Sub-Account Custodian must control the equipment software upgrade process to ensure that all operational cryptographic equipment, including equipment held in reserve, are compatible. All mandatory upgrades must be completed by the date directed by CICA.

NOTE: The completion of mandatory software upgrades is auditable and must be reported to COMSEC Client Services.

12 Disposal of Accountable COMSEC Material

12.1 General Requirement

ACM must not be disposed of without specific authorization from CICA. Disposal of ACM may be accomplished in one of three ways: transfer, sale or destruction.

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.

12.2 Authorization

Except for removed and/or replaced pages, only key that is authorized for destruction through a CICA status letter is permitted to be destroyed by a private sector company. The authority for destruction must be quoted in COMSEC records and reports when destroying ACM.

12.3 Destruction of Key

12.3.1 General

Authorized destruction procedures, methods and devices must be used in the destruction of key. Private sector companies must establish procedures and provide the resources to conduct routine destruction of key, as detailed in this directive.

12.3.2 Unavailability of Destruction Devices

Key that cannot be zeroized or destroyed at a COMSEC Sub-Account due to unavailability of destruction devices must be returned to CICA for destruction.

12.3.3 Key Issued for Use

Superseded key, whether regularly or irregularly superseded, must always be destroyed within 12 hours of supersession except in the following circumstances:

- in the case of an extended holiday period or when special circumstances prevent compliance with the 12-hour rule (e.g. destruction facility not operational), key must be destroyed as soon as possible and should not be held longer than 72 hours following supersession;
- where authorized destruction devices are not available, superseded key must be destroyed as soon as practicable upon completion of operations;
- the destruction of KEK must be accomplished as soon as it is filled into the cryptographic equipment unless equipment-specific doctrine allows retention; or
- key involved in compromised situations must be destroyed within 72 hours after disposition instructions are received. In this situation, a *Destruction Report* must be sent to CICA immediately following destruction.

12.4 Destruction of Accountable Cryptographic Equipment, Publications, Removable Storage Media and Hardware Key

Under normal circumstances, accountable cryptographic equipment, publications, RSM and hardware key (e.g. Programmable Read-Only Memory [PROM], permuting plugs and their manufacturing aids) must be returned to the GC sponsor for disposal.

12.5 Performance of Routine Key Destruction

12.5.1 Personnel

12.5.1.1 COMSEC Sub-Account Custodian and Alternate Custodian

The COMSEC Sub-Account Custodian and the Alternate Custodian will normally perform routine destruction of key. However, granting the authority to destroy superseded key to other appropriately cleared and COMSEC-briefed individuals (who then verify the destruction to the COMSEC Sub-Account Custodian) is preferable to delaying destruction, even for a short time.

12.5.1.2 Loan Holder

The COMSEC Sub-Account Custodian may grant a Loan Holder authority to destroy key in the presence of an appropriately cleared and COMSEC-briefed witness, if an approved destruction device is available. If an approved destruction device is not available, the key must be returned to the COMSEC Sub-Account Custodian for destruction.

12.5.1.3 Witness

The destruction of key on physical media that does not provide for an audit trail must be completed in the presence of an authorized witness.

NOTE 1: Under no circumstances is a person permitted to sign as a witness without sighting the key that is identified.

NOTE 2: Care must be taken to ensure that only the key authorized for destruction is destroyed.

12.5.2 Authorized Personnel Requirements

The COMSEC Sub-Account Custodian must ensure that the individuals they authorize to destroy key:

- meet the requirements for access to ACM and are cleared to the highest level of key being destroyed; and
- are briefed on the correct destruction procedures.

12.5.3 Destruction Steps

The following steps must be carried out by the two authorized individuals when destroying key:

1. verify that the key to be destroyed is authorized for destruction (refer to Article 12.2) before listing the material on the *Destruction Report*;
2. list all material to be destroyed on the *Destruction Report* as detailed in Article 7.4.5. Use the (unsigned) *Destruction Report* (or HI/DR Card or other local destruction log) as a “check list” during the destruction process to ensure that the correct ACM will be destroyed;
3. immediately before destruction, verify the material being destroyed (short title, edition, accounting number, and quantity for each item) against the *Destruction Report* (or HI/DR Card or other local destruction log) ensuring that all accounting information is correct;
4. immediately destroy the material using approved destruction methods;
5. examine the destruction device and the surrounding area to ensure that all material has been destroyed;

6. thoroughly inspect the residue to ensure that the destruction was complete; and
7. sign and witness the *Destruction Report* (or HI/DR Card or other local destruction log) unless the equipment-specific doctrine states that a witness is not required. The *Destruction Report* must not be signed until the complete destruction of the listed material is confirmed.

12.6 Routine Destruction Methods

12.6.1 General

The destruction criteria listed in the following articles apply to accountable key.

NOTE: If there is any uncertainty as to whether or not a method for destruction of key will meet the minimum standards detailed below, contact CICA for guidance.

12.6.2 Incineration

The burning of paper key (e.g. key tape) must be complete (so that key tape is reduced to white ash) and contained (so that no unburned pieces escape). Ashes must be inspected and, if necessary, broken up.

12.6.3 Pulverizing, Chopping or Pulping

Pulverizing, chopping and pulping devices used to destroy paper key must reduce the key to bits no larger than five millimeters (⅕ inch) in any dimension.

12.6.4 Cross-Cut Shredding

Utilizing Type II shredders reduce material to shreds not more than 1.0 millimeters wide and 14.3 millimeters long is considered terminally destroyed (refer to the RCMP G1-001 for details).

12.6.5 Electronic Key

The destruction of electronic key is accomplished by zeroization or overwriting of the key.

For specific instructions on the destruction or zeroization of electronic key loaded in accountable COMSEC equipment, refer to the equipment-specific doctrine or contact CICA.

12.6.6 Plastic Canisters

Empty canisters must be fractured or smashed to ensure all key segments have been removed, and then disposed of as unclassified waste.

13 COMSEC Sub-Account Inventory

13.1 Reasons for Inventory

An inventory is the verification of a COMSEC Sub-Account's holdings. CICA maintains a database that reflects all ALC 1, ALC 2, ALC 4, ALC 6 and ALC 7 ACM charged to the COMSEC Sub-Account. The data is taken from *COMSEC Material Reports* (e.g. *Destruction Reports* and *Possession Reports*) that a COMSEC Sub-Account submits to CICA. *COMSEC Material Reports* that were processed by the Sub-Account but were not entered in CICA database will result in a discrepancy between CICA database and the COMSEC Sub-Account records.

Inventories serve to ensure that:

- COMSEC Sub-Account records are up-to-date;
- CICA database is up-to-date by verifying that all *COMSEC Material Reports* have been forwarded to CICA and have been processed by CICA;
- ACM charged to a COMSEC Sub-Account is actually on-hand and sighted by authorized personnel; and
- ACM charged to a COMSEC Sub-Account is still required for use by the account.

13.2 Types of Inventory

13.2.1 Periodic Inventory

The COMSEC Sub-Account Custodian and the Alternate Custodian must conduct periodic (minimally every 18 months) sight inventory of all ACM in their COMSEC Sub-Account (including all Loan Holders holdings).

CICA will send to the COMSEC Sub-Account Custodian an *Inventory Report* (GC-223) that lists all ACM charged to that COMSEC Sub-Account as of the date of printing. The COMSEC Sub-Account Custodian and the Alternate Custodian must then conduct a sight inventory to verify the presence of all material listed on the report (refer to Article 13.3.3 for material not listed) and return the signed *Inventory Report* to CICA no later than 10 working days after the initial receipt of that report.

