Directive
for
Reporting and Evaluating COMSEC Incidents
Involving
Accountable COMSEC Material

ITSD-05
Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material (ITSD-05)

Foreword

The Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material (ITSD-05) is an UNCLASSIFIED publication issued under the authority of the Chief, Communications Security Establishment Canada in accordance with the Treasury Board of Canada Secretariat Policy on Government Security.

This Directive is aligned with the Directive for the Application of Communications Security in the Government of Canada (ITSD-01) and the Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03).

The Communications Security Establishment Canada will issue appropriate direction to notify users of changes to this directive.

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

Effective Date

This directive takes effect on date of signature.

 Originally signed by

Toni Moffa
Deputy Chief, IT Security

April 16, 2012
Date


It is permissible to reproduce or make extracts from this publication provided it is used for Government of Canada departmental use. Reproduction of multiple copies of this publication for the purpose of commercial redistribution is prohibited except with written permission from the Government of Canada’s copyright administrator, Public Works and Government Services Canada.
Directive for Reporting and Evaluating COMSEC Incidents
Involving Accountable COMSEC Material (ITSD-05)

This page intentionally left blank.
Record of Amendments

<table>
<thead>
<tr>
<th>Amendment No.</th>
<th>Date</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

Foreword....................................................................................................................... i
Record of Amendments............................................................................................... iii
List of Tables ............................................................................................................... vii

1 Introduction ........................................................................................................... 1
  1.1 Purpose........................................................................................................ 1
  1.2 Authority ....................................................................................................... 1
  1.3 Scope ............................................................................................................ 1
  1.4 Definitions .................................................................................................... 1
  1.5 Context ......................................................................................................... 2
  1.6 Application.................................................................................................... 2
  1.7 Expected Results ......................................................................................... 3
  1.8 Compliance .................................................................................................. 3
  1.9 Consequence of Non-Compliance................................................................. 3
    1.9.1 Disciplinary Action............................................................................. 3
  1.10 Requests for Exceptions or Waivers ............................................................ 3
  1.11 Contact Information...................................................................................... 4
  1.12 COMSEC User Portal................................................................................... 4
  1.13 Communications Security Establishment Canada – Web Site ..................... 5

2 Roles and Responsibilities................................................................................... 7
  2.1 Communications Security Establishment Canada........................................ 7
    2.1.1 National COMSEC Incident Office .................................................... 7
  2.2 Departmental Security Officer ...................................................................... 7
  2.3 Departmental COMSEC Authority ............................................................... 8
  2.4 Controlling Authority ................................................................................... 8
  2.5 COMSEC Custodian .................................................................................... 8

3 COMSEC Incidents – Classes and Categories ................................................... 9
  3.1 General ......................................................................................................... 9
    3.1.1 Practice Dangerous to Security ............................................................. 9
    3.1.2 Compromising ....................................................................................... 9
      3.1.2.1 Cryptographic ............................................................................. 9
      3.1.2.2 Personnel .............................................................................. 9
      3.1.2.3 Physical.................................................................................. 10

4 Practice Dangerous to Security – Reporting and Handling............................. 11
  4.1 General ........................................................................................................ 11
  4.2 Private Sector.............................................................................................. 11

5 Compromising Incident - Reporting and Handling ........................................ 13
  5.1 General ........................................................................................................... 13
Directive for Reporting and Evaluating COMSEC Incidents
Involving Accountable COMSEC Material (ITSD-05)

5.2 Reporting a Compromising Incident ........................................................... 13
5.2.1 Private Sector ................................................................................. 13
5.3 Roles and Responsibilities ......................................................................... 13
5.3.1 Controlling Authority ........................................................................ 13
5.3.2 COMSEC Custodian ....................................................................... 14
5.3.3 Departmental COMSEC Authority .................................................. 14

6 Investigations, Reports and Evaluations .......................................................... 15
6.1 General ...................................................................................................... 15
6.2 Initial Investigation...................................................................................... 15
6.3 COMSEC Incident Reports ........................................................................ 15
6.3.1 General........................................................................................... 15
6.3.2 COMSEC Incident Initial Report ..................................................... 15
6.3.3 COMSEC Incident Evaluation Report ............................................. 16
6.3.4 Amplifying Report............................................................................ 16
6.3.5 Final Assessment and Closure Report............................................ 16

7 Classification and Dissemination ...................................................................... 17
7.1 Classification........................................................................................... 17
7.2 Dissemination............................................................................................. 17

8 Glossary............................................................................................................... 19

9 Bibliography ........................................................................................................ 23
9.1 Legislation ................................................................................................. 23
9.2 Treasury Board of Canada Secretariat....................................................... 23
9.3 Communications Security Establishment Canada ...................................... 23

Annex B – Compromising Incidents (Cryptographic) - Examples ...................... B-1
Annex C – Compromising Incidents (Personnel) - Examples ............................. C-1
Annex D – Compromising Incidents (Physical) Examples ................................. D-1
Annex E – COMSEC Incident Initial Report - Template .....................................E-1
Annex F – Compromising Incident Action Flow Chart .......................................F-1
List of Tables

