Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

IT Security Directive for Reporting and Evaluating Communications Security (COMSEC) Incidents

ITSD-05A

COMSEC

Canada

FOREWORD

The *IT Security Directive for Reporting and Evaluating COMSEC Incidents* (ITSD-05A) 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*.

Previously distributed versions of ITSD-05 are superseded by this directive. Superseded versions and all previously distributed drafts must be destroyed in accordance with departmental procedures for the disposal of government information.

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

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

EFFECTIVE DATE

This doctrine takes effect on date of signature.

Original signed by

Scott Jones

Head, Canadian Centre for Cyber Security

April 22, 2021

REPRODUCTION AND DISTRIBUTION

D96-77/2021E-PDF ISBN 978-0-660-40875-0

SUMMARY OF CHANGES FROM ITSD-05 TO ITSD-05A

Although all COMSEC personnel should read this document in its entirety, the following major changes have been made.

Reference	Change
Throughout	• Departmental Security Officer (DSO) has been replaced by Chief Security Officer (CSO) as per the new *Policy on Government Security*, dated July 1, 2019; • Enterprise Services Organization, Enterprise Security Officer and Enterprise COMSEC Authority have been added as a result of the Enterprise service model introduced in 2015; • The definition of Compromising Incident has been revised to exclude "unauthorized viewing of ACM"; and • The use of an acronym for Compromising Incident (CI) has been added.
Article 2.3	• An article describing the private sector Company Security Officer role and its responsibilities related to COMSEC incident reporting has been added.
Article 4.2	• A COMSEC Incident Initial Report (CIIR) must be completed for all Practices Dangerous to Security (PDS) and retained locally on file.
Article 4.4	• Consistently reoccurring PDS may be escalated to Compromising Incident (CI).
Article 4.4.1	• PDS CIIRs, or a spreadsheet summary of PDS, must be submitted annually to the National COMSEC Incidents Office (NCIO) and provided to the National COMSEC Audit Team (NCAT) prior to every cyclical audit.
Article 4.5	• Incident report classification requirements have been clarified.
Appendix A	• A breakdown of Compromising Incident (CI) and PDS by type, with examples, has been added.

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The Treasury Board of Canada Secretariat (TBS) *Policy on Government Security* (PGS) identifies lead security agencies and their responsibilities to provide leadership, advice, services, and guidance to support the Government of Canada (GC) in maintaining acceptable levels of security while achieving strategic goals and service delivery imperatives. As stated in the PGS, the Communications Security Establishment (CSE) is responsible for helping to ensure the protection of electronic information and information infrastructures of importance to the GC and for serving as the national authority for Communications Security (COMSEC).

COMSEC is the application of cryptographic security, transmission and emission security, personnel security safeguards, physical security measures, and operational practices and controls to deny unauthorized access to information derived from telecommunications and that ensure the authenticity of such telecommunications.

1.1 AUTHORITY

This directive is promulgated in accordance with the PGS which identifies CSE as the national authority for COMSEC. CSE develops, approves, and promulgates COMSEC-related policy instruments and develops guidelines and tools related to Information Technology (IT) security.

1.2 PURPOSE

This directive provides the minimum reporting and evaluation requirements for COMSEC incidents involving COMSEC material (as described in Article 1.3) by GC departments, enterprise services organizations, GC-sponsored Other Levels of Government (OLG) organizations, and GC-sponsored Canadian private sector companies.

Refer to Article 3.1 for the definition of COMSEC incident.

1.3 SCOPE

This directive applies to COMSEC incidents involving:

- National Accountable COMSEC Material (ACM);
- North Atlantic Treaty Organization (NATO), Combined Communications Electronics Board (CCEB), and Allied ACM that has been entrusted to Canada through international partnership agreements;
- COMSEC material managed within a COMSEC In-Process (IP) Account; and
- Other COMSEC material that may or may not be classified and is not accounted for in the National COMSEC Material Control System (NCMCS) but must be controlled through a local register system.

NOTE: The term “COMSEC material” will, hereinafter and unless specified otherwise, be used to refer to all of the above.

1.4 CONTEXT

The TBS directs that departments meet the security controls defined by Annex A of the PGS, including those related to the IT security requirements, practices, and controls necessary to “provide reasonable assurance that information systems can be trusted to adequately protect information, are used in an acceptable manner, and support government programs, services and activities”. This directive supports CSE in its lead role for IT security, as stated in the PGS and the Directive on Security Management (DSM).

1.5 APPLICATION

This directive applies to GC departments, enterprise services organizations, GC-sponsored OLG organizations, and GC-sponsored Canadian private sector companies that are authorized to handle, control, and safeguard CSE-approved COMSEC material designed for the protection of GC classified and protected information and data.

For the purpose of this directive, the term:

- "GC department" includes any federal institution (e.g. department, agency, organization) defined by Section 2 of the Financial Administration Act (FAA) or entity included in Schedules IV and V of the same document, unless excluded by specific acts, regulations or Orders in Council;

  NOTE: Unless specified otherwise, GC department includes enterprise service organizations.

- "OLG organizations" includes provincial, municipal and local government organizations (e.g. law enforcement agencies); and

- "Canadian private sector companies", hereinafter referred to as private sector companies, includes Canadian companies, organizations or individuals that do not fall under the FAA or are not subordinate to a provincial or municipal government. It also includes Canadian based industries (or other non-government organizations) where security is administered by the Industrial Security Program (ISP) of Public Service and Procurement Canada (PSPC).

1.6 COMPLIANCE

GC departments, OLG organizations, and private sector companies (as noted in Article 1.5) that handle COMSEC material must comply with the baseline COMSEC incident reporting and evaluation requirements detailed in this directive.

While compliance with these minimum COMSEC incident reporting and evaluation requirements is the responsibility of each GC department, OLG organization, and private sector company, it does not preclude individual organizations from applying more stringent requirements. Departmental directives that exceed the minimum requirements of this directive take precedence within that department.

1.6.1 CONSEQUENCE OF NON-COMPLIANCE

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

1.6.2 DISCIPLINARY ACTION

Disciplinary action, if deemed warranted by circumstance, is entirely in the purview of the GC departmental authority (e.g. Chief Security Officer [CSO] or Enterprise Security Officer [ESO]). Failing to report a COMSEC incident may be considered "willful or gross neglect" and must be evaluated accordingly.