13.2.2 Change of COMSEC Sub-Account Custodian Inventory

When a COMSEC Sub-Account Custodian departs, either indefinitely or permanently, the newly appointed COMSEC Sub-Account Custodian must conduct a sight inventory of all ACM in the COMSEC Sub-Account before the formal COMSEC Sub-Account Custodian handover.

Upon completion of the inventory, the new COMSEC Sub-Account Custodian must sign the *Inventory Report* as the COMSEC Sub-Account Custodian. The new COMSEC Sub-Account Custodian, except for discrepancies being resolved, assumes responsibility for all ACM in the account.

13.2.3 Special Inventory

The COMSEC Sub-Account Custodian must complete a special inventory when directed to do so by CICA. Special inventories may be requested for reasons such as the suspected loss of ACM or frequent deviations from accounting procedures.

The procedures used for a periodic inventory (sometimes called an annual inventory in other documentation) must be used for a special inventory.

13.3 Inventory Reports

13.3.1 Initial Inventory Report

Initial Inventory Reports are distributed by CICA to all COMSEC Sub-Accounts to announce the beginning of the inventory process. Each *Inventory Report* lists all ALC 1, ALC 2, ALC 4, ALC 6 and ALC 7 ACM that have been recorded in the CICA database for the respective COMSEC Sub-Account as of the date of the printing of the *Inventory Report*.

13.3.2 COMSEC Sub-Account Inventory Report

Inventory Reports produced by the COMSEC Sub-Account Custodian may be directed at two different audiences:

- within the COMSEC Sub-Account, where they may be distributed for use during the physical sighting of on-hand material; and
- CICA, in order to report the complete holdings of the COMSEC Sub-Account.

13.3.2.1 Report Distribution within the COMSEC Sub-Account

The COMSEC Sub-Account Custodian prepares *Inventory Reports* for internal distribution to Loan Holders. These *Inventory Reports* list all ALC 1, ALC 2, ALC 4, ALC 6 and ALC 7 ACM that the COMSEC Sub-Account Custodian has issued to Loan Holders within the COMSEC Sub-Account and the ones that are still out on loan.

13.3.2.2 Report Distribution to CSE Industrial COMSEC Account

The COMSEC Sub-Account Custodian compiles the results of all *Inventory Reports* that were distributed within the Sub-Account and returns an *Inventory Report* to CICA. This report contains all ALC 1, ALC 2, ALC 4, ALC 6 and ALC 7 ACM held by the COMSEC Sub-Account.

13.3.3 Amendment to Inventory Report

The *Amendment to Inventory Report* (GC-223) is used to report any discrepancies between the COMSEC Sub-Account's inventory and the initial *Inventory Report* distributed by CICA. For example, if the COMSEC Sub-Account failed to submit a *Destruction Report* to CICA, all the material destroyed by the COMSEC Sub-Account that was listed on that *Destruction Report* would not be recorded in the CICA database.

Consequently, the *Inventory Report* initiated by CICA would list that material as being on hand at the COMSEC Sub-Account. An *Amendment to Inventory Report* would provide the details of the missing *Destruction Report*.

When submitting an *Amendment to Inventory Report*, the COMSEC Sub-Account Custodian must attach all supplemental accounting reports in order for CICA to proceed with the inventory reconciliation.

13.4 Inventory Conduct

13.4.1 General

The COMSEC Sub-Account Custodian must ensure that a sight inventory of the entire COMSEC Sub-Account holdings is carried out during an inventory. Before the expected receipt of the initial *Periodic Inventory Report* distributed by CICA, the COMSEC Sub-Account Custodian must:

- generate a COMSEC Sub-Account *Inventory Report*;
- conduct a sight inventory of ACM that has been issued to Loan Holders or direct the Loan Holders to do so with an appropriate witness; and
- conduct a sight inventory of the COMSEC material on-hand, under the direct custody of the COMSEC Sub-Account Custodian.

13.4.2 Sight Inventory

The COMSEC Sub-Account Custodian will provide an *Inventory Report* for personnel conducting a sight inventory of ACM. The following applies when conducting a sight inventory of ACM:

- the sight inventory must be conducted by two authorized individuals who meet the requirements for access to ACM (refer to Article 8);
- the two individuals must verify that the ACM on-hand agrees with the COMSEC Sub-Account *Inventory Report*;
- unsealed COMSEC publications must be page-checked;
- cryptographic equipment in use does not need to be opened to verify it contains all the required subassemblies and elements;
- removable assemblies that are listed separately on an inventory report and are not listed on the equipment's chassis must be physically sighted unless the equipment is undergoing tests or is in operation; and
- electronic key stored in equipment that has a verifiable audit trail may be inventoried without a witness.

13.4.3 Reconciling the COMSEC Sub-Account Inventory Report

13.4.3.1 Loan Holder Inventory Reconciliation

Persons conducting Loan Holder inventories may markup the *Inventory Report* to indicate that material is on-hand, or, conversely, that it is lost, missing or contains extra material. They must both sign the *Inventory Report* before returning it to the COMSEC Sub-Account Custodian.

The COMSEC Sub-Account Custodian must reconcile the *Inventory Reports* returned from all Loan Holders with the COMSEC Sub-Account *Inventory Report*.

13.4.3.2 COMSEC Sub-Account Inventory Reconciliation

The COMSEC Sub-Account Custodian must return his or her signed *Inventory Reports* to CICA for reconciliation. If discrepancies are noted in any COMSEC Sub-Account *Inventory Report*, CICA must direct the Custodian of that COMSEC Sub-Account to take corrective action within 48 hours of receipt of such notice, advise CICA of the action taken and submit any substantiating reports required. CICA must reconcile all *Inventory Reports*.

13.4.4 Completion and Submission of Inventory Reports and Supplements

Upon completion of the COMSEC Sub-Account inventory, the COMSEC Sub-Account Custodian and the witness must sign and date the *Inventory Report*. The number of supplemental accounting reports and pages of amendments must be entered on the last page of the *Inventory Report*.

The *Inventory Report* and the *Amendment to Inventory Report* with all supplemental *COMSEC Material Reports* (if required) must be sent to CICA no later than 10 working days after receipt of the initial *Inventory Report* distributed by CICA. A signed copy of the *Inventory Report* must be retained on file.

13.4.5 CICA Reconciliation of a COMSEC Sub-Account Inventory Report

CICA will process *Inventory Reports* submitted by a COMSEC Sub-Account.

If CICA notifies a COMSEC Sub-Account of discrepancies between the COMSEC Sub-Account's *Inventory Report* and CICA's *Inventory Report*, the COMSEC Sub-Account Custodian must attempt to resolve the discrepancies.

If the discrepancies are the result of missing *COMSEC Material Reports*, the COMSEC Sub-Account Custodian must prepare and submit, within 48 hours, an *Amendment to Inventory Report* with all supplemental *COMSEC Material Reports* to update CICA database.

If the sight inventory of the COMSEC Sub-Account is correct, and there are no missing *COMSEC Material Reports*, CICA will issue an *Inventory Reconciliation Report*, which certifies the inventory as being correct.

If the sight inventory reveals lost or missing ACM or other discrepancies, a COMSEC incident must be reported as detailed in Article 16. An *Inventory Reconciliation Report* will not be issued until all discrepancies have been resolved or an investigation into the incident has been completed and disposal instructions issued.