Table 1 – Contact Information ................................................................. 4
Directive for Reporting and Evaluating COMSEC Incidents
Involving Accountable COMSEC Material (ITSD-05)

This page intentionally left blank.
List of Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM</td>
<td>Accountable COMSEC Material</td>
</tr>
<tr>
<td>ALC</td>
<td>Accounting Legend Code</td>
</tr>
<tr>
<td>CA</td>
<td>Controlling Authority</td>
</tr>
<tr>
<td>CCEB</td>
<td>Combined Communications Electronics Board</td>
</tr>
<tr>
<td>CCI</td>
<td>Controlled Cryptographic Item</td>
</tr>
<tr>
<td>CFD</td>
<td>Common Fill Device</td>
</tr>
<tr>
<td>CICA</td>
<td>CSEC Industrial COMSEC Account</td>
</tr>
<tr>
<td>CMAC</td>
<td>Crypto Material Assistance Centre</td>
</tr>
<tr>
<td>COMSEC</td>
<td>Communications Security</td>
</tr>
<tr>
<td>cryptonet</td>
<td>Cryptographic Network</td>
</tr>
<tr>
<td>CSEC</td>
<td>Communications Security Establishment Canada</td>
</tr>
<tr>
<td>CUP</td>
<td>COMSEC User Portal</td>
</tr>
<tr>
<td>DAO</td>
<td>Department, Agency or Organization</td>
</tr>
<tr>
<td>DCA</td>
<td>Departmental COMSEC Authority</td>
</tr>
<tr>
<td>DGSM</td>
<td>Directive on Departmental Security Management</td>
</tr>
<tr>
<td>DSO</td>
<td>Departmental Security Officer</td>
</tr>
<tr>
<td>FAA</td>
<td>Financial Administration Act</td>
</tr>
<tr>
<td>FSU</td>
<td>Field Software Upgrade</td>
</tr>
<tr>
<td>GC</td>
<td>Government of Canada</td>
</tr>
<tr>
<td>ICMCM</td>
<td>Industrial COMSEC Material Control Manual</td>
</tr>
<tr>
<td>IP</td>
<td>In-Process</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITSD</td>
<td>Information Technology Security Directive</td>
</tr>
<tr>
<td>KMID</td>
<td>Key Material Identifier</td>
</tr>
<tr>
<td>KP</td>
<td>Key Processor</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NCIO</td>
<td>National COMSEC Incidents Office</td>
</tr>
<tr>
<td>NCMCS</td>
<td>National COMSEC Material Control System</td>
</tr>
<tr>
<td>NCOR</td>
<td>National Central Office of Record</td>
</tr>
<tr>
<td>NLZ</td>
<td>No-Lone Zone</td>
</tr>
<tr>
<td>OLG</td>
<td>Other Levels of Government</td>
</tr>
<tr>
<td>PDS</td>
<td>Practice Dangerous to Security</td>
</tr>
<tr>
<td>PGS</td>
<td>Policy on Government Security</td>
</tr>
<tr>
<td>TPI</td>
<td>Two Person Integrity</td>
</tr>
<tr>
<td>T3MD</td>
<td>Tier 3 Management Device</td>
</tr>
</tbody>
</table>
This page intentionally left blank.
1 Introduction

1.1 Purpose

The purpose of this directive is to provide minimum requirements for reporting and evaluating Communications Security (COMSEC) incidents involving Accountable COMSEC Material (ACM). In addition to sovereign requirements, this directive is consistent with allied COMSEC incident reporting processes.

1.2 Authority

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

1.3 Scope

This directive applies to COMSEC incidents involving ACM. It also applies to In-Process accounting and control (refer to the Directive for the Control of COMSEC Material in the Government of Canada [ITSD-03]), as well as North Atlantic Treaty Organization (NATO), Combined Communications Electronics Board (CCEB) and Allied ACM that has been entrusted to Canada through international partnership agreements.

1.4 Definitions

The following definitions apply for this directive:

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

Accountable COMSEC Material – COMSEC material that requires control and accountability within the National COMSEC Material Control System (NCMCS) in accordance with its Accounting Legend Code (ALC) and for which transfer or disclosure could be detrimental to the national security of Canada.

COMSEC Incident – Any occurrence that jeopardizes or potentially jeopardizes the security of classified or protected Government of Canada information while it is being stored, processed, transmitted or received during the telecommunications process.
Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material (ITSD-05)

National COMSEC Incidents Office – The entity at CSEC 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.

Refer to the glossary for additional definitions of terms used in this directive.