1.7 CONFLICT RESOLUTION

Any conflict between this Information Technology Security Directive (ITSD) and any other national (e.g. other ITSDs, PGS and DSM) publication must be submitted to COMSEC Client Services (CCS) for resolution.

1.8 REQUESTS FOR EXCEPTION OR WAIVER

A request for an exception (substitution) or a waiver (temporary exemption from a specific requirement) must be submitted by the Departmental COMSEC Authority (DCA) or Enterprise COMSEC Authority (ECA) in writing, and with a justification, to CCS for approval.

2 ROLES AND RESPONSIBILITIES

2.1 COMMUNICATIONS SECURITY ESTABLISHMENT

The Director, Cryptographic Client Services and Operations (CCSO) has been delegated by the Head of the Canadian Centre for Cyber Security (CCCS) as the final adjudicator and signatory for the Final Assessment and Closure Report of all Compromising Incidents (CIs).

2.1.1 NATIONAL COMSEC INCIDENT OFFICE

Under the direction of the Head CCCS, the National COMSEC Incidents Office (NCIO) is responsible for:

- Maintaining national records of all COMSEC incidents;

  Refer to Article 3.1 for the definition of COMSEC incident.
- Coordinating cross-border COMSEC incident resolution with international partners;
- Verifying and documenting Compromising Incidents (CIs);
- Coordinating multi-departmental incident reporting;
- Determining the need for, and appropriateness of, Compromising Incident (CI) recovery actions;
- Notifying applicable authorities of recovery actions taken; and
- Providing responsible CSO/ESOs and DCA/ECAs with Final Assessment and Closure Reports for Compromising Incidents (CIs).

2.2 DEPARTMENTAL AND ENTERPRISE AUTHORITIES

The CSO/ESO is responsible for the overall management of the departmental or enterprise security program, including that of the COMSEC program, as defined by the DSM.

2.2.1 DEPARTMENTAL OR ENTERPRISE COMSEC AUTHORITY

The DCA/ECA is responsible for the development, implementation, maintenance, coordination, and monitoring of the departmental COMSEC program in a manner consistent with the PGS and its operational standards. Additionally, the DCA is responsible for the overall control of COMSEC material that has been charged to the departmental COMSEC Account.

The DCA/ECA is responsible for:

- Establishing an awareness program that will ensure every individual with access to COMSEC material is aware of what constitutes a COMSEC incident and understands the importance of their prompt, complete, and accurate reporting;
- Establishing 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, COMSEC material;
- Establishing departmental/enterprise COMSEC incident monitoring processes, including those for sponsored OLG organizations and private sector companies that handle COMSEC material;
- Conducting an immediate initial investigation and completing a COMSEC Incident Initial Report (CIIR) of all confirmed or suspected COMSEC incidents;

  NOTE: Should the DCA/ECA be absent or lack availability, the DCA/ECA may delegate the initial investigation to the COMSEC Custodian provided that they were not involved in the incident.
- Submitting a CIIR for confirmed or suspected Compromising Incidents (CIs) to the NCIO within 24 hours of being notified of the incident;
- Continuing Compromising Incident (CI) investigation to its conclusion and providing a COMSEC Incident Evaluation Report (CIER) to the NCIO, if requested;
- Locally resolving Practices Dangerous to Security (PDS) and maintain records of all departmental/enterprise PDS;

- Providing PDS records to the NCIO annually and to the National COMSEC Audit Team (NCAT) prior to scheduled COMSEC Account audits; and
- Ensuring that the CSO/ESO is advised of all COMSEC incidents occurring within their area of responsibility.

2.3 PRIVATE SECTOR COMPANY SECURITY OFFICER

Private sector companies with a requirement to hold COMSEC material must be sponsored by a GC department and managed by the CSE Industrial COMSEC Account (CICA), as detailed in the current version of the *IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector* (ITSD-06).

The Company Security Officer (may also be referred to as the Corporate Security Officer) is responsible for the overall company COMSEC security posture including the establishment of internal COMSEC incident and response procedures and the prompt and accurate reporting of COMSEC incidents, as described herein and in the current version of ITSD-06, to the CICA DCA.

2.4 CONTROLLING AND COMMAND AUTHORITIES

The Controlling Authority (ConAuth)/Command Authority (CmdAuth) must ensure that cryptographic network (cryptonet) members are aware of the procedures for reporting and evaluating COMSEC incidents. With respect to COMSEC incidents, the ConAuth/CmdAuth is responsible for:

- Reporting COMSEC incidents to the responsible DCA/ECA or COMSEC Custodian;
- Ensuring that COMSEC incident reporting procedures are followed;
- Initiating cryptographic key compromise recovery action as detailed in the current version of ITSD-04; and
- Providing assistance, upon request, in the investigation of COMSEC incidents or in the completion of CIIRs.

NOTE: For the purpose of this directive, the term “key” is used to refer to all forms of physical or electronic cryptographic key. It is used as a singular and plural term.

2.5 COMSEC CUSTODIAN

The COMSEC Custodian is responsible for:

- Ensuring that every individual who uses or has access to COMSEC material can recognize a COMSEC incident and understands the importance of prompt reporting;
- Immediately notifying the DCA/ECA of COMSEC incident occurrences;
- Conducting an initial investigation, if delegated by the DCA/ECA;

  NOTE: Delegation may only be bestowed on the COMSEC Custodian when the DCA/ECA is absent or unavailable and the COMSEC Custodian is not involved in the incident.
- Placing any affected COMSEC material, where appropriate, in quarantine and marking the material as “Pending Investigation” in the inventory file; and
- Maintaining accountability for affected COMSEC material, where appropriate, until the COMSEC incident investigation has been completed and disposition instructions are received from the NCIO via a Final Assessment and Closure Report.

3 COMSEC INCIDENT TYPES

3.1 DEFINITION

A COMSEC incident is any occurrence that jeopardizes or potentially jeopardizes the security of COMSEC material, or the security of protected or classified GC information and data, while it is being stored, processed, transmitted, or received during the telecommunications process.

There are two types of COMSEC incidents:

- Compromising Incidents (CIs); and
- Practices Dangerous to Security (PDS).