14 COMSEC Emergency Protection Planning

14.1 Requirement

Every private sector company that holds ACM must prepare and maintain a current, documented *COMSEC Emergency Plan* for the protection and positive control of ACM appropriate for:

- natural disasters or accidental emergencies likely to occur in their location (e.g. hurricanes, tornadoes, earthquakes, floods or fires). Consideration must be given to incorporating this plan into the *Business Continuity Plan* established for the entire private sector company. Procedures must emphasize maintaining security control over the ACM until order is restored without endangering life; and
- high risk environments (e.g. those with potential or imminent hostile situations). *COMSEC Emergency Plans* in high risk environments must include *Emergency Destruction Procedures*. Procedures must emphasize maintaining security control over the ACM until order is restored without endangering life.

14.2 Planning for Natural Disasters and Emergencies

Planning must provide for:

- safety of all personnel;
- assignment of on scene responsibility for ensuring the protection and positive control of all ACM;
- protection or removal of ACM in the event that the admission of unauthorized individuals into the secure area(s) becomes necessary;
- evacuation of the area(s);
- assessment and reporting of the probable exposure of ACM to unauthorized individuals during the emergency;
- post-emergency inventory of ACM and reporting of the loss or unauthorized exposure of ACM to the CSO, CICA, and the CICA DCA;

- identification of primary and secondary recovery sites, when recovery will not be possible at the current location;
- identification of critical resources required to support the recovery;
- off-site storage facilities; and
- business continuity during and business resumption following the emergency event.

14.3 The Emergency Plan

14.3.1 Development

The CSO, in coordination with the COMSEC Sub-Account Custodian, is responsible for the preparation, implementation and annual re-evaluation of the *COMSEC Emergency Plan*. Coordination with appropriate security, fire and safety personnel will ensure that the plan is realistic and workable, and accomplishes the goals for which it is prepared. The duties under the plan must be clearly described and the contact information for all individuals with duties under the plan must be documented. Refer to the *COMSEC Emergency Plan Template* for an outline of the *COMSEC Emergency Plan*, including emergency destruction priorities.

14.3.2 Maintaining and Testing the Plan

The COMSEC Sub-Account Custodian must ensure that:

- all individuals that are responsible for the safeguard and control of ACM are aware of the existence of the plan and how alerts and warnings to an emergency event will be communicated;
- each individual who has duties assigned under the plan receives detailed instructions on how to carry out these duties when the plan is put into effect;
- all individuals are familiar with all duties, so changes in assignment can be made if necessary;
- training exercises are conducted periodically, to ensure that all personnel (especially new personnel) can carry out their duties; and
- the plan is revised (if necessary) based on experience gained in the training exercises.

14.4 Planning for Emergency Events

14.4.1 COMSEC Sub-Accounts Operating in Normal Conditions

The COMSEC Sub-Account Custodian must organize normal operating routines such that the number and complexity of the activities that must be taken during an emergency are minimized. The COMSEC Sub-Account Custodian must ensure that:

- only the minimum amount of ACM necessary for operational and contingency requirements are held by the COMSEC Sub-Account (refer to Table 5);
- ACM is stored in a manner that will facilitate emergency evacuation or destruction;
- routine destruction is always conducted promptly upon authorization; and
- excess ACM is promptly disposed of in accordance with any disposition instructions.

15 COMSEC Sub-Account Audit

15.1 Planning the Audit

15.1.1 Purpose of an Audit

A COMSEC audit provides an independent review of a COMSEC Sub-Account's records and activities to ensure ACM produced by or entrusted to the COMSEC Sub-Account is controlled as detailed in this directive.

15.1.2 Frequency of Audits

One CICA designated representative/auditor (or two) will normally audit each COMSEC Sub-Account at least once every 18 months (refer to ITSD-08 for frequency of IP audits). Audits may be conducted more or less frequently based on:

- previous audit findings;
- size of the COMSEC Sub-Account inventory;
- volume of *COMSEC Material Reports*;
- frequency of deviations from COMSEC directives;
- abnormal number of COMSEC Sub-Account Custodian changes; or
- type of automated accounting system in use at the COMSEC Sub-Account.

15.1.3 Scheduling the Audit

CICA will normally provide three weeks advance notice of an impending audit. However, the audit may occur on short notice when irregularities of a serious nature have occurred. The CICA designated representative/auditor conducting the audit will:

- contact the COMSEC Sub-Account Custodian (usually via a telephone call or e-mail) to schedule the audit;
- confirm the date and time of the audit, in writing; and
- provide an audit check list that will be used as a guide during the audit.

15.2 Conducting the Audit

15.2.1 Access to COMSEC Sub-Account Holdings

The CICA designated representative/auditor is authorized to have supervised access to all COMSEC Sub-Account reports, records and files, including electronic files and databases, upon presentation of his or her CSE identification badge and copy of his or her *COMSEC Briefing Certificate.*

NOTE 1: The CICA representative does not require a *COMSEC Visit Authorization*; however, CICA will provide visitor information as detailed in Article 8.5.

NOTE 2: The CICA representative may require supervised access to Loan Holder sites. Loan Holder audits must be coordinated by the COMSEC Sub-Account Custodian.

15.2.2 Scope of the Audit

The audit must be sufficient in scope to determine the accuracy of COMSEC Sub-Account accounting records and to confirm that ACM control procedures have been, and continue to be, correctly applied. The audit includes:

- verification that accounting reports, records and files are complete and accurate;
- verification of compliance with packaging, marking and distribution procedures;
- verification of the consistent application of procedures and processes (including physical security) related to the control, storage and use of ACM;
- assessment of the adequacy of automated accounting system controls;
- a detailed audit of IP accounting records, if applicable;
- verification of the completion of Loan Holder audits, if applicable; and
- discussion with the COMSEC Sub-Account Custodian regarding any problems encountered with the control of ACM or maintenance of the COMSEC Sub-Account.

15.2.3 Exit Interview

Upon conclusion of the COMSEC Sub-Account audit, the CICA representative will hold an exit interview with the CSO and the COMSEC Sub-Account Custodian to advise them of any situations that require immediate corrective action(s) and to brief them on the audit findings and recommendations.

NOTE: Both the CSO and COMSEC Sub-Account Custodian need to be available for the exit interview. If they are not available at the same time, the CICA representative will reschedule the exit interview.

15.3 Audit Reporting

15.3.1 COMSEC Sub-Account Audit Report

The COMSEC Sub-Account Audit Report will document all observations, recommendations and required corrective actions. CICA will provide the CSO with a copy of the COMSEC Sub-Account *Audit Report* within 15 working days of audit completion. If corrective actions are required, a SOA form will be included with the COMSEC Sub-Account *Audit Report*.

15.3.2 Statement of Action Form

The COMSEC Sub-Account Custodian must complete the corrective actions stated in the COMSEC Sub-Account *Audit Report* and return a signed SOA form to CICA within ten working days of receipt of the COMSEC

Sub-Account *Audit Report*. If due to operational requirements, the required corrective actions cannot be completed before the due date, CICA may grant an extension to this period.

15.3.3 Failure to Return a Statement of Action Form

CICA will send a tracer notice to the CSO if the signed SOA form is not received when due. If a signed SOA form is not returned to CICA at the end of an additional 10 working days following dispatch of the initial tracer notice, a second tracer notice will be sent by CICA to the CICA DCA and a copy to the CSO and COMSEC Sub-Account Custodian. After another five working days, following the second tracer, if the signed SOA form has not yet been received by CICA, the matter must be treated as a **COMSEC incident** and forwarded to the National COMSEC Incidents Office (NCIO) for action.