1.5 Context

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

- Directive for the Application of Communications Security in the Government of Canada (ITSD-01) January 2005; and


1.6 Application

This directive applies to:

- Government of Canada (GC) departments within the meaning of Schedules I, I.1, II, IV and V of the Financial Administration Act (FAA), unless excluded by specific acts, regulations or Orders in Council;

- GC departments not listed in the above mentioned FAA schedules, but that have entered into a written agreement with the Treasury Board of Canada Secretariat (TBS) to adopt the requirements of the PGS; and

- private sector companies that are sponsored by a GC department (Refer to ITSD-01 for sponsorship requirements) and are managing ACM as detailed in the Industrial COMSEC Material Control Manual (ICMCM). If a situation arises that is not covered by the ICMCM, or a discrepancy arises between it and the contents of this directive, this directive takes precedence.

NOTE: The Directive for the Control of COMSEC Material in the Canadian Private Sector (ITSD-06) will supersede the ICMCM in the near future.

NOTE: For the purpose of this directive:

- the term “GC department” includes any federal institution (e.g. Department, Agency, Organization [DAO]) subject to the FAA and PGS; and

- the term “private sector company” includes companies, organizations or individuals that do not fall under the FAA or are not subordinate to a provincial or municipal government.
1.7 Expected Results

The implementation of this directive will enable early mitigation and final resolution of a loss or compromise of ACM, information or services. It will also ensure that Canada’s commitments to safeguard and control ACM obtained through international partnership agreements meet partner’s security requirements.

1.8 Compliance

GC departments and private sector companies identified in Article 1.6 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 and private sector company, it does not preclude a GC department or private sector company from applying more stringent requirements within their department or company.

1.9 Consequence of Non-Compliance

Failure to comply with this directive may result in compromise to national security and the security of Canada’s international partners.

In cases of non-compliance, CSEC may escalate administrative control of a department’s COMSEC account, including temporary suspension.

1.9.1 Disciplinary Action

Disciplinary action, if deemed warranted by circumstance, is entirely in the purview of the GC departmental authorities (e.g. Departmental Security Officer [DSO]). Failure to report a COMSEC incident, or cover it up, may be considered “wilful or gross neglect” and must be evaluated accordingly.

1.10 Requests for Exceptions or Waivers

Requests for exceptions (substitution) or waivers (an exemption from a specific requirement) to any of the direction contained herein must be submitted to COMSEC Client Services at CSEC for approval. Requests must be submitted in writing and include justification.

NOTE: Exceptions and waivers are designed to be remedial and of limited duration.
1.11 Contact Information

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

**NOTE:** Unless otherwise specified, CSEC’s telephone and secure facsimile contact numbers listed are operational from 8 a.m. to 4 p.m. Eastern Standard Time, Monday-Friday.

<table>
<thead>
<tr>
<th>Office</th>
<th>Phone Numbers</th>
<th>E-mail Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMSEC Client Services</td>
<td>613-991-8495</td>
<td><a href="mailto:comsecclientservices@cse-cst.gc.ca">comsecclientservices@cse-cst.gc.ca</a></td>
</tr>
<tr>
<td>Crypto Material Assistance Centre (CMAC) and National Central Office of Record (NCOR)</td>
<td>613-991-8600</td>
<td><a href="mailto:cmac-camc@cse-cst.gc.ca">cmac-camc@cse-cst.gc.ca</a></td>
</tr>
</tbody>
</table>
| National COMSEC Incidents Office (NCIO) | Telephone: 613-991-8175
BlackBerry: 613-355-4467
Unclassified Facsimile: 613-991-7588
Classified Facsimile: Call 613-991-8175 for set up
**After office hours:**
SGSM: 613-668-3537 (U)
613-513-1384 (S)
Blackberry: 613-355-4467 | ncio@cse-cst.gc.ca |
| CSEC Industrial COMSEC Account (CICA) | 613-991-8162 | cica-ccic@cst-cst.gc.ca |

1.12 COMSEC User Portal

Authorized users may access the CSEC COMSEC User Portal (CUP) at
The CSEC CUP provides COMSEC-related information and Field Software Upgrades (FSUs), up to PROTECTED A, associated with high assurance products, systems and services. For information on becoming an authorized user of the CSEC CUP, contact the CMAC at CSEC.

1.13 Communications Security Establishment Canada – Web Site

Other COMSEC directives and information (UNCLASSIFIED only) associated with high assurance products, systems and services are available at http://www.cse-cst.gc.ca/its-sti/publications/index-eng.html.
2 Roles and Responsibilities

2.1 Communications Security Establishment Canada

The Deputy Chief, Information Technology Security (DCITS) at CSEC, or a CSEC authority delegated by the DCITS, is the final adjudicator for Final Assessment and Closure of all compromising COMSEC incidents, involving ACM.

2.1.1 National COMSEC Incident Office

Under the direction of the DCITS at CSEC, the National COMSEC Incidents Office (NCIO) responsibilities include:

a. verifying and documenting compromising incidents;
b. coordinating multi-departmental incident reporting;
c. coordinating cross border incident resolution with international partners;
d. determining the need for and appropriateness of compromising incident recovery actions;
e. notifying applicable authorities of recovery actions taken;
f. providing compromising incident final assessment and closure reports;
g. maintaining a national database of all compromising incidents; and
h. providing an annual trend and analysis report of all COMSEC incidents.

