National Defence / Défense nationale

Chief Review Services / Chef - Service d'examen

CRS / CS Ex

Audit of Security Incident Management

June 2010

7050-33-2 (CRS)



Canada

Table of Contents

Acronyms and Abbreviations

BOI	Board of Inquiry
CF	Canadian Forces
CFCSU	Canadian Forces Crypto Support Unit
CFNOC	Canadian Forces Network Operations Centre
COMSEC	Communications Security
CRS	Chief Review Services
CSEC	Communications Security Establishment Canada
CSIS	Canadian Security Intelligence Service
Dir IM Secur	Director Information Management Security
DND	Department of National Defence
DPM Secur	Deputy Provost Marshal (Security)
DSO	Departmental Security Officer
FCA	Formation COMSEC Authority
GSP	Government Security Policy
IHA	Incident Handling Authority
INFOSEC	Information Security
ISSI	Information Systems Security Incident
ISSO	Information Systems Security Officer
IT	Information technology
MP	Military Police
NDSP	National Defence Security Policy
OPI	Office of Primary Interest
PGS	Policy on Government Security
QR&O	Queen's Regulations and Orders
SAMPIS	Security and Military Police Information System
SI	Summary Investigation
SSAC	Senior Security Advisory Committee
VCDS	Vice Chief of the Defence Staff

Results in Brief

Overall Assessment

[redacted]

Security incident management involves all the activities and processes in place to ensure that security incidents are detected, reported, investigated and acted upon in an appropriate manner so as to minimize damage and prevent recurrence. These activities and processes occur in response to individual security incidents or periodically at a strategic level, to protect critical assets, information and services related to the Department of National Defence/Canadian Forces (DND/CF) and Government of Canada operations.

The Policy on Government Security (PGS) (July 2009) states that when significant issues arise regarding policy compliance, allegations of misconduct, suspected criminal activity, security incidents, or workplace violence, Departments are responsible for ensuring:

- Incidents are investigated, acted on and reported to the appropriate law enforcement authority, national security agency or lead security agency; and
- Appropriate remedial action is taken.

The PGS also requires that a DSO be appointed to manage the departmental security program on behalf of the Deputy Heads. At the time of the audit, the Deputy Provost Marshal (Security) (DPM Secur) was the DND/CF DSO and therefore responsible for security incident management.

Key Finding and Recommendations

Security Incident Management. [redacted]

It is recommended that:

- [redacted]
- [redacted]

- [redacted]

Note: For a more detailed list of Chief Review Services (CRS) recommendations and management response, please refer to Annex A—Management Action Plan.

Introduction

Background

The Government Security Policy (GSP) (2002) stated that "Departments must develop procedures for reporting and investigating security incidents and taking corrective action. Through effective reporting and investigation of security incidents, vulnerabilities can be determined and the risk of future occurrence reduced."[1] The GSP further defines a security incident as a "compromise of an asset, or any act or omission that could result in a compromise, threat or act of violence toward employees."[2]

The PGS, released in July 2009 to replace the GSP, re-emphasized the requirement to effectively manage security incidents by stating that "at a government-wide level, security threats, risks and incidents must be proactively managed to help protect the government's critical assets, information and services, as well as national security."[3] It went further to identify "management of security incidents is effectively coordinated within departments and government-wide"[4] as one of the expected policy results. To this end, departments are responsible for ensuring that when significant issues arise regarding policy compliance, allegations of misconduct, suspected criminal activity, security incidents, or workplace violence:

- They are investigated, acted on and reported to the appropriate law enforcement authority, national security agency or lead security agency; and
- Appropriate remedial action is taken.

The policy also requires that a DSO be appointed to manage the departmental security program on behalf of the Deputy Heads. At the time of the audit, DPM Secur was the DND/CF DSO and therefore responsible for security incident management.

Security Incident Management

Security incident management involves all the activities and processes in place to ensure that security incidents are detected, reported, investigated and acted upon in an appropriate manner so as to minimize damage and prevent recurrence. These activities may occur at the individual security incident level, as well as from a program or departmental perspective.