Refer to Appendix A for examples of each. Equipment-specific COMSEC incidents can be found in the Canadian Cryptographic Doctrine (CCD) corresponding to the equipment.

3.2 COMPROMISING INCIDENTS

A Compromising Incident (CI) is a COMSEC incident that could result in the loss of control or unauthorized access of COMSEC material, or in a compromise of information, assets, or functionality, and may have a serious negative consequence to operational security.

3.3 PRACTICES DANGEROUS TO SECURITY

A PDS is a COMSEC incident that is considered a minor violation of administrative requirements but does not result in the loss of control or unauthorized access to COMSEC material. Although a PDS does not result in a compromise of information, assets, or functionality, it could create a situation where exploitation or compromise is possible if the practice is not corrected.

Any PDS found to consistently reoccur at an account may, at the discretion of the NCIO (and in collaboration with the NCAT), be escalated to a Compromising Incident (CI).

4 COMSEC INCIDENT REPORTING

4.1 THE COMSEC INCIDENT REPORTING PROCESS

The prompt and accurate reporting of COMSEC incidents is essential to ensuring corrective actions are taken in a timely manner to mitigate or eliminate their impact on COMSEC.

NOTE: Corrective actions vary and are beyond the scope of this directive.

Any individual who handles or otherwise has access to COMSEC material must promptly alert the responsible COMSEC Custodian to any confirmed or suspected COMSEC incident, regardless of the material's country of origin and regardless of how seemingly insignificant the incident may be. All confirmed or suspected COMSEC incidents must be reported to the DCA/ECA for investigation.

Following the detection of an COMSEC incident, the reporting process consists of three main steps: initial investigation, reporting, and further steps according to incident type (Compromising Incident [CI] or PDS) leading to incident resolution (refer to Figure 1).

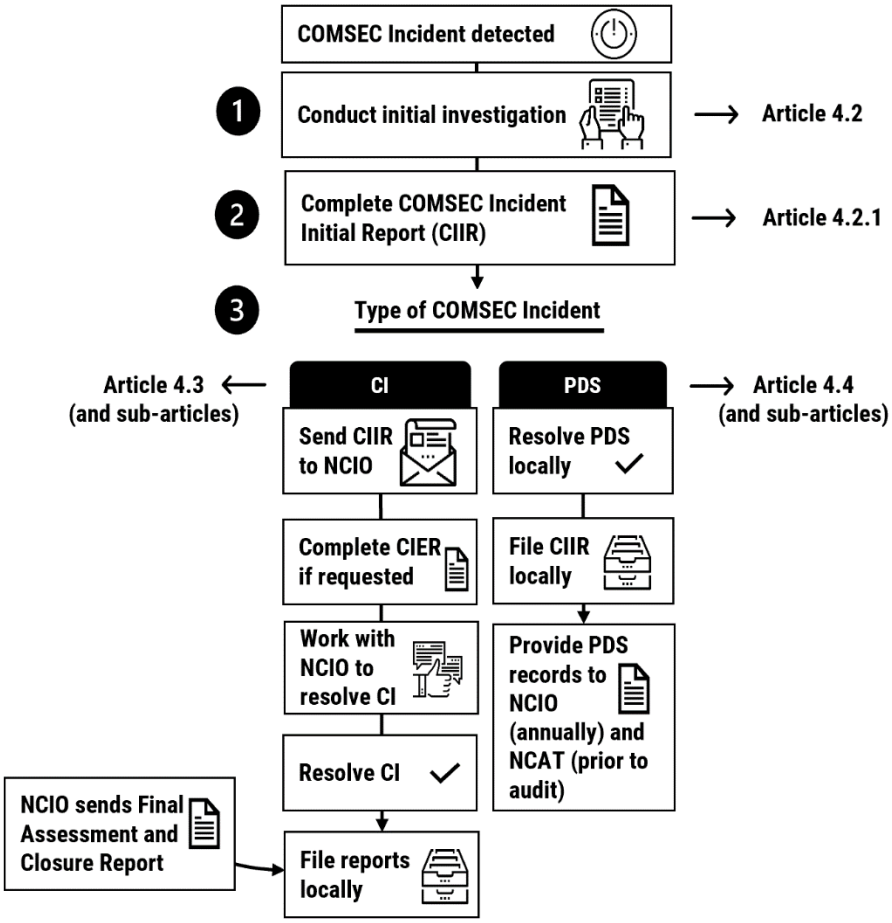

Figure 1 – COMSEC Incident Reporting Process

4.1.1 COMSEC INCIDENTS IN THE PRIVATE SECTOR

Canadian private sector companies that handle COMSEC material, including those that handle IP COMSEC material, must immediately report all COMSEC incidents to the CICA, as detailed in the current versions of ITSD-06 and the *IT Security Directive for the Control and Management of In-Process COMSEC Material* (ITSD-08), as applicable.

4.2 COMSEC INCIDENTS: INITIAL INCIDENT INVESTIGATION

The DCA/ECA must begin an initial investigation within 24 hours of being notified that a COMSEC incident has occurred. The initial investigation includes the completion of a COMSEC Incident Initial Report (CIIR) form (ITS-020). Completing the CIIR will assist the DCA/ECA in their collection of the facts and circumstances surrounding the incident. A CIIR must be completed for all COMSEC incidents, regardless of type.

Following their initial investigation, the DCA/ECA should have sufficient information to determine if the COMSEC incident is a Compromising Incident (CI) or a PDS. If the incident is determined to be a:

- **Compromising Incident (CI)** – the DCA/ECA must submit the CIIR to the NCIO by secure phone or secure facsimile. Upon doing so, the DCA/ECA must, in consultation with the NCIO, resolve the issue (refer to Article 4.3); or
- **PDS** – the DCA/ECA must take immediate action to locally resolve the PDS (refer to Article 4.4).

NOTE: If unsure as to whether a COMSEC incident is a Compromising Incident (CI) or PDS, contact the NCIO or report the incident as a Compromising Incident (CI).

4.2.1 COMSEC INCIDENT INITIAL REPORT

A CIIR must be completed for all COMSEC incidents. The CIIR form (ITS-020) can be found on the CSE COMSEC User Portal (CUP; refer to Article 5.3).