2.2 Departmental Security Officer

The DSO is appointed by the Department Deputy Head. Among other duties, as listed in the PGS, the DSO is responsible to manage the departmental security program. For more information on the roles and responsibilities of the DSO, consult the DDSM document.

The DSO must establish:

a. internal COMSEC incident identification and response procedures that will ensure prompt and accurate reporting of COMSEC incidents and that will minimize the potential for or actual loss or compromise of ACM material;
b. an awareness program that will ensure each individual having access to ACM is aware of what constitutes a COMSEC incident and the importance of prompt, complete and accurate reporting; and

c. departmental COMSEC incident monitoring to include sponsored Other Levels of Government (OLG) and private sector companies.
2.3 Departmental COMSEC Authority

A Departmental COMSEC Authority (DCA) may be appointed by the DSO, to act in his/her stead, to manage the departmental COMSEC program. The DCA is responsible to the DSO for developing, implementing, maintaining, coordinating and monitoring a departmental COMSEC program that is consistent with the PGS and related policy instruments.

NOTE: In departments where a DCA is not appointed, the DSO must assume the roles and responsibilities of the DCA.

2.4 Controlling Authority

A Controlling Authority (CA) must ensure cryptographic network (cryptonet) members are aware of the procedures to be followed in the event of a COMSEC incident.

CA responsibilities include:

- reporting a COMSEC incident to the responsible DCA or COMSEC Custodian;
- initiating cryptographic key compromise recovery action as detailed in ITSD-04; and

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 also used to refer to both singular and multiple quantities of key.

- providing assistance, when requested, in a COMSEC incident investigation or completion of a COMSEC Initial Incident Report.

2.5 COMSEC Custodian

The COMSEC Custodian must ensure that each individual who uses, or otherwise has access to ACM, is capable of recognizing a COMSEC incident and understands the importance of expeditiously reporting a COMSEC incident.
3 COMSEC Incidents – Classes and Categories

3.1 General

COMSEC incidents involving ACM fall into two classes: Practice Dangerous to Security (PDS) or Compromising.

3.1.1 Practice Dangerous to Security

A PDS incident is an incident that does not result in the loss of control, unauthorized access or viewing of ACM and is considered a minor violation of administrative requirements. Although a PDS does not result in a compromise of information, assets or functionality, it could create a situation where exploitation or compromise of ACM is possible unless action is taken to correct the practice.

Annex A provides an example listing of possible practices dangerous to security.

3.1.2 Compromising

A compromising incident is an incident that results in loss of control, unauthorized access or viewing of ACM and that may have a serious negative consequence to operational security. It also results in the compromise of information, assets or functionality. Investigation of a compromising incident will determine the impact to security, as well as recovery from compromise requirements.

Compromising incidents involving ACM fall into three categories: cryptographic, personnel and physical.

3.1.2.1 Cryptographic

Cryptographic incidents are directly related to the improper or unauthorized use of key and/or cryptographic equipment or systems. Annex B provides an example listing of possible cryptographic incidents.

3.1.2.2 Personnel

Personnel incidents are situations involving individuals who have access to ACM, which could jeopardize the security of that ACM. Annex C provides an example listing of possible personnel incidents.
3.1.2.3 Physical

Physical incidents are situations that adversely affect the physical security of ACM. Annex D provides an example listing of possible physical incidents.

**NOTE:** Equipment specific doctrine provides a list of COMSEC incidents specific to the equipment identified in the doctrine.
4 Practice Dangerous to Security – Reporting and Handling

4.1 General

Every person who handles or otherwise has access to ACM must promptly report a PDS (confirmed or suspected) to the DCA.

A PDS is considered an administrative infraction that is investigated and resolved locally by the DCA in accordance with departmental procedures. Even a minor violation may warrant an evaluation.

To address national trend analysis and audit processing, DCAs must record and track all PDS within their departments. Additionally, the DCA must provide a written subjective assessment of these records to the NCIO during the department’s annual COMSEC audit.

The NCIO must be informed of a PDS if the DCA believes that there is a possibility for a similar PDS occurring within another department.

NOTE: If in doubt as to whether or not an incident is a PDS or a compromising incident, consult the NCIO or report as a compromising incident.

4.2 Private Sector

Canadian private sector companies must immediately report all PDS incidents to the CICA, including those that involve In-Process (IP) COMSEC material (refer to ITSD-03), as detailed in the ICMCM. CICA must handle all practices dangerous to security as detailed in this directive.

NOTE: ITSD-06 will supersede the ICMCM in the near future.
This page intentionally left blank.
5 Compromising Incident - Reporting and Handling

5.1 General

A compromising incident (confirmed or suspected) must always be reported to the NCIO.