[1] GSP, 10.15 Investigation of Security Incidents, 2002.
[2] GSP, Appendix B—Glossary, 2002.
[3] PGS, 2009, Section 3.4.
[4] PGS, 2009, Section 5.2.

For each security incident these activities may include:

- Coordinating and reviewing damage assessments and associated decisions regarding remedial actions;
- Overseeing security investigations and actions taken to address the identified weaknesses; and
- Reporting security incidents to DND/CF and external stakeholders where necessary.

From a departmental perspective, activities may include:

- Conducting trend analyses to identify repeat offenders, vulnerabilities, possible policy change requirements, and opportunities to target training and awareness programs; and
- Reporting security information to senior management to increase security awareness and ownership of security controls across the Department.

At the time of the audit, there were three distinct technical streams under which a security incident could be grouped:

1. **Communications Security (COMSEC) Incidents**—security incidents involving COMSEC material.[5] Director Information Management Security (Dir IM Secur) is the departmental COMSEC Authority with a member of Dir IM Secur 5 serving as the Deputy COMSEC Authority and, as such, the primary incident handling authority (IHA) for COMSEC security incidents.

    - Other key stakeholders in the COMSEC security incident category include Canadian Forces Crypto Support Unit (CFCSU), Formation COMSEC Authorities (FCA), and COMSEC custodians.

2. **Information System Security Incidents (ISSI)**—security incidents involving information systems and associated components. Dir IM Secur is the Information Technology Security Coordinator for DND/CF and Dir IM Secur 4[6] is the primary IHA for ISSI.

    - Other key stakeholders in the ISSI security incident category include the Canadian Forces Network Operations Centre (CFNOC), Information Technology (IT) help desks, and Information System Security Officers (ISSO).

[5] Includes cryptomaterial, ancillary devices, COMSEC publications, and other non-crypto material such as selected call signs, authentication systems, training and maintenance key tapes.
[6] Note that during the course of the audit, Dir IM Secur 4 merged with Dir IM Secur 3.

3. **All Other Security Incidents**—at the time of the audit, DPM Secur was not only the DSO, but also responsible for other elements of the security program, including physical security, personnel security, and information security. As such, members of DPM Secur staff serve as the primary IHA for security incidents related to these areas.

    - Other key stakeholders in this security incident category include Environment/Command Provost Marshals, local Military Police (MP) Security Offices, and Unit Security Supervisors.

In addition to the technical chain, the success of the security incident management process is highly dependent on the ability of all DND employees and CF members to recognize a potential security incident and report it to the appropriate authorities. Also, Commanding Officers, establishment heads, or persons in charge must ensure that each security incident is investigated "…to determine the nature, cause, extent and seriousness of the situation, to identify those responsible for the incident and to suggest any corrective action necessary to prevent a recurrence."[7]

Objective

The objective of this audit was to determine whether all identified security incidents were reported to the DSO and required external organizations, whether the security incidents were investigated, and whether measures were taken to minimize damage and/or prevent recurrence.

The audit criteria are detailed in Annex B.

Scope

- The scope of the audit included assessing the processes used by National Defence Headquarters organizations (primarily DPM Secur and Dir IM Secur) to manage security incidents from the time a security incident is reported through to conclusion.
    - It did not include an assessment of processes used at formation headquarters, bases/wings, or units. Therefore, observations noted in this report are limited to the information contained in the IHA security incident files.
    - It did not assess the quality or adequacy of investigations or damage assessments but rather focussed on whether IHAs had evidence that investigations and damage assessments had been performed and if IHAs made this type of assessment.

- The audit sample was selected from security incidents reported to and tracked by DPM Secur, Dir IM Secur, and CFNOC[8] in 2006 and 2007. Additional sample

[7] National Defence Security Policy (NDSP), Chapter 18: Breaches & Violations—Investigations & Reporting, 2007, 18.10.
[8] Although not identified as a primary IHA, security incidents tracked by CFNOC were included as a separate sample selection source due to risks identified in the planning phase associated with communication between CFNOC and Dir IM Secur 4 staffs.

items were selected from 2008 and early 2009 where these organizations indicated that the processes had changed from previous years.