When completing the CIIR, the following must be included:

- The name of the DCA/ECA, or designated COMSEC Custodian, responsible for investigating and evaluating the incident;
- The name of the responsible CmdAuth or ConAuth, if applicable;
- The names, citizenship, position, and clearance levels of all individuals involved;
- Identification of the reporting COMSEC Account and the COMSEC Account in which the incident occurred;
- The type of COMSEC incident (Compromising Incident [CI] or PDS). If the COMSEC incident is determined to be a:
  - **Compromising Incident (CI)**– indicate an initial assessment of the possibility of a compromise (refer to Article A.1.1) and the Compromising Incident (CI) category and Compromising Incident (CI) type, if possible (refer to Articles A.1.2 and A.1.3, respectively, for definitions and examples); and
  - **PDS** – indicate the PDS type, if possible (refer to Article A.2.1 for definitions and examples).
- A detailed description of the circumstances surrounding the event, including the date and time the COMSEC incident was initially discovered and the date that it was actually reported to the responsible COMSEC Custodian and/or DCA/ECA;
- A complete list of all COMSEC material involved including short titles, editions, and segments of key loaded in cryptographic equipment, accounting numbers (e.g. Key Material Identifiers [KMIDs]), classifications, and key expiry or supersession date; and
- Corrective action taken or planned.

4.3 COMPROMISING INCIDENTS: EVALUATION, ASSESSMENT AND CLOSURE

Upon receipt and review of the CIIR, the NCIO may request additional detail about the reported Compromising Incident (CI). This additional information, provided on a COMSEC Incident Evaluation Report (CIER) form (ITS-038), can help the NCIO finalize impact assessment and recovery requirements.

4.3.1 COMSEC INCIDENT EVALUATION REPORT

When completing a CIER, the DCA/ECA must include:

- A detailed chronological account of the nature and circumstances surrounding the Compromising Incident (CI);
- Amplification of details provided in the CIIR; and
- A description of corrective action taken to limit damage resulting from the incident and to prevent reoccurrence of the incident.

The CIER form (ITS-038) can be found on the CSE CUP (refer to Article 5.3).

4.3.2 REPORTING CHANGES TO A CIIR OR CIER (AMPLIFYING REPORT)

When new information is discovered that may influence or change a previously submitted CIIR or CIER, the DCA/ECA must submit those changes, in writing, to the NCIO. The CIIR form may be used.

4.3.3 FINAL ASSESSMENT AND CLOSURE REPORT

A Final Assessment and Closure Report is issued to the DCA/ECA and the COMSEC Custodian by the NCIO upon collection and assessment of all gathered information and available records. The report will include recommendations for the prevention of reoccurrences as well as recommendations for the prevention of similar incidents. The report will also provide disposition instructions for the affected COMSEC material, if required.

The NCAT will follow up on the implementation of the NCIO's recommendations during scheduled audits.

4.4 PDS: LOCAL REPORTING AND RESOLUTION

All PDS must be investigated by the DCA/ECA and a CIIR must be completed, as described in Article 4.2.1. The DCA/ECA is expected to work with COMSEC Account personnel to locally resolve all PDS in accordance with departmental procedures. Should the DCA/ECA believe that a PDS could occur at other departments, the DCA/ECA must notify the NCIO.

Any PDS found to consistently reoccur at an account may, at the discretion of the NCIO (and in collaboration with the NCAT), be escalated to a Compromising Incident (CI) and must be reported accordingly.

4.4.1 PDS RECORDS

All PDS reports (i.e. CIIRs) must be retained (refer to Article 4.6). The DCA/ECA may optionally create a spreadsheet that summarizes each PDS. The PDS records or spreadsheet summary must be provided to the NCIO annually and to the NCAT prior to every COMSEC Account audit.

4.5 REPORT CLASSIFICATION

COMSEC incident reports (CIIR, CIER, amplifying, and Final Assessment and Closure Report) must be classified at the highest level of the COMSEC material exposed, lost, or compromised, but never less than PROTECTED B. The content of the report should also be considered. For example:

- If the report includes (or infers) status information about a key (e.g. key expiry date or cryptoperiod), the report must be classified, minimally, as CONFIDENTIAL; and
- If the COMSEC incident involves an IT system that processes information at a level higher than that of the affected COMSEC material, the report may require classification at the IT system level. For example:
  - If a COMSEC incident involves a SECRET network but the report only contains information up to PROTECTED B, the report may be classified as PROTECTED B; but
  - If a COMSEC incident involves a SECRET network and the report contains information about the network, the report must be classified as SECRET.

NOTE: Care must be taken to avoid the over-classification of reports. Reports that are classified (CONFIDENTIAL, SECRET, or TOP SECRET) will require special transmission, handling, and storage considerations.

4.6 REPORT RETENTION

COMSEC incident reports (CIIR, CIER, amplifying, and Final Assessment and Closure Report) must be retained for a minimum of five years, as detailed in the current version of ITSD-03.

4.7 REPORT DISSEMINATION

Dissemination of COMSEC incident reports, or information related to COMSEC incidents, must be limited to those with a clear need to know and a security clearance commensurate with the classification of the information provided. Personal information must be protected as detailed in the *Privacy Act*.

5 REFERENCES

5.1 ABBREVIATIONS AND ACRONYMS

ACM	Accountable COMSEC Material
ACMCA	Accountable COMSEC Material Control Agreement
ALC	Accounting Legend Code
CCCS	Canadian Centre for Cyber Security
CCD	Canadian Cryptographic Doctrine
CCEB	Combined Communications Electronics Board
CCI	Controlled Cryptographic Item
CCS	COMSEC Client Services
CCSO	Cryptographic Client Services and Operations
CEP	COMSEC Emergency Plan
CI	Compromising Incident
CICA	CSE Industrial COMSEC Account
CIER	COMSEC Incident Evaluation Report
CIIR	COMSEC Incident Initial Report
CIK	Cryptographic Ignition Key
CMAC	Crypto Material Assistance Centre
CmdAuth	Command Authority
COMSEC	Communications Security
ConAuth	Controlling Authority
Cryptonet	Cryptographic Network
CSE	Communications Security Establishment
CSO	Chief Security Officer
CUP	COMSEC User Portal
DCA	Departmental COMSEC Authority
DIAS	Distributed INFOSEC Accounting Software
DR	Destruction Report
DSM	*Directive on Security Management*
ECA	Enterprise COMSEC Authority
ECU	End Cryptographic Unit
EKMS	Electronic Key Management System
ESO	Enterprise Security Officer
FAA	Financial Administration Act
FSU	Field Software Upgrade
FTR	Field Tamper Recovery
GC	Government of Canada
HA	High Assurance
HTTPS	Hypertext Transfer Protocol Secure
IP	In-Process
ISP	Industrial Security Program
IT	Information Technology
ITSD	Information Technology Security Directive