Although it is the DCA’s responsibility to report a compromising incident, the DCA may delegate preliminary investigation and reporting to the COMSEC Custodian in times of the DCA’s absence or unavailability as long as there is no conflict of interest (i.e. the Custodian is not implicated in the incident).

5.2 Reporting a Compromising Incident

Every person who handles or otherwise has access to ACM must promptly report all compromising incidents (confirmed or suspected) to their COMSEC Custodian.

Prompt and accurate reporting of a compromising incident will minimize the potential for a compromise of ACM and the information that it protects. It will allow corrective action to be implemented in a timely manner to mitigate or eliminate the impact to COMSEC.

A compromising incident involving ACM, regardless of origin of material (e.g. Canadian, Allied, NATO), must be reported to the NCIO within 24 hours from the time the incident (confirmed or suspected) was reported.

5.2.1 Private Sector

Canadian private sector companies must immediately report all compromising incidents (confirmed or suspected) to CICA, including those that involve IP COMSEC material (refer to ITSD-03), as detailed in ICMCM. CICA must handle all compromising incidents as detailed in this directive.

NOTE: ITSD-06 will supersede the ICMCM in the near future.

5.3 Roles and Responsibilities

5.3.1 Controlling Authority

Upon discovery or notification that a compromising incident has occurred, the CA must:

a. if deemed necessary, take immediate recovery action as detailed in ITSD-04; and

b. report the incident to the responsible DCA or COMSEC Custodian (i.e. the COMSEC Account that is accountable for the ACM in question).
5.3.2 COMSEC Custodian

Upon discovery or notification that a compromising incident has occurred, the COMSEC Custodian must:

- immediately report the incident to the DCA;
- place all items of affected ACM in quarantine and mark as “Pending Investigation” in the COMSEC material inventory file (refer to ITSD-03); and
- maintain accountability for the ACM until the COMSEC investigation is complete and a Final Assessment and Closure Report has been received from CSEC authorizing the disposition of the ACM (e.g. transfer to CSEC for evaluation, destruction, and relief from accountability).

5.3.3 Departmental COMSEC Authority

Upon discovery or notification that a compromising incident has taken place, the DCA must, within 24 hours:

a. conduct a preliminary investigation, verify the validity of the report and determine any immediate corrective action required;

b. report the incident to the DSO;

c. submit a COMSEC Incident Initial Report (refer to Annex E) to the NCIO;

d. inform all individuals within and outside of the GC department who have a need to be aware of the incident; and

e. on request, submit a COMSEC Incident Evaluation Report to the NCIO.

NOTE 1: If the compromise involves cryptographic equipment or key that is used on a cryptonet, the cryptonet CA must be consulted prior to compromise recovery action (refer to ITSD-04) being taken (e.g. supersession of key).

NOTE 2: The DCA must consider the impact of corrective action or inaction on national and international security.
6 Investigations, Reports and Evaluations

6.1 General

The DCA who is initially made aware of a compromising incident must submit a COMSEC Incident Initial Report (refer to Annex E) to the NCIO.

Annex F provides a compromising incident action flow chart.

6.2 Initial Investigation

The DCA must complete a preliminary investigation (within 24 hours) to determine if the incident is a compromising incident or a PDS. If it is determined that the incident is a PDS, the DCA must take action as detailed in Chapter 4. If the initial investigation indicates that there was a compromise of ACM or that a compromise cannot be ruled out, the DCA must submit a COMSEC Incident Initial Report.

6.3 COMSEC Incident Reports

6.3.1 General

COMSEC incident reports are used as the basis for identifying trends in incident occurrences and for developing procedural and doctrinal measures to prevent recurrence of similar incidents.

6.3.2 COMSEC Incident Initial Report

A COMSEC Incident Initial Report is required for every compromising incident involving ACM.

The COMSEC Incident Initial Report can be submitted to the NCIO by secure phone or secure facsimile (refer to Article 1.11). The COMSEC Incident Initial Report must provide, as a minimum, the following information:

- identification of the COMSEC Account in which the incident occurred;
- category of the incident (i.e. Cryptographic, Personnel and/or Physical);
- identification of all ACM involved including short title(s), edition and segment of key(s) loaded in cryptographic equipment, accounting numbers (e.g. Key Material Identifier (KMID), classification, responsible CA and key expiry or supersession date;
- identity of all individual(s) involved including name, citizenship, position and security clearance level;
- description of circumstances surrounding the incident including the date of incident or discovery and the date reported;
- name of the DCA responsible for investigating and evaluating the incident;
- immediate corrective action(s) taken, or planned; and
Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material (ITSD-05)

- possibility of a compromise (i.e. “Certain”, “Possible” or “Impossible”).