16 COMSEC Incidents

16.1 General

A COMSEC incident occurs whenever there is a situation or activity that jeopardizes the confidentiality, integrity or availability of COMSEC information, material or services.

Prompt and accurate reporting of COMSEC incidents (e.g. Loan Holder – COMSEC Sub-Account Custodian – CSO – CICA – CICA DCA – NCIO) minimizes the potential for compromise of ACM and the classified information that it protects. Unless all personnel who handle or manage ACM immediately report all COMSEC incidents (real or suspected) corrective action cannot be implemented in a timely manner.

Evidence of a COMSEC incident must be reported immediately to CICA.

The reporting of COMSEC incidents involving ACM includes those related to IP COMSEC material management (refer to ITSD-08).

Article 16.8 provides examples of COMSEC incidents that commonly occur.

16.2 Handling of Incidents

16.2.1 Identification and Response Procedures

The CSO must establish internal COMSEC incident identification and response procedures that will ensure prompt and accurate reporting of COMSEC incidents and minimize the potential for or actual loss or compromise of ACM.

The COMSEC Sub-Account Custodian must ensure that each individual who uses, or otherwise has access to ACM is capable of recognizing a COMSEC incident and understands the requirements for immediately reporting a COMSEC incident.

16.2.2 COMSEC Sub-Account Custodian Responsibility

When ACM is actually or potentially compromised, the COMSEC Sub-Account Custodian must take the following steps:

1. immediately report the circumstances to the CSO, who in turn must immediately report the incident to CICA;
2. mark all items of the affected ACM as “Pending Investigation” in the COMSEC material inventory file; and

3. maintain accountability for the ACM until the COMSEC investigation is complete and a *Final Assessment and Closure Report* has been received from CICA authorizing the disposition of the ACM (e.g. returned to CICA for evaluation, destruction and relief from accountability for lost item).

16.3 COMSEC Incident Initial Report

The *COMSEC Incident Initial Report* is used to report COMSEC incident and can be submitted to CICA by secure telephone or secure fax machine (refer to Article 1.12). If a secure telephone or fax machine is not available, arrangements must be made with CICA for delivery of the report by the most expedient route possible. A formal written report may also be requested by CICA to clarify details.

Upon receipt of an *Initial COMSEC Incident Report*, CICA will assess the security classification of future reporting and additional information and reporting requirements required to satisfy NCIO and ACMCA obligations.

16.4 COMSEC Incident Evaluation Report

A *COMSEC Incident Evaluation Report* (refer to ITSD-05) provides details surrounding a COMSEC incident and helps in finalizing impact assessment and recovery requirements.

Once the CICA *COMSEC Incident Initial Report* has been reviewed, CICA will request, except for very minor cases, a *COMSEC Incident Evaluation Report*. The request will include the requirement to provide:

- a detailed chronological account of the nature and circumstances of the incident;
- amplification of details provided in the *COMSEC Incident Initial Report*; and
- a description of corrective actions taken to limit damage resulting from the incident and to prevent recurrence of the incident.

16.5 Amplifying Report

An amplifying report is required whenever new information is discovered that may influence or change a previous *COMSEC Incident Evaluation Report*, or whenever requested by the CICA.

16.6 Final Assessment and Closure Report

Following the collection and assessment of all information received or available from existing records, the NCIO will issue a *COMSEC Incident Final Assessment and Closure Report* to the CICA DCA. CICA will then finalize the COMSEC incident with the private sector company CSO. The final report will include direction on how to prevent or reduce the possibility of the recurrence of a similar incident. It will also provide disposition instructions for the affected ACM. CICA will verify that the report's recommendations have been implemented.

16.7 Report Classification and Dissemination

16.7.1 Classification

A *COMSEC Incident Report* must be protected, handled and reported at a level of classification commensurate with that of the ACM exposed, lost or compromised in the incident, but never less than PROTECTED B. The following additional rules apply:

- when deemed necessary, the CSO may classify a *COMSEC Incident Report* at a higher level than the compromised material;
- a *COMSEC Incident Initial Report* involving ACM of different levels of sensitivity must be protected, handled and reported at the most sensitive level applicable to the incident; and
- in a case where the ACM relates to IT systems processing information at a classification level greater than that of the ACM, the incident must be handled and reported at the greater classification level (e.g. an incident involving a PROTECTED A authentication key used on an IT system processing SECRET information will be protected and reported at the SECRET level).

16.7.2 Dissemination

Dissemination of reports or information relevant to a COMSEC incident must be limited to those with a clear need-to-know and a security clearance commensurate with the classification of the information provided. Although information collected by CICA will be kept as Commercial Confidence (with personal information protected as detailed in the *Privacy Act*), CICA may be obligated to share information with the sponsoring GC department, PSPC or others, as determined by the CGP or ITAR.

16.8 Examples of COMSEC Incidents

The following list provides examples (not meant to be all inclusive) of COMSEC incidents reportable to CICA.

- premature or out-of-sequence use of key without the approval of the cryptonet CA;
- inadvertent destruction of key without authorization;
- removing key from its manufacturer's protective packaging prior to issue for use, or removing the protective packaging without authorization;
- failure to zeroize key from a Common Fill Device (CFD) or T3MD within the time limits permitted (refer to equipment-specific doctrine or contact CICA for guidance);
- destruction of ACM not performed within required time limits;
- failure to upload T3MD audit trail data;
- the use of key which is compromised, superseded, defective, previously used (and not authorized for reuse) or incorrectly used. For example:
  - unauthorized use of key for other than its intended purpose;
  - unauthorized extension of a cryptoperiod (refer to ITSD-04);
  - unauthorized use of ACM; and
  - premature use of key;
- the use of CSE-approved cryptographic systems, equipment and software, and operational practices or maintenance practices which are not approved by CSE. For example:
  - the maintenance of cryptographic equipment by unauthorized or unqualified individuals; and
  - tampering with, or unauthorized modification of a cryptographic component, equipment or system;

- the operational use of cryptographic equipment having defective cryptographic logic circuitry or use of an unapproved operating procedure;
- discussion via non-secure communications of the details of a cryptographic equipment failure or malfunction;
- any unauthorized use of key or CSE-approved cryptographic equipment;
- failure to maintain required TPI or NLZ controls for TOP SECRET key;
- receipt of classified equipment, CCI or key marked 'CRYPTO' with a damaged inner wrapper;
- destruction of ACM by other than authorized means;
- actual or attempted unauthorized cryptographic equipment maintenance (including maintenance by unqualified individuals) or the use of a maintenance procedure that deviates from established directives;
- known or suspected tampering with or penetration of ACM including, but not limited to, ACM received in protective packaging which shows evidence of tampering and unauthorized premature opening;
- unauthorized copying, reproducing or photographing of ACM;
- loss of ACM;
- discovery of ACM outside of required accountability and physical control including;
    - ACM reflected on a *Destruction Report* as having been destroyed and witnessed, but found not completely destroyed; and
    - ACM left unsecured and unattended where unauthorized individuals could have had access, and
- ACM improperly packaged or shipped.