KMID	Key Material Identifier
KMSP	Key Management Support Plan
LCMS	Local COMSEC Management System
NATO	North Atlantic Treaty Organization
NCAT	National COMSEC Audit Team
NCIO	National COMSEC Incidents Office
NCMCS	National COMSEC Material Control System
NCOR	National Central Office of Record
NLZ	No-Lone Zone
OLG	Other Levels of Government
PDS	Practice Dangerous to Security
PGS	*Policy on Government Security*
PIN	Personal Identification Number
PSPC	Public Services and Procurement Canada
RCMP	Royal Canadian Mounted Police
RMA	Return of Material Authority
SCIP	Secure Communications Interoperability Protocol
SOP	Standard Operating Procedure
SSO	Site Security Office
T3MD	Tier 3 Management Device
TBS	Treasury Board of Canada Secretariat
TPI	Two Person Integrity
TRA	Threat and Risk Assessment
TV	Trusted Vendor

5.2 GLOSSARY

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

Table 1 – Glossary

UNCLASSIFIED	
Accountable COMSEC Material (ACM)	COMSEC material that requires control and accountability within the NCMCS in accordance with its Accounting Legend Code (ALC) and for which loss or disclosure could be detrimental to the national security of Canada.
Canadian Cryptographic Doctrine (CCD)	The minimum security standards for the safeguard, control and use of CSE-approved cryptographic equipment and systems.
Chief Security Officer (CSO)	The individual responsible for developing, implementing, maintaining, coordinating and monitoring a departmental security program consistent with the *Policy on Government Security* and its standards.
Communications Security (COMSEC)	The application of cryptographic security, transmission and emission security, personnel security safeguards, physical security measures, and operational practices and controls to deny unauthorized access to information derived from telecommunications and that ensure the authenticity of such telecommunications.
Compromising Incident (CI)	A COMSEC incident that could result in the loss of control or unauthorized access of COMSEC material, or in a compromise of information, assets or functionality, and may have a serious negative consequence to operational security.
COMSEC Account	An administrative entity, identified by an account number, used to maintain accountability, custody and control of COMSEC material produced by or entrusted to the entity.
COMSEC Custodian	The individual designated by the departmental or enterprise services organization COMSEC authority to be responsible for the receipt, storage, access, distribution, accounting, disposal and destruction of all COMSEC material that has been charged to the COMSEC Account.
COMSEC Incident	Any occurrence that jeopardizes or potentially jeopardizes the security of COMSEC material or the secure transmission of national security information while it is being stored, processed, transmitted or received during the telecommunications process.
COMSEC Material	Material designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, modules, devices, documents, hardware, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions. COMSEC material includes items that may or may not be classified but must be accounted for in the NCMCS or controlled through a register system (i.e. locally tracked).
Controlled Cryptographic Item (CCI)	Unclassified secure telecommunications or information handling equipment, or associated cryptographic components, that are governed by a special set of control requirements within the NCMCS and marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI".

UNCLASSIFIED	
CRYPTO	A marking which is applied to key indicating that items so marked are subject to specific controls governing access, distribution, storage, accounting, disposal and destruction.
Departmental COMSEC Authority (DCA)	The individual designated by, and responsible to, the CSO for developing, implementing, maintaining, coordinating and monitoring a departmental COMSEC program which is consistent with the *Policy on Government Security* and its standards.
Enterprise COMSEC Authority (ECA)	The individual designated by, and responsible to, the ESO for developing, implementing, maintaining, coordinating and monitoring an enterprise COMSEC program which is consistent with the *Policy on Government Security* and its standards. **NOTE**: The ECA role may be split into two separate roles (operations and program) based upon the complexity of the enterprise.
Enterprise Security Officer (ESO)	The individual responsible for developing, implementing, maintaining, coordinating and monitoring an enterprise security program consistent with the *Policy on Government Security* and its standards.
Enterprise Services Organization	A GC department that has been assigned the lead role to provide COMSEC management services to other GC departments and agencies that are outside of the organization's traditional accountability chain.
Government of Canada (GC) Department	Any federal department, organization, agency or institution subject to the *Policy on Government Security*.
National Central Office of Record (NCOR)	The entity at CSE responsible for overseeing the management and accounting of ACM, produced in, or entrusted to Canada.
National COMSEC Audit Team (NCAT)	The entity at CSE responsible for conducting COMSEC audits of the COMSEC accounts within the NCMCS.
National COMSEC Incidents Office (NCIO)	The entity at CSE responsible for managing COMSEC incidents through registration, validation, assessment, evaluation and closure, and for direct liaison and coordination with other national and international COMSEC incident offices.
Other Levels of Government (OLG)	Provincial, municipal, and local government organizations (e.g. law enforcement agencies).
Practice Dangerous to Security (PDS)	A COMSEC incident that does not result in the loss of control or unauthorized access to COMSEC material and is considered a minor violation of administrative requirements. **NOTE**: Although a PDS does not result in a compromise of information, assets or functionality, it could create a situation where exploitation or compromise is possible unless action is taken to correct the practice.
Private Sector	Canadian organizations, companies or individuals that do not fall under the FAA or are not subordinate to a provincial or municipal government.

5.3 COMSEC USER PORTAL

Authorized users may access the CSE CUP at https://comsecportal.cse-cst.gc.ca. The CSE CUP provides COMSEC-related UNCLASSIFIED and PROTECTED A information and forms, as well as Field Software Upgrades (FSUs) associated with CSE-approved High Assurance (HA) and Trusted Vendor (TV) products, systems, and services.

For information on becoming an authorized user of the CSE CUP, contact the Crypto Material Assistance Centre (CMAC).