**NOTE:** The following definitions apply:

- **Certain** - available evidence and facts clearly prove that compromise has occurred (i.e. ACM was made available to unauthorized personnel)
- **Possible** - evidence and facts cannot clearly prove that a compromise has not occurred
- **Impossible** - evidence and facts clearly prove that ACM was not made available to an unauthorized person

**NOTE:** Refer to Annex E – Initial COMSEC Incident Report – Template.

### 6.3.3 COMSEC Incident Evaluation Report

A COMSEC Incident Evaluation Report provides the NCIO with the required details and facts surrounding a COMSEC incident and helps in finalizing impact assessment and recovery requirements.

Once the NCIO has reviewed the COMSEC Incident Initial Report, the NCIO will request, except for very minor cases which will be determined by the NCIO, a COMSEC Incident Evaluation Report. The request will include the requirement to provide:

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

### 6.3.4 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 NCIO.

### 6.3.5 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 responsible DCA(s) who must report the closure to the DSO. The report will include recommendations to prevent or reduce the possibility of the recurrence of a similar incident. It will also provide disposition instructions for the affected ACM. The NCIO will verify that the report’s recommendations have been implemented.
7 Classification and Dissemination

7.1 Classification

A COMSEC incident report must be protected, handled and reported at a level 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 DCA 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).

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. Personal information must be protected as detailed in the Privacy Act.
# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accountable COMSEC Material (ACM)</strong></td>
<td>COMSEC material that requires control and accountability within the National COMSEC Material Control System (NCMCS) in accordance with its Accounting Legend Code (ALC) and for which transfer or disclosure could be detrimental to the national security of Canada.</td>
</tr>
<tr>
<td><strong>Canadian Cryptographic Doctrine (CCD)</strong></td>
<td>The minimum security standards for the safeguard, control and use of Communications Security Establishment Canada-approved cryptographic equipment and systems.</td>
</tr>
<tr>
<td><strong>Common Fill Device (CFD)</strong></td>
<td>One of a family of devices developed to read-in, transfer, or store key (e.g. KOI-18, KYK-13 and KYX-15).</td>
</tr>
<tr>
<td><strong>Communications Security (COMSEC)</strong></td>
<td>The application of cryptographic security, transmission and emission security, physical security measures, operational practices and controls to deny unauthorized access to information derived from telecommunications and that ensure the authenticity of such telecommunications.</td>
</tr>
<tr>
<td><strong>Compromising Incident</strong></td>
<td>An incident that results in loss of control, unauthorized access or viewing of Accountable COMSEC Material and that may have a serious negative consequence to operational security.</td>
</tr>
<tr>
<td><strong>COMSEC Account</strong></td>
<td>An administrative entity identified by an Electronic Key Management System Identifier (i.e. COMSEC Account number), used to maintain accountability, custody and control of COMSEC material that has been entrusted to the entity.</td>
</tr>
</tbody>
</table>
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COMSEC Custodian</strong></td>
<td>The individual designated by the Departmental COMSEC Authority to be responsible for the receipt, storage, access, distribution, accounting, disposal and destruction of all COMSEC material that has been charged to the departmental COMSEC Account.</td>
</tr>
<tr>
<td><strong>COMSEC Incident</strong></td>
<td>Any occurrence that jeopardizes or potentially jeopardizes the security of classified or protected Government of Canada information while it is being stored, processed, transmitted or received during the telecommunications process.</td>
</tr>
<tr>
<td><strong>COMSEC Material</strong></td>
<td>Material designed to secure or authenticate telecommunications information. COMSEC material includes, but is not limited to key, equipment, modules, devices, documents, hardware, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.</td>
</tr>
<tr>
<td><strong>Controlled Cryptographic Item (CCI)</strong></td>
<td>Unclassified secure telecommunications or information handling equipment, or associated cryptographic components, that are governed by a special set of control requirements within the National COMSEC Material Control System and marked &quot;CONTROLLED CRYPTOGRAPHIC ITEM&quot; or, where space is limited, &quot;CCI&quot;.</td>
</tr>
<tr>
<td><strong>CRYPTO</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Cryptographic Equipment</strong></td>
<td>Communications Security Establishment Canada-approved cryptographic equipment (equipment that embodies a cryptographic logic) and systems designed to protect classified and/or PROTECTED information and data for the Government of Canada. It may also include crypto ancillary, crypto production, and authentication equipment.</td>
</tr>
</tbody>
</table>
**Glossary**