17 References

17.1 List of Abbreviations and Acronyms

ACM	Accountable COMSEC Material
ACMCA	Accountable COMSEC Material Control Agreement
ALC	Accounting Legend Code
CA	Controlling Authority
CCD	Canadian Cryptographic Doctrine
CCF	Canadian Central Facility
CCI	Controlled Cryptographic Item
CD	Compact Disk
CEO	Chief Executive Officer
CEPA	COMSEC Equipment Purchase Authorization
CER	COMSEC Equipment Requirements
CFD	Common Fill Device
CGP	Controlled Goods Program
CGR	*Controlled Goods Regulations*
CICA	CSE Industrial COMSEC Account
CIK	Cryptographic Ignition Key
CISD	Canadian Industrial Security Directorate
CKL	Compromised Key List
CMAC	Crypto Material Assistance Centre
COMSEC	Communications Security
ConAuth	Controlling Authority
CONOP	Concept of Operations
Cryptonet	Cryptographic Network
CSI	COMSEC Safeguarding Inspection
CSE	Communications Security Establishment
CSEC	Communications Security Establishment Canada
CSO	Company Security Officer
DCA	Departmental COMSEC Authority
DCITS	Deputy Chief Information Technology Security
DDSM	*Directive on Department Security Management*
DoS	Department of State
DSC	Document Safeguarding Capability
DSO	Departmental Security Officer
ESO	Enterprise Security Officer
FAA	*Financial Administration Act*
FOCI	Foreign Ownership, Control or Influence
FSC	Facility Security Clearance

GC	Government of Canada
GC EKMS	Government of Canada Electronic Key Management System
GFE	Government Furnished Equipment
HI/DR	Handling Instructions/Disposition Record
IC	Integrated Circuit
ICMCM	*Industrial COMSEC Material Control Manual*
ID	Identifier
IISD	International Industrial Security Directorate
IP	In-Process
ISM	*Industrial Security Manual*
ISP	Industrial Security Program
ISS	Industrial Security Sector
IT	Information Technology
ITAR	*International Traffic in Arms Regulations*
ITSA	Information Technology Security Alert
ITSB	Information Technology Security Bulletin
ITSD	Information Technology Security Directive
ITSLC	Information Technology Security Learning Centre
KEK	Key Encryption Key
KMID	Key Material Identifier
KMSP	Key Material Support Plan
KP	Key Processor
KSD	Key Storage Device
KSO	Key Senior Official
LOA	Letter of Agreement
MITS	*Management of IT Security*
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCER	National Cryptographic Equipment Reserve
NCIO	National COMSEC Incidents Office
NCMCS	National COMSEC Material Control System
NCOR	National Central Office of Record
NDA	National Distribution Authority
NLZ	No-Lone Zone
ORR	Operational Rekey Report
PGS	*Policy on Government Security*
PIN	Personal Identification Number
PMO	Project Management Office
PROM	Programmable Read-Only Memory
PSI	Project Security Instruction
PSPC	Public Services and Procurement Canada
PSTN	Public Switched Telephone Network

PWA	Printed Wiring Assembly
RCMP	Royal Canadian Mounted Police
RFP	Request for Proposal
RSM	Removable Storage Media
R&M	Repair and Maintenance
SCIP	Secure Communication Interoperability Protocol
SDNS	Secure Data Network System
SKCR	Seed Key Conversion Report
SOA	Statement of Action
SPIRS	SNDS PSTN-ISDN Rekey Subsystem
SRCL	Security Requirements Check List
T3MD	Tier 3 Management Device
TAA	Technical Assistance Agreement
TBS	Treasury Board of Canada Secretariat
TEK	Traffic Encryption Key
TPI	Two-Person Integrity
TRA	Threat and Risk Assessment
U/FOUO	UNCLASSIFIED/For Official Use Only
UK	United Kingdom
ULC	Underwriters Laboratories of Canada
U.S.	United States
USML	United States Munitions List

17.2 Glossary

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

Accountability	The responsibility of an individual for the safeguard and control of COMSEC material which has been entrusted to his or her custody.
Accountable COMSEC Material (ACM)	COMSEC material that requires control and accountability within the NCMCS in accordance with its accounting legend code and for which transfer or disclosure could be detrimental to the national security of Canada.
Accounting Legend Code (ALC)	A numeric code used to indicate the minimum accounting controls for COMSEC material within the NCMCS.
Accountable COMSEC Material Control Agreement (ACMCA)	A binding agreement between CSE and an entity (Government or Canadian private sector) not listed in Schedules I, I.1, II, IV and V of the FAA that will permit the acquisition, accounting, control, management and final disposition of communications security material.

Accounting Legend Code 1 (ALC 1)	A numeric code assigned to physical and electronic ACM that is subject to continuous accountability by serial or register number to NCOR/COR within NCMCS.
Accounting Legend Code 2 (ALC 2)	A numeric code assigned to physical ACM that is subject to continuous accountability by quantity to NCOR/COR within NCMCS.
Accounting Legend Code 4 (ALC 4)	A numeric code assigned to physical ACM and traditional key in electronic format that, following initial receipt, is locally accountable by serial or register number to the responsible COMSEC Account within the NCMCS.
Accounting legend Code 6 (ALC 6)	A numeric code assigned to electronic key that is subject to continuous accountability by register number(s) to NCOR/COR within NCMCS.
Accounting Legend Code 7 (ALC 7)	A numeric code assigned to electronic key that, following initial receipt, is subject to local accountability by register number(s) to the responsible COMSEC Account within NCMCS.
Authorized User	For the purpose of this directive, an authorized user is an individual (other than the Custodian, Alternate Custodian or Loan Holder), who is required to use COMSEC material in the performance of assigned duties.
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 is accountable to the ISP and to the private sector company's designated KSO on all industrial security matters.
Compromise	The unauthorized access to, disclosure, destruction, removal, modification, use or interruption of assets or information.
COMSEC Incident	Any occurrence that jeopardizes or potentially jeopardizes the security of classified or protected GC 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.
COMSEC Sub-Account	An administrative entity, identified by an account number, established by a COMSEC Account to assist in the control of the COMSEC material produced by or entrusted to the COMSEC Account.
COMSEC Sub-Account Custodian	The individual designated by the DCA to be responsible for the receipt, storage, access, distribution, accounting, disposal and destruction of all COMSEC material that has been charged to the COMSEC Sub-Account.
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 the National COMSEC Material Control System and marked “CONTROLLED CRYPTOGRAPHIC ITEM” or, where space is limited, “CCI”.
COMSEC Courier Certificate	A certificate that authorizes an individual to transport classified or protected information and assets.
Controlling Authority (CA)	The entity designated to manage the operational use and control of key assigned to a cryptographic network.
CRYPTO	A marking which is applied to key or other accountable COMSEC material indicating that items so marked are subject to specific controls governing access, distribution, storage, accounting, disposal and destruction (see Cryptographic).
Cryptographic	Pertaining to or concerned with cryptography. **NOTE:** Often abbreviated as “crypto” and used as a prefix, e.g. cryptonet.
Cryptographic Equipment	Equipment that performs encryption, decryption, authentication or key generation functions.
Cryptographic Ignition Key (CIK)	A device or electronic key that can be used to access the secure mode of cryptographic equipment.

Cryptographic Key	A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature validation.
Cryptographic Material	All material, including documents, devices and equipment, which contain cryptographic information and is essential to the encryption, decryption or authentication of communications.
Cryptographic Network (Cryptonet)	Two or more pieces of cryptographic equipment connected together that utilize cryptographic key for the protection of information.
Cryptoperiod	A specific length of time during which a cryptographic key is in effect.
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 PGS and its related policy instruments for the management of ACM.
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 PGS and its standards.
Departmental Security Officer (DSO)	The individual responsible for developing, implementing, maintaining, coordinating and monitoring a departmental security program consistent with the PGS and its standards.
Government of Canada (GC) Sponsor	A GC department that has agreed to sponsor a private sector company to have access to or receive (for use), manufacture, reproduce or repair ACM.
In-Process (IP) COMSEC Material	COMSEC material being developed, produced, manufactured or repaired. See COMSEC Material.
Issue	The process of distributing COMSEC material from a COMSEC Account to its COMSEC Sub-Account(s) or Loan Holder(s).
Local Accounting	The process by which a COMSEC Custodian records and controls, in the NCMCS, COMSEC material that is not reportable to the NCOR/COR.
Loan Holder	An individual registered at a COMSEC Account or COMSEC Sub-Account who is authorized to receive COMSEC material from that account.