5.4 CANADIAN CENTRE FOR CYBER SECURITY WEBSITE

COMSEC directives and information (UNCLASSIFIED only) associated with CSE-approved HA products, systems, and services are available at https://www.cyber.gc.ca/en/comsec.

5.5 CONTACT INFORMATION

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

Table 2 – Contact Information for COMSEC Offices

COMSEC Client Services (CCS)	
Telephone: 613-991-8495 **Secure Fax:** 613-991-8565	comsec@cyber.gc.ca
Crypto Material Assistance Centre (CMAC) and National Central Office of Record (NCOR)	
Telephone: 613-991-8600 **Fax:** 613-991-7440 **Secure Fax:** 613-998-5686	cmac-camc@cyber.gc.ca
National COMSEC Incidents Office (NCIO)	
Telephone: 613-991-8175 **Unclassified Fax**: 613-990-2737 **Secure Fax**: 613-991-7581 (call 613-991-8175 to set up) ncio@cyber.gc.ca	
CSE Industrial COMSEC Account (CICA)	
Telephone: 613-991-8162	cica-ccic_comsec@cyber.gc.ca

NOTE: Unless specified otherwise, the telephone and secure fax contact numbers listed are attended Monday to Friday, from 8 a.m. to 4 p.m. Eastern Time.

5.6 BIBLIOGRAPHY

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

Communications Security Establishment

- *IT Security Directive for Cryptographic Key Ordering* (ITSD-09), December 2016.
- *IT Security Directive for the Application of Communications Security Using CSE-Approved Solution* (ITSD-01A), January 2014.
- *IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector* (ITSD-06A), June 2016.
- *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), April 2016.
- *IT Security Directive for the Management of CSE-Approved Cryptographic Equipment and Key to Secure a Telecommunications Network* (ITSD-04A), January 2017.

Justice Canada

- *Access to Information Act* (R.S.C., 1985, c. A-1).
- *Financial Administration Act* (R.S.C., 1985, c. F-11).
- *Privacy Act* (R.S.C., 1985, c. P-21).
- *Security of Information Act* (R.S.C., 1985, c. O-5).

Royal Canadian Mounted Police

- *Guide to the Application of Physical Security Zones* (G1-026), September 2005.

Treasury Board of Canada Secretariat

- *Directive on Security Management* (DSM), July 2019.
- *Policy on Government Security* (PGS), July 2019.

Appendix A EXAMPLES OF COMSEC INCIDENTS

A.1 COMPROMISING INCIDENTS

A Compromising Incident (CI) is a COMSEC incident that could result in the loss of control or unauthorized access of COMSEC material, or in a compromise of information, assets or functionality, and may have a serious negative consequence to operational security.

A.1.1 COMPROMISING INCIDENT ASSESSMENT

The act of reporting a Compromising Incident (CI) creates a record of the potential for an event to have resulted in an actual compromise. It is not until a full investigation has occurred that a Compromising Incident (CI) can be assessed as having resulted, or possibly resulted, in a compromise to COMSEC material. Compromising Incidents (CIs) are assessed as follows:

- **Compromise Certain** – the evidence and facts clearly prove that a compromise has occurred;
- **Compromise Possible** – the evidence and facts cannot clearly prove that a compromise has not occurred; or
- **No Compromise** – the evidence and facts clearly prove that a compromise has not occurred.

A.1.2 COMPROMISING INCIDENTS BY CATEGORY

Compromising Incidents (CIs) fall into three categories:

- **Cryptographic** - any malfunction, or COMSEC personnel or operator error that adversely affects the security of COMSEC material;
- **Personnel** - any attempt by, or on behalf of, an unauthorized individual to gain access to COMSEC material, including falsification of COMSEC records to support unauthorized access; and
- **Physical** - any loss of control, theft, capture, recovery by salvage, tampering, unauthorized modification, unauthorized access, or unauthorized photographing that has the potential to jeopardize COMSEC material.

A.1.2.1 COMPROMISING INCIDENT CATEGORY: CRYPTOGRAPHIC

A cryptographic Compromising Incident (CI) is any malfunction, or COMSEC personnel or operator error that adversely affects the security of COMSEC material. Cryptographic Compromising Incidents (CIs) are directly related to improper or unauthorized use of key or cryptographic equipment or systems. Examples of cryptographic Compromising Incidents (CIs) include:

- 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; and
  - Premature use of key;
- The use of cryptographic systems, equipment, and/or software approved by CSE, with 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. For example:
  - Plain text transmission resulting from a cryptographic equipment failure or malfunction;
  - Any transmission during a failure, or after an uncorrected failure that may cause improper operation of cryptographic equipment; and

- Compromising emanations from a cryptographic equipment or system while processing classified information;

- Discussion of the details of a cryptographic equipment failure or malfunction via non-secure communications;
- Activation of the anti-tamper mechanism or unexplained zeroization of a key processor; and
- Any unauthorized use of key or CSE-approved cryptographic equipment.

A.1.2.2 COMPROMSING INCIDENT CATEGORY: PERSONNEL

A personnel Compromising Incident (CI) is any event that involves any attempt by, or on behalf of, an unauthorized individual to gain access to COMSEC material, including falsification of COMSEC records to support unauthorized access. Examples of personnel Compromising Incidents (CIs) include:

- Deliberate falsification of COMSEC records or reports;
- Known or deliberate failing to report a confirmed or suspected COMSEC incident (Compromising Incident [CI] or PDS);
- Unauthorized disclosure, or attempted unauthorized disclosure, of information concerning ACM or other sensitive COMSEC material;
- Processing, storage or transmission of classified or PROTECTED C information on an inappropriate cryptographic equipment or system (accidentally or knowingly);
- Theft; and
- Known or suspected defection or treason, espionage or sabotage, and suspected subversion.

A.1.2.3 COMPROMSING INCIDENT CATEGORY: PHYSICAL

A physical Compromising Incident (CI) is any event that involves the loss of control, theft, capture, recovery by salvage, tamper, unauthorized modification, unauthorized access, or unauthorized photography that has the potential to jeopardize COMSEC material. Examples of physical Compromising Incidents (CIs) include:

- Loss of ACM or other sensitive COMSEC material;
- Unauthorized access to ACM or other sensitive COMSEC material;
- 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;
- Failure to maintain Two Person Integrity (TPI) or No-Lone Zone (NLZ) controls for TOP SECRET key;
- Improper packaging or shipment of COMSEC material;
- Receipt of classified equipment, Controlled Cryptographic Item (CCI) or key marked CRYPTO with a damaged inner wrapper;
- Destruction of COMSEC material by unauthorized 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 or penetration of COMSEC material; and
- Unauthorized copy, reproduction or photography of ACM or other sensitive COMSEC material.