**April 2012**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Key</td>
<td>Information used to set up and periodically change the operations performed in cryptographic equipment for the purpose of encrypting and decrypting electronic signals and digital signatures, determining electronic countermeasure patterns, or producing other key.</td>
</tr>
<tr>
<td>Cryptoperiod</td>
<td>A specific period of time during which a cryptographic key is in effect.</td>
</tr>
<tr>
<td>Crypto Material Assistance Centre (CMAC)</td>
<td>The entity within the Communications Security Establishment Canada responsible for all aspects of key ordering including privilege management, the management of the National Central Office of Record and the administration of the Assistance Centre.</td>
</tr>
<tr>
<td>Departmental COMSEC Authority (DCA)</td>
<td>The individual designated by, and responsible to, the Departmental Security Officer for developing, implementing, maintaining, coordinating and monitoring a departmental COMSEC program which is consistent with the <em>Policy on Government Security</em> and its standards.</td>
</tr>
<tr>
<td>Departmental Security Officer (DSO)</td>
<td>The individual responsible for developing, implementing, maintaining, coordinating and monitoring a departmental security program consistent with the <em>Policy on Government Security</em> and its standards.</td>
</tr>
<tr>
<td>Government of Canada (GC) Department</td>
<td>Any federal department, organization, agency or institution subject to the <em>Policy on Government Security</em>.</td>
</tr>
<tr>
<td>Key</td>
<td>See Cryptographic Key.</td>
</tr>
<tr>
<td>Local Element</td>
<td>Individual registered at a COMSEC Account or COMSEC Sub-Account who may receive COMSEC material from that account.</td>
</tr>
<tr>
<td>National Central Office of Record (NCOR)</td>
<td>The entity at the Communications Security Establishment Canada responsible for maintaining records of accountability for all accountable COMSEC material, produced in, or entrusted to, Canada.</td>
</tr>
</tbody>
</table>
# Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material (ITSD-05)

| **National COMSEC Incidents Office (NCIO)** | The entity at CSEC 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. |
| **National Interest** | Concerns the defence and maintenance of the social, political and economic stability of Canada. |
| **Other Levels of Government (OLG)** | Provincial, municipal and local government organizations (e.g. law enforcement agencies). |
| **Private Sector** | Canadian organizations, companies or individuals that do not fall under the *Financial Administration Act* or are not subordinate to a provincial or municipal government. |
| **Tier 3 Management Device (T3MD)** | A Communications Security Establishment Canada-approved device (e.g. AN/CYZ-10/10A, KIK-20 and AN/PYQ-10), that securely stores, transports and transfers (electronically) both COMSEC and TRANSEC key and that is programmable to support modern mission systems. Designed to be backwards compatible with previous generations of common fill devices. |
| **Two Person Integrity (TPI)** | A control procedure whereby TOP SECRET key material and other specified key material is never handled or made available to one individual only. |
9 Bibliography

The following references were used in the preparation of this directive:

9.1 Legislation

- *Security of Information Act*.
- *Access to Information Act*.
- *Privacy Act*.
- *Financial Administration Act (FAA)*.

9.2 Treasury Board of Canada Secretariat


9.3 Communications Security Establishment Canada

This page intentionally left blank.
Annex A – Practices Dangerous to Security - Examples

The following list provides examples (not meant to be all inclusive) of Communications Security (COMSEC) incidents that may be considered practices dangerous to security.

<table>
<thead>
<tr>
<th>Practice Dangerous to Security</th>
<th>Report to:</th>
</tr>
</thead>
</table>
|                                                                                               | Departmenta
t1 COMSEC Authority | COMSEC Custodian | Controllin
g Authority |
| Premature or out-of-sequence use of key without the approval of the cryptographic network (cryptonet) Controlling Authority (CA). | X                                   | X                  | X                  |
| Inadvertent destruction of key without authorization, as long as the destruction was properly performed and documented. | X                                   | X                  | X                  |
| Removing key from its protective packaging prior to issue for use, or removing the protective packaging without authorization, as long as the removal was documented, the exposed key was properly protected, and there was no reason to suspect compromise. | X                                   | X                  |                     |
| Receipt of a package with damaged outer wrapper, but an intact inner wrapper.                      | X                                   | X                  |                     |
| Except for a Key Processor (KP), activation of the anti-tamper mechanism or unexplained zeroization of accountable cryptographic equipment as long as there were no other indications of unauthorized access or penetration. | X                                   | X                  |                     |
| Failure to zeroize key from a Common Fill Device (CFD) or Tier 3 Management Device (T3MD) Within the time limits as detailed in ITSD-03. | X                                   | X                  |                     |
### Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material (ITSD-05)

<table>
<thead>
<tr>
<th>Practice Dangerous to Security</th>
<th>Report to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Departmental COMSEC Authority</td>
</tr>
<tr>
<td>Destruction of Accountable COMSEC Material (ACM) not performed within required time limits as long as the material was always appropriately controlled and accounted for.</td>
<td>X</td>
</tr>
<tr>
<td>Loss of audit trail data in a T3MD due to the failure to upload when the time and means are unavailable.</td>
<td>X</td>
</tr>
</tbody>
</table>
Annex B – Compromising Incidents (Cryptographic) - Examples

The following list provides examples (not meant to be all inclusive) of compromising incidents that are considered cryptographic incidents:

- 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); and
  - premature use of key.