Local Tracking	The process used by the COMSEC Custodian to control and monitor the movement of COMSEC-related material outside of the NCMCS. **NOTE:** This process does not assign an ALC.
National COMSEC Material Control System (NCMCS)	A centralized system, which includes personnel, training and procedures, that enables GC departments to effectively control and handle ACM.
National COMSEC Incidents Office (NCIO)	The entity at CSE responsible for managing communications security incidents through registration, investigation, assessment, evaluation and closure.
Plik Seal	A tamper evident, theft prevention, high security seal that is affixed to packages before shipment.
Protective Packaging	Packaging techniques for COMSEC material, which discourage penetration, and reveal that a penetration has occurred, or which inhibit viewing or copying of COMSEC material, before the time it is exposed for use.
Removable Storage Medium (RSM)	A small device that is used to transport or store data (e.g. disk, memory card, flash drive).
Short Title	An identifying combination of letters and numbers assigned to COMSEC material to facilitate handling, accounting and control.
Sight Inventory	The physical verification of the presence of each item of COMSEC material charged to a COMSEC Account or Sub-Account.
Tier 3 Management Device (T3MD)	A cryptographic equipment that securely stores, transports and transfers (electronically) cryptographic key and that is programmable to support modern mission systems.
Transfer	The process of distributing COMSEC material from one COMSEC account to another COMSEC account.

18 Bibliography

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

- **Communications Security Establishment**
  - *Clearing and Declassifying Electronic Data Storage Devices* (ITSG-06), July 2006.
  - *Cryptographic Key Ordering Manual* (ITSG-13), May 2006.
  - *Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material* (ITSD-05), April 2012.
  - *Directive for the use of CSE-Approved COMSEC Equipment and Key on a Telecommunications Network* (ITSD-04), November 2011.
  - *Government of Canada Facility Evaluation Procedures* (ITSG-12), June 2005.
  - *IT Security Directive for the Control of COMSEC Material in the Government of Canada* (ITSD-03A), March 2014.
- **Department of Justice**
  - *Controlled Goods Regulations*, May 20, 2013.
  - *Financial Administration Act* (FAA), 1985.
  - *Privacy Act*, 1985 (current to November 25, 2012).
- **Public Services and Procurement Canada**
  - *Industrial Security Manual*, October 2014.
- **Royal Canadian Mounted Police**
  - *Guide to the Application of Physical Security Zones* (G1-026).
  - *Security Equipment Guide* (G1-001), March 2006.
- **Treasury Board of Canada Secretariat**
  - *Directive on Departmental Security Management* (DDSM), July 2009.
  - *Management of Information Technology Security* (MITS), April 2004.
  - *Operational Security Standard on Physical Security*, February 18, 2013.
  - *Policy on Government Security* (PGS), July 1, 2009.
- **Underwriters Laboratories of Canada (ULC)**
  - *Underwriters Laboratories of Canada (ULC) Standard* (ULC-S306-03).
- **United States Department of State**
  - *International Traffic in Arms Regulations* (ITAR), April 1, 2012.

Annex A COMSEC Sub-Account Roles and Responsibilities

A.1 COMSEC Sub-Account Custodian

The COMSEC Sub-Account Custodian responsibilities include:

- protecting and controlling ACM charged to the COMSEC Sub-Account or otherwise in possession of the private sector company;
- maintaining knowledge and record of the company's involvement in GC or foreign contracts and programs that require ACM support;
- 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 ACM issued to the company COMSEC Sub-Account, or produced within the facility;
- maintaining COMSEC accounting and related records as detailed in this directive;
- as requested by CICA, and upon appointment of a new COMSEC Sub-Account Custodian, conducting a COMSEC inventory and submitting an *Inventory Report* to CICA;
- disposing of COMSEC material only when directed and by means authorized by CICA;
- submitting *Inventory*, *Destruction*, and *Possession Reports* when required;
- ensuring the prompt and accurate entry of all amendments to COMSEC publications (refer to Article 11);
- ensuring that required page checks are accomplished on all COMSEC material requiring page checks;
- being aware at all times of the location of every item of ACM held by the facility and the general purpose for which it is being used;
- establishing "in-house" procedures to ensure strict control of each item of ACM whenever the material is outside of the COMSEC Sub-Account Custodian's secure storage facility;
- ensuring that appropriate ACM is readily available to authorized individuals whose duties require its use;
- reporting immediately to the CSO all known or suspected COMSEC incidents;
- assisting in the preparation of the *COMSEC Emergency Plan* for the safeguarding of COMSEC material;
- verifying the access to ACM prerequisites prior to granting access to such material or any records or files associated with the COMSEC Sub-Account;
- notifying, in writing, the local mail room or shipment receiving department of the requirement to deliver all parcels or envelopes addressed to the COMSEC Sub-Account Custodian or marked "TO BE OPENED ONLY BY THE COMSEC SUB-ACCOUNT CUSTODIAN", directly to the COMSEC Sub-Account Custodian without being opened;
- assisting in the preparation of the COMSEC portion of the company security plan;
- providing a COMSEC Briefing to all personnel who require access to ACM;

- ensuring ACM issued in support of a specific contract is not used for another contract unless authorized by the Project Management Office (PMO) or GC sponsor and CICA is informed;
- reporting any issues or concerns regarding ACM management to the CSO or CICA as appropriate;
- ensuring the Alternate Custodian(s) knowledge of the COMSEC Sub-Account requirements is maintained at a level that will allow proper management of the COMSEC Sub-Account in the absence of the COMSEC Sub-Account Custodian;
- ensuring this directive is adhered to by all company personnel who handle or manage ACM;
- ensuring continued requirement for ACM by Loan Holders/Users;
- ensuring all ACM is returned to the sponsor at the end-of contract or agreement through CICA; and
- advising CICA of any changes affecting management of the COMSEC Sub-Account.

A.2 COMSEC Sub-Account Alternate Custodian

The COMSEC Sub-Account Alternate Custodian duties include:

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

A.3 Loan Holder

ACM is provided for use exclusively within a private sector company. ACM provided to a Loan Holder must be for a specified period of time, and the loan must be renewed every six months. The Loan Holder is responsible to the COMSEC Sub-Account Custodian for the safeguarding of the ACM provided to the Loan Holder. However, the overall responsibility for all ACM provided to the private sector company rests with the COMSEC Sub-Account Custodian. As a minimum the following requirements must be adhered to:

- the Loan Holder must possess a valid need-to-know;
- the Loan Holder must possess a current *COMSEC Briefing Certificate* which is on file;
- the Loan Holder must have signed a *Loan Holder Responsibilities* form;
- the ACM must be both "loaned to" and "returned from" the Loan Holder on a signature basis using the Hand Receipt method or the COMSEC Material Control Register method;
- the intended Loan Holder must be an actual user of the material (clerical or other personnel who are not users of the ACM must not be appointed as a Loan Holder);
- the Loan Holder must meet the requirements for access to ACM;

- the Loan Holder must be subject to "no notice" inspections or audits of ACM holdings by the COMSEC Sub-Account custodial staff;
- the Loan Holder's ACM holdings must be formally sighted as detailed in this directive;
- the Loan Holder must immediately inform the custodial staff of any COMSEC incidents and infractions; and
- where cryptographic equipment (classified or CCIs) is being used, the Loan Holder must be trained by the COMSEC Sub-Account Custodian on its use or attend CSE-approved training.