A.1.3 COMPROMISING INCIDENTS BY TYPE

Compromising Incidents (CIs) can be grouped by type. There are nine types and each is described, with examples, in the following articles.

A.1.3.1 COMPROMISING INCIDENT TYPE: ACCOUNTING

Accounting Compromising Incidents (CIs) involve the improper cataloguing and tracking of COMSEC material. Examples include:

- Accounting discrepancies (e.g. misidentified short titles, incorrect serial, register or KMID numbers and/or quantities);
- Removal of ACM from accountability while awaiting destruction or approval for destruction; and
- COMSEC material not listed on current inventory (e.g. found COMSEC material).

A.1.3.2 COMPROMISING INCIDENT TYPE: DAMAGE

Damage Compromising Incidents (CIs) involve breakage, damage, or tamper to COMSEC material. Examples include:

- Accidental damage to COMSEC material caused by, for example, items being dropped on the floor or falling from a vehicle;
- Malicious damage to COMSEC material caused by unauthorized opening or tampering;
- Damage to the inner protective packaging of a parcel containing COMSEC material; and
- Damage to COMSEC material caused by known or suspected unauthorized penetration of COMSEC material.

A.1.3.3 COMPROMISING INCIDENT TYPE: DESTRUCTION

Destruction Compromising Incidents (CIs) relate to the unauthorized or improper destruction of End Cryptographic Units (ECUs) or key. Examples include:

- Incomplete destruction of COMSEC material listed on a duly processed/witnessed GC-223 Destruction Report [DR];
- Inadvertent destruction and removal from accountability of ACM as a result of a clerical error on the GC-223 DR (e.g. incorrect serial number, key short title or edition);
- Destruction of key prior to its scheduled supersession date and subsequent removal from NCMCS accountability;
- Retention of superseded key, including in storage, without authorization;
- Unwitnessed destruction;
- Destruction resulting from a natural disaster (e.g. fire, hurricane, volcanic eruption, earthquake, tsunami); and
- All destruction of COMSEC material in an emergency situation, even when authorized and performed properly.

A.1.3.4 COMPROMISING INCIDENT TYPE: EQUIPMENT

Equipment Compromising Incidents (CIs) relate to equipment errors or problematic operation. Examples include:

- Use of malfunctioning equipment (e.g. defective cryptographic logic circuitry) and transmissions made during an equipment failure (or after an equipment malfunction);
- Failure to perform mandatory firmware/software upgrades to operational ECUs held within specified time period;
- Unexplained zeroization; and
- Improper maintenance including actual or attempted use of maintenance procedures that deviate from established directives, maintenance of cryptographic equipment by unauthorized or unqualified individuals, and unauthorized modifications to cryptographic equipment.

A.1.3.5 COMPROMISING INCIDENT TYPE: LOSS (PERMANENT)

Permanent loss Compromising Incidents (CIs) occur when COMSEC material cannot be physically located or adequately accounted for, or where there is a loss of control of COMSEC material. Examples include:

- Loss of control when COMSEC material is printed, copied, reproduced, or photographed without authorization;
- Loss of COMSEC material where an item cannot be located or adequately accounted for during inventory verification; and
- Theft of COMSEC material where item is not subsequently recovered.

A.1.3.6 COMPROMISING INCIDENT TYPE: LOSS (TEMPORARY)

Temporary loss Compromising Incidents (CIs) occur when COMSEC material is temporarily lost, either physically or as a result of a loss of control. Examples include:

- Temporary loss of control when COMSEC material is discovered outside of required accountability or physical control but that accountability or control is subsequently re-established (e.g. unattended COMSEC vault or secure container is locked shortly after it was discovered open);
- Unauthorized access by an individual without a need-to-know, an appropriate security clearance, a signed COMSEC briefing form, and a signed loan holder responsibility form; and
- Unauthorized disclosure of key status information or details about a cryptographic equipment failure or malfunction via an insufficiently protected system (e.g. unclassified email).

A.1.3.7 COMPROMISING INCIDENT TYPE: MOVEMENT

Movement Compromising Incident (CIs) occur when COMSEC material is transferred from one COMSEC account to another or to a remotely located end user. Examples include:

- Failure by a commercial carrier to provide 24-hour tracking of COMSEC material from its original location to its final destination;
- Improper shipment of COMSEC material (e.g. shipment of an End Cryptographic Unit [ECU] in a keyed state, via unauthorized means, or with its associated Cryptographic Ignition Keys [CIKs], Personal Identification Numbers [PINs] or passwords in the same package);
- Transmission, storage, or processing classified or PROTECTED C information via an inappropriate or insufficiently protected cryptographic system, equipment, or network;
- Improper packaging (e.g. poorly wrapped, insufficiently padded) of COMSEC material; and
- Damage to packages during transit (e.g. outer/inner wrappers may be penetrated).

A.1.3.8 COMPROMISING INCIDENT TYPE: PROCESS

Process Compromising Incidents (CIs) relate to failures to adhere to national COMSEC policy, doctrine, or Standard Operating Procedures (SOPs). Examples include:

- Failure to adhere to established COMSEC doctrine and procedures related to the configuration or operational use of CSE-approved cryptographic systems, equipment, or software;
- Failure to log or conduct audit trail reviews, as prescribed;
- Failure to ensure TPI or NLZ controls for TOP SECRET key;
- Unauthorized extension of cryptoperiod; and
- Unauthorized use of key (e.g. use for other than its intended purpose, premature use, use of compromised, superseded, or defective key, or previously used key that is not authorized for re-use).

A.1.3.9 COMPROMISING INCIDENT TYPE: OTHER

Any Compromising Incident (CI) that cannot be placed into any of the other eight types may be identified as "Other". Examples include:

- Equipment manufacturing error or key production error;
- Unauthorized absence or failing to report as scheduled; and
- Negligence (e.g. deliberately not following instructions).