- the use of cryptographic systems, equipment, and/or software approved by Communications Security Establishment Canada (CSEC), with operational practices or maintenance practices which are not approved by CSEC. For example:
  - the maintenance of cryptographic equipment by unauthorized or unqualified individuals;
  - 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 via non-secure communications of the details of a cryptographic equipment failure or malfunction;

- activation of the anti-tamper mechanism or unexplained zeroization of a Key Processor (KP); and

- any unauthorized use of key or CSEC-approved cryptographic equipment.
This page intentionally left blank.
Annex C – Compromising Incidents (Personnel) - Examples

The following list provides examples (not meant to be all inclusive) of compromising incidents that are considered personnel incidents:

- known or suspected defection or treason;
- known or suspected espionage or sabotage;
- known or suspected subversion;
- theft of Accountable COMSEC Material (ACM);
- deliberate falsification of Communications Security (COMSEC) records or reports;
- known or deliberate failing to report a confirmed or suspected COMSEC incident (Practice Dangerous to Security [PDS] or Compromising);
- unauthorized disclosure, or an attempt at disclosure, of information concerning ACM; and
- accidentally or knowingly processing, storing or transmitting classified or PROTECTED C information on an inappropriate cryptographic equipment or system.
This page intentionally left blank.
Annex D – Compromising Incidents (Physical) Examples

The following list provides examples (not meant to be all inclusive) of compromising incidents that are considered physical incidents:

- loss of Accountable COMSEC Material (ACM);
- unauthorized access to 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;
- failure to maintain required Two Person Integrity (TPI) or No-Lone Zone (NLZ) controls for TOP SECRET key;
- ACM improperly packaged or shipped;
- receipt of classified equipment, Controlled Cryptographic Item (CCI) or key marked ‘CRYPTO’ with a damaged inner wrapper;
- destruction of ACM 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 with or penetration of ACM including, but not limited to, ACM received in protective packaging which shows evidence of tampering and unauthorized premature opening; and
- unauthorized copying, reproducing or photographing of ACM.
This page intentionally left blank.
Annex E – COMSEC Incident Initial Report - Template

Reported by: ______________________________      Job/Title: ______________________________
Date: ____________     Time: _______________
Location: ___________________________________________________
Contact information: ________________________________________________

Personnel involved:

<table>
<thead>
<tr>
<th>Name (print)</th>
<th>Position</th>
<th>Citizenship</th>
<th>Clearance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Category: □ Cryptographic □ Personnel □ Physical

Possibility of compromise: □ Certain □ Possible □ Impossible (refer to Article 6.3.2)

Rational: ___________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________

Reporting department: ____________________________________________
COMSEC Account number: ______________________

Violating department: _____________________________________________
COMSEC Account number: ______________________
Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material (ITSD-05)

Identification of Accountable COMSEC Material (ACM) involved (complete as applicable):

Key

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Classification</th>
<th>Short Title</th>
<th>Universal</th>
<th>Edition(s)</th>
<th>Expiry Date</th>
<th>Register/KMID Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Equipment

<table>
<thead>
<tr>
<th>Short Title</th>
<th>Serial Number</th>
<th>Classification</th>
<th>Long Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Other

<table>
<thead>
<tr>
<th>Short Title</th>
<th>Registration and/or Serial Number</th>
<th>Classification</th>
<th>Long Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material (ITSD-05)

Circumstances surrounding discovery of COMSEC incident (What happened):

__________________________________________________________________
__________________________________________________________________
__________________________________________________________________
__________________________________________________________________
__________________________________________________________________
__________________________________________________________________
__________________________________________________________________

Initial recovery action taken (e.g. Key supersession):

__________________________________________________________________
__________________________________________________________________
__________________________________________________________________
__________________________________________________________________
__________________________________________________________________

ATTENTION: A COMSEC Incident Evaluation Report may be requested by the National COMSEC Incident Office (NCIO). Refer to Article 6.3.3.

NOTE 1: Use attachment if amplifying information available.

NOTE 2: Classification of this Annex, when completed, must be as detailed in Article 7.1.
Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material (ITSD-05)

This page intentionally left blank.
Annex F – Compromising Incident Action Flow Chart

- Incident Detected
  - Recovery Actions
    - Refer to ITSD-04 and ITSD-03
  - Initial Investigation
    - Refer to Article 6.2
      Complete within 24 hours
  - COMSEC Incident Initial Report
    - Refer to Article 6.3.2
      Submit to National COMSEC Incidents Office (NCIO)
      within 24 hours
  - Amplifying Report
    - Refer to Article 6.3.4
      New information to be provided
  - COMSEC Incident Evaluation Report
    - Refer to Article 6.3.3
      As requested by NCIO
  - Final Assessment and Closure Report
    - Refer to Article 6.3.5
      Completed by NCIO
      Provided to the Departmental COMSEC Authority (DCA)
  - Provide report to DCA
    - Take corrective action as detailed in report

NOTE: Ensure all reports are classified as detailed in Article 7.1
Directive for Reporting and Evaluating COMSEC Incidents
Involving Accountable COMSEC Material (ITSD-05)

This page intentionally left blank.