Annex B Procedures for the Receipt of Accountable COMSEC Material

B.1 Preparation before Receiving Accountable COMSEC Material

Before receipt of any ACM, the COMSEC Sub-Account Custodian must:

- notify the company mailroom or shipping area, in writing, of the following:
  - the name of the company COMSEC Sub-Account that has been established;
  - the name and internal address of the COMSEC Sub-Account Custodian; and
  - the requirement to deliver mail and packages addressed to the COMSEC Sub-Account to the COMSEC Sub-Account Custodian unopened;
- instruct the company mailroom or shipping area that if the outer wrapper of a shipment is inadvertently opened by them that it is to be kept and provided to the COMSEC Sub-Account Custodian along with the package;
- provide the company mailroom or shipping area with up-to-date copies of the *COMSEC Signing Authority* form; and
- ensure other individuals who are authorized to sign for packages can provide appropriate secure storage for the received package(s) (when the COMSEC Sub-Account Custodian or Alternate Custodian is not available).

B.2 Inspection of Packages

On receipt of a shipment, the COMSEC Sub-Account Custodian must:

- carefully inspect the outer wrapping and inner wrapping of the shipment for signs of damage or tampering before removing each wrapping;
- check the addresses on both outer and inner wrapping to confirm the shipment has been sent to the intended recipient; and
- immediately report any evidence of possible tampering with either the inner or outer wrappings or unauthorized access to the contents as a possible COMSEC incident as detailed in Article 16:
  - pending investigation of a possible compromise, discontinue unwrapping the package and quarantine the package; and
  - notify the shipping COMSEC Sub-Account Custodian, if known, to annotate all ACM involved as “Pending Investigation”.

B.3 Sealed Cryptographic Equipment

Cryptographic equipment received in specially designed, sealed shipping containers which have not been opened or do not exhibit signs of tampering, may be receipted for without physically sighting the material on the inside as long as the special label on the container agrees with the *COMSEC Material Report*. If it does not, the contents must be physically inventoried. The COMSEC Sub-Account Custodian must bear in mind that, although the opening of certain types of material need not take place prior to actual usage, time must be allowed between opening and usage to obtain replacements for incomplete or defective items. Additionally, it is the COMSEC Sub-Account Custodian’s responsibility to report all shipment discrepancies to the CSE Industrial COMSEC Account (CICA).

Annex C Acquisition of Accountable Cryptographic Equipment

C.1 General

A Canadian private sector company is not permitted to purchase or own accountable cryptographic equipment. However, a Canadian private sector company may be provided accountable cryptographic equipment (including supporting key, ancillaries and equipment specific doctrine), if sponsored by a Government of Canada (GC) department that has an established Communications Security (COMSEC) Account. COMSEC Client Services must coordinate the signing of an Accountable COMSEC Material Control Agreement (ACMCA) by all parties (refer to Article 1.7).

NOTE: Although a private sector company may not purchase ACM, its GC sponsor may apply cost recovery for the supply of the equipment. The ACMCA or formal agreement must clearly state that the equipment (including key and ancillaries) will be returned to the GC sponsor (through CICA) for disposal once no longer required to meet the terms stated in the ACMCA or formal agreement.

The GC sponsor must seek approval from COMSEC Client Services prior to providing (through CICA) any accountable cryptographic equipment to a private sector company. Approval will be based on, but not limited to, such criteria as the:

- nature and extent of Foreign Ownership, Control or Influence (FOCI), refer to Article 1.11.1;
- type and classification of cryptographic equipment to be released;
- level of access required;
- Facility Security Clearance (FSC);
- Document Safeguarding Capability (DSC); and
- CSI.

C.2 With a Government of Canada Contract

Accountable cryptographic equipment may be provided to a Canadian private sector company through a contract procured through Public Services and Procurement Canada (PSPC).

The contract must specifically identify within the contract SRCL, a requirement to hold and use accountable cryptographic equipment (including supporting key and ancillaries).

C.3 Without a Government of Canada Contract

Under normal circumstances, ACM may be provided, without a GC contract procured through PSPC, to a private sector company only if the private sector company has established a COMSEC Sub-Account as detailed in Article 5.1.

Under exceptional circumstances (e.g. government-sponsored special events) COMSEC Client Services may authorize a short term loan of ACM (including associated key) to a private sector company through a sponsorship agreement without a COMSEC Sub-Account being established.

NOTE: When there is no longer a requirement for ACM to support the above, all ACM (including key and ancillaries) must be returned to its owner through CICA.

C.4 Installation of Accountable Cryptographic Equipment

The sponsoring GC department is responsible for conducting a Threat and Risk Assessment (TRA) and a Security Assessment and Authorization prior to permitting a sponsored private sector company to operate accountable cryptographic equipment.

C.5 Key Requirements

The sponsoring GC department is responsible for establishing key ordering privileges and for the ordering of key from the CSE. CICA is responsible for its delivery and management.

C.6 Acquisition Procedure

There are seven steps that must be followed when a private sector company will be required to hold accountable cryptographic equipment to meet a GC contract procured through PSPC:

1. GC sponsor DSO or DCA to identify COMSEC required by the private sector company early in the contracting process;
2. GC sponsor to provide detailed, written request to COMSEC Client Services. Include a completed CER and CEPA form, if required. Depending on the requirement, additional documentation such as a *Concept of Operations* (CONOP), a KMSP or an IP plan may be required. Requirements for other ACM (e.g. key and publications) must also be initiated as early in the process as possible.
3. upon favourable review and validation of the requirement by COMSEC Client Services, a CSE confirmation letter will be provided to the GC sponsor (letter will include acknowledgement and validation of the requirement only). Final release authority will be provided by COMSEC Client Services once all security requirements are in place (refer to Step 6). An ACMCA will be initiated by CSE at this time.
4. GC sponsor submits a package to the PSPC ISP containing the CSE confirmation letter, a completed and signed SRCL and a copy of the formal sponsorship agreement (e.g. contract, pre-contractual agreement or other type of sponsorship agreement). A copy of the SRCL must also be sent to COMSEC Client Services.

   NOTE 1: The sponsorship agreement must identify the private sector company, identify its location, describe the work to be conducted, identify the GC CCIs and any other ACM required to support the contract, how the equipment will be acquired and how the CCI and any other COMSEC material will be used.

   NOTE 2: The GC sponsor should contact COMSEC Client Services for guidance on completing the SRCL as it relates to COMSEC requirements. While the SRCL must describe the CSI with the highest sensitivity level of the ACM being accessed, the level must be, at a minimum, SECRET.

5. when the GC sponsor's package has been received, the ISP will:
   - contact the private sector company and confirm that it meets the security requirements of the sponsoring agreement or SRCL, and

- when adherence to security requirements has been confirmed, advise the private sector company that it has been awarded the required FOCI, FSC, as well as a DSC, IT and Production (if required) inspection. The GC sponsor and COMSEC Client Services will receive a copy of the award letter;

6. when COMSEC Client Services receives the ISP notification, it will authorize the establishment of a private sector company COMSEC Sub-Account and ensure all associated documentation, including the ACMCA, is completed and approved.