A.2 PRACTICES DANGEROUS TO SECURITY

A PDS is a COMSEC incident that is considered a minor violation of administrative requirements but does not result in the loss of control or unauthorized access to COMSEC material. Although a PDS does not result in a compromise of information, assets, or functionality, it could create a situation where exploitation or compromise is possible if the practice is not corrected.

A.2.1 PDS BY TYPE

There are six types of PDS. The following articles describe each type and list examples.

A.2.1.1 PDS TYPE: ADMINISTRATION

An administration PDS is any deficiency in the accounting or tracking of COMSEC material. Examples of administration PDS include:

- Missing, incomplete, outdated, or unsigned files including:
  - COMSEC Account or Local Element registration forms or electronic credentials;
  - COMSEC role appointment/termination forms,
  - Accountable COMSEC Material Control Agreements (ACMCAs),
  - COMSEC Emergency Plan (CEPs),
  - GC-223 COMSEC Material Reports for all applicable transactions,
  - COMSEC mail signing authority forms;
  - SOPs, and
  - Exceptions/waivers.
- Key Management Support Plan (KMSP) not in place;
- Failing to perform file updates and/or backups, as required;
- Incorrectly classifying, designating, or marking documents; and
- Failing to make policy directives, doctrine, and other documents required to operate a COMSEC Account readily available to all COMSEC personnel (via CUP access).

A.2.1.2 PDS TYPE: EQUIPMENT

An equipment PDS is any practice that could result in an unauthorized individual gaining access or exposure to equipment (e.g. CCI, ECUs, or secure telephone terminals). Examples of equipment PDS include:

- Failing to store ECUs appropriately (e.g. separate from associated CIKs);
- Failing to perform mandatory firmware/software upgrades to ECUs held in storage (i.e. non-operational) within specified time period;
- Failing to periodically rekey unused or backup ECUs, in a timely manner (e.g. prior to making them operational);
- Failing to monitor ECU activity logs, as required;
- Failing to maintain battery husbandry processes;
- Failing to set correct time on Tier 3 Management Devices (T3MDs);

- Holding surplus COMSEC material in inventory; and
- Holding unserviceable ECUs in storage, except while awaiting CCS authority to destroy or for a Return of Material Authority (RMA) from the manufacturer for repair.

A.2.1.3 PDS TYPE: INVENTORY

An inventory PDS is any occurrence where inventory management requirements are not met. Examples of inventory PDS include:

- Using COMSEC accounting procedures that are not approved for use;
- Using a Distributed INFOSEC Accounting Software (DIAS) version that is out of date or no longer approved for use;
- Missing, incomplete, or outdated Loan Holder responsibility forms;
- Failing to annually renew/verify hand receipts;
- Failing to physically sight COMSEC material during verification of COMSEC inventory;
- Failing to page check ACM publications prior to transfer, return, or during COMSEC inventory verifications;
- Failing to muster or verify CIKs (ECU, T3MD or Field Tamper Recovery [FTR]), as stipulated in supporting doctrine (e.g. annually or semi-annually);
- Missing COMSEC Custodial personnel, loan holder, or witness signatures on COMSEC inventory reports; and
- Failing to reconcile the COMSEC inventory with the NCOR.

A.2.1.4 PDS TYPE: PROCESS AND PROCEDURE

A process and procedure PDS is any failure to follow established COMSEC processes or procedures as specified by national COMSEC directives, doctrine, and SOPs. Examples of process and procedure PDS include:

- Failing to assign at least one alternate COMSEC Custodian;
- Failing to complete mandatory COMSEC training or recommended cryptographic handling courses, where appropriate;
- Failing to assume, or inability to assume, the responsibilities of COMSEC Custodian, when required (applies to Alternate COMSEC Custodian);
- Failing to notify recipient of incoming COMSEC shipment;
- Improperly/inadequately managing COMSEC material entrusted to care and control of COMSEC Account or authorized end users;
- Improper completion of the Electronic Key Management System (EKMS) Local COMSEC Management System (LCMS) archive process;
- Receiving package containing COMSEC material with a damaged outer wrapper (inner wrapper intact, i.e. not ripped or otherwise damaged) but no evidence of any other tampering;
- Holding unauthorized key (e.g. due to improper short title or the key is associated ECU not held by account);
- Explainable zeroization or activation of anti-tamper mechanism when there are no other indications of tamper, unauthorized access to, or penetration of COMSEC material;
- Using key prematurely or out-of-sequence without prior approval of the ConAuth or CmdAuth, as applicable;
- Inadvertently destroying key without authorization (but destruction was properly performed and documented);
- Removing key from its protective packaging prior to operational use or without authorization (provided the removal was appropriately documented, all exposed key was under positive control, and there is no reason to suspect that the key was compromised);

- Failing to destroy accountable equipment and accountable publications in a timely manner, provided item was always properly stored and NCMCS-accountable;
- Failing to periodically rekey Secure Communications Interoperability Protocol (SCIP) devices; and
- Failing to destroy key on a T3MD following fill to ECU within time limits specified in supporting COMSEC policy and doctrine.

A.2.1.5 PDS TYPE: SECURITY

A security PDS is any practice where the physical security measures recommended by the Royal Canadian Mounted Police (RCMP) for the care and control of COMSEC material are not properly implemented. Examples of security PDS include:

- Missing, incomplete, or outdated Threat and Risk Assessment (TRA) for COMSEC facility;
- Affixing unauthorized labels to COMSEC equipment;
- Missing/damaged tamper labels;
- Failing to verify an individual's need-to-know, Canadian citizenship, clearance level, and requirement for access prior to issuing COMSEC material;
- Failing to ensure all COMSEC personnel and authorized users are COMSEC briefed;
- Failing to store COMSEC material using RCMP-approved containers and/or locks;
- Failing to periodically change lock combinations, as prescribed;
- Failing to properly segregate COMSEC material in storage by classification;
- Failing to change a Site Security Officer (SSO) passwords or supervisor PINs, as prescribed;
- Unauthorized access or use of SSO passwords and/or supervisor PINs during operations; and
- Loss of T3MD audit trail data during exceptional circumstances (e.g. DCA/ECA authorized continued use of T3MD with full audit trail).

A.2.1.6 PDS TYPE: OTHER

Any PDS that can not be placed into any of the other five types may be identified as "Other".