   If a commensurate sensitivity level private sector COMSEC Sub-Account already exits, COMSEC Client Services will arrange for completion and approval of the required ACMCA, MOA and MOU (if applicable or required). Final CSE authority to release ACM to private sector partners is promulgated by COMSEC Client Services; and

7. when the GC sponsor receives the ISP notification, it will transfer the required GC cryptographic equipment or other ACM through the National COMSEC Material Control System (NCMCS) to CICA. Once release authority is provided by COMSEC Client Services, CICA will issue the ACM to the applicable COMSEC Sub-Account.

   NOTE 1: ACM will not be released from CSE until a COMSEC Sub-Account has been established by CICA.

   NOTE 2: Contact COMSEC Client Services for guidance on the acquisition of ACM other than to meet a GC contract procured through PSPC (e.g. Request for Proposal [RFP] requirement – refer to Article 8.1.3).

Annex D Roles and Responsibilities Quick Reference Guides

D.1 Roles and Responsibilities – With a Government of Canada Contract

The following Table provides a quick reference guide for the major roles and responsibilities of the Communications Security Establishment (CSE), Public Services and Procurement Canada (PSPC), the GC sponsor and the private sector when a private sector company holds a contract procured through PSPC that requires it to hold Accountable COMSEC Material (ACM).

Table 7 – Roles and Responsibilities – With Government of Canada Contract

CCS = COMSEC Client Services	CSE		PSPC ISP	GC Sponsor	Private Sector Company
	CICA	CCS			
Notifying CSE of contract or agreement requirements that require ACM access				▲ 2.5	
Signing *Accountable COMSEC Material Control Agreements* (ACMCAs)				▲ 2.5	▲ 2.6.2
Ensuring COMSEC Client Services is in receipt of SRCL				▲ 2.5	
Providing *Facility Security Clearance* (FSC), *Document Designated Organization Screening* (DSC), and CSI equivalents as required by CSE				▲ 2.5	
Identifying ACM requirements and submitting a CER form and a CEPA form to CSE (if required)				▲ 2.5 and Annex C.6	
Providing a Controlling Authority for authorized Cryptographic Networks				▲ 2.5	
Coordinating release of ACM to a private sector company with CICA				▲ 2.5	
Completing a FOCI Assessment			▲ 1.11.1 and 2.3.1		
Providing FSC, DSC, and CSI			▲ 2.3.1		
Providing assessment of suitability for an FSC, CSI, DSC and Production inspection, and FOCI			▲ 8.1.3		

CCS = COMSEC Client Services	CSE		PSPC ISP	GC Sponsor	Private Sector Company
	CICA	CCS			
Coordinating the screening of private sector companies and personnel for North Atlantic Treaty Organization (NATO) and foreign contracting security requirements			▲ 2.3.1		
Arranging the transfer of non-COMSEC classified and protected information and assets between Canadian and foreign governments and the private sector			▲ 2.3.1		
Coordinating the development of international Project Security Instructions (PSIs)			▲ 2.3.1		
Providing Visit Clearance authority			▲ 2.3.1		
Opening and closing a COMSEC Sub-Account	▲ 2.2.3, 5.1 and 5.5				
Authorizing and coordinating the movement and distribution of ACM	▲ 2.2.3				
Providing support and guidance on the use of CSE-approved cryptographic equipment and key	▲ 2.2.3				
Performing annual inventory reconciliations	▲ 2.2.3				
Being the CSE initial point of contact for reporting COMSEC incidents	▲ 16.1				
Conducting Private Sector COMSEC Sub-Account audits	▲ 2.2.3 and 15.1.2				
Providing COMSEC management advice, guidance and direction	▲ 2.2.3				
Temporarily suspending a COMSEC Sub-Account	▲ 5.7				

CCS = COMSEC Client Services	CSE		PSPC ISP	GC Sponsor	Private Sector Company
	CICA	CCS			
Providing authorization for change of an Accounting Legend Code	▲ 6.2.5.1				
Providing initial COMSEC Briefings to COMSEC Sub-Account Custodian	▲ 8.2.1				
Approving COMSEC Sub-Account Custodian work area	▲ 9.2				
Authorizing the storage or shipment of keyed equipment	▲ 9.6.2 and 10.4				
Authorizing the appointment of private sector company couriers	▲ 10.10.1				
Completing In-Process (IP) COMSEC Account audits	▲ ITSD-08				
Providing advice and guidance on the movement of ITAR controlled ACM		▲ 2.2.1			
Providing an assessment of suitability to hold a COMSEC Sub-Account		▲ 2.2.1 and 8.1.3			
Authorizing the establishment or closure of a private sector COMSEC Sub-Account		▲ 2.2.1			
Authorizing the establishment and closure of an In-Process Account		▲ ITSD-08			
Validating private sector requirements to hold CSE-approved COMSEC Solutions and material		▲ 2.2.1			
Confirming all security pre-requisites are met prior to authorizing the establishment of a Sub-Account		▲ 2.2.1			

CCS = COMSEC Client Services	CSE		PSPC ISP	GC Sponsor	Private Sector Company
	CICA	CCS			
Coordinating the signing and distribution of ACMCAs, TAAs, Non-Disclosure Agreements and other agreements		▲ 2.2.1 and Annex C.1			
Validation of Key Material Support Plans		▲ 2.2.1			
Coordinating the provision of TEMPEST inspections		▲ 2.2.1			
Coordinating cross-border shipments of ACM with other National Security Authorities		▲ 2.2.1			
Authorizing COMSEC access for visits		▲ 4.2.1 and 8.5			
Authorizing the change of classification level of a COMSEC Sub-Account		▲ 5.3.4			
Authorizing a COMSEC Sub-Account to hold a zero balance		▲ 5.6			
Authorizing access to ACM by foreign Nationals		▲ 8.1.2			
Authorizing work areas outside established COMSEC Facilities		▲ 9.1.1			
Approving In-Process plans		▲ ITSD-08			
Implementing the requirements of the Canadian *Controlled Goods Program* and the United States *International Traffic in Arms Regulations*					▲ 1.11.2 and 1.11.3
Ensuring ACM management within the company meets the minimum standards required by CSE					▲ 2.6.2
Submitting an *Appointment Certificate* to CICA for the COMSEC Sub-Account Custodian and Alternate Custodian (s)					▲ 5.1.2

CCS = COMSEC Client Services	CSE		PSPC ISP	GC Sponsor	Private Sector Company
	CICA	CCS			
Providing COMSEC briefings to COMSEC Sub-Account Staff					▲ 8.2.1
Developing a *COMSEC Emergency Plan*					▲ 2.6.2 and 14.3.1
Developing an *In-Process (IP) Plan*					▲ ITSD-08
Reporting COMSEC incidents to CICA					▲ 2.2.3, 16 and ITSD-05
Ensuring subcontractors meet the security requirements of the PSPC ISM and this directive prior to being provided access to ACM					▲ 2.6.2

D.2 Roles and Responsibilities – Without a Government of Canada Contract

The roles and responsibilities listed in Table 7 apply to a requirement for a private sector company to hold Accountable COMSEC Material (ACM) without a contract except for the following, which will be provided (as required by CSE) by the GC sponsor and validated by COMSEC Client Services:

- *Facility Security Clearance* (FSC) equivalency;
- *Document Safeguarding Capability* (DSC) equivalency;
- *Information Technology Processing* (ITP);
- *COMSEC Safeguarding Inspection*; and
- providing additional supporting documentation.