Methodology

- Reviewed Government of Canada and DND/CF policies, guidelines and directives associated with security incidents (detailed list in Annex C).
- Interviewed staff from the DPM Secur, Dir IM Secur and CFNOC organizations.
- Analyzed security incident data contained in six different "systems" (i.e., database, spreadsheet, list) created by DPM Secur, Dir IM Secur and CFNOC.
- Reviewed a judgmental sample of 69 security incident files.
  - The sample was selected using factors, where available, such as status, year, classification, incident type, location, likelihood of compromise, etc.
  - [redacted]

Reviewed by CRS in accordance with the *Access to Information Act* (AIA). Information UNCLASSIFIED.

Finding and Recommendations

Reporting Security Incidents to the DSO

The primary DND/CF policy on security incidents[9] clearly states that all security incidents should be reported to DPM Secur (formerly D Secur)—the current DSO. It also recognizes that not reporting security incidents or unnecessary reporting delays may result in the continued or increased exposure of assets to compromise.

The ability to ensure that the DSO is notified of all security incidents is hindered by:

- The manner in which security incidents are tracked; and
- The degree, to which reporting processes are established, documented, communicated and followed.

[9] NDSP, Chapter 18: Breaches & Violations—Investigations & Reporting, 2007.

- [redacted]

[redacted]

- [redacted]

- [redacted]

- [redacted]

[redacted]

The initial reporting step provides the DSO with an early opportunity to ensure that appropriate response and mitigation actions are taken to minimize damage and prevent recurrence of significant security incidents, and subsequently, facilitate the conduct of departmental trend analyses.

[redacted]

Damage Assessments

DND/CF policies pertaining to security incidents[10] and damage assessments[11] clearly require that a damage assessment be completed upon being advised of a compromise or probable compromise of classified/designated information or assets. "Damage assessments address the consequences of an actual or suspected compromise of matter and must provide a sound and timely analysis on which to recommend appropriate remedial action in order to minimize the damage caused as a result of the breach of security."[12] Damage assessments, including a statement or an analysis of the injury to the

[10] NDSP, Chapter 18: Breaches & Violations—Investigations & Reporting, 2007.
[11] NDSP, Chapter 19: Damage Assessments, 2004.
[12] NDSP, Chapter 19: Damage Assessments, 2004, 19.07.

national or other interest that has resulted, are to be completed and forwarded through the appropriate unit and command headquarters to DPM Secur —the departmental authority for damage assessments—within 10 days.

According to policy, "a damage assessment is to be completed by the person(s) who originated, or is responsible for the matter concerned, or a person in authority who has a detailed knowledge of the subject"[13]

Once a damage assessment is completed, DND/CF policy indicates that Commanding Officers and/or establishment heads are responsible for implementing the associated remedial actions. Policy also states that "in order to deal effectively with such matters there must be a coordination of effort between all parties concerned and agreement on the necessary follow-up action when there is multiple or collateral interest and involvement."[14]

[13] NDSP, Chapter 19: Damage Assessments, 2004, 19.05.
[14] NDSP, Chapter 19: Damage Assessments, 2004, 19.04.

Security Investigations

The DND/CF policy on security incidents states that:

"All violations of security orders shall be investigated and reported upon whether they result in compromise of classified/designated information or not."[15] "…security investigations shall be pursued to the extent necessary to determine the nature, cause, extent and seriousness of the situation, to identify those responsible for the incident and to suggest any corrective action necessary to prevent a recurrence."[16]

Formal security investigations are required where there is a compromise, or possible compromise of classified information and/or assets. There are two types of formal investigations: a board of inquiry (BOI) or a summary investigation (SI), which is less formal.

[15] NDSP, Chapter 18: Breaches & Violations—Investigations & Reporting, 2007, 18.07.
[16] NDSP, Chapter 18: Breaches & Violations—Investigations & Reporting, 2007, 18.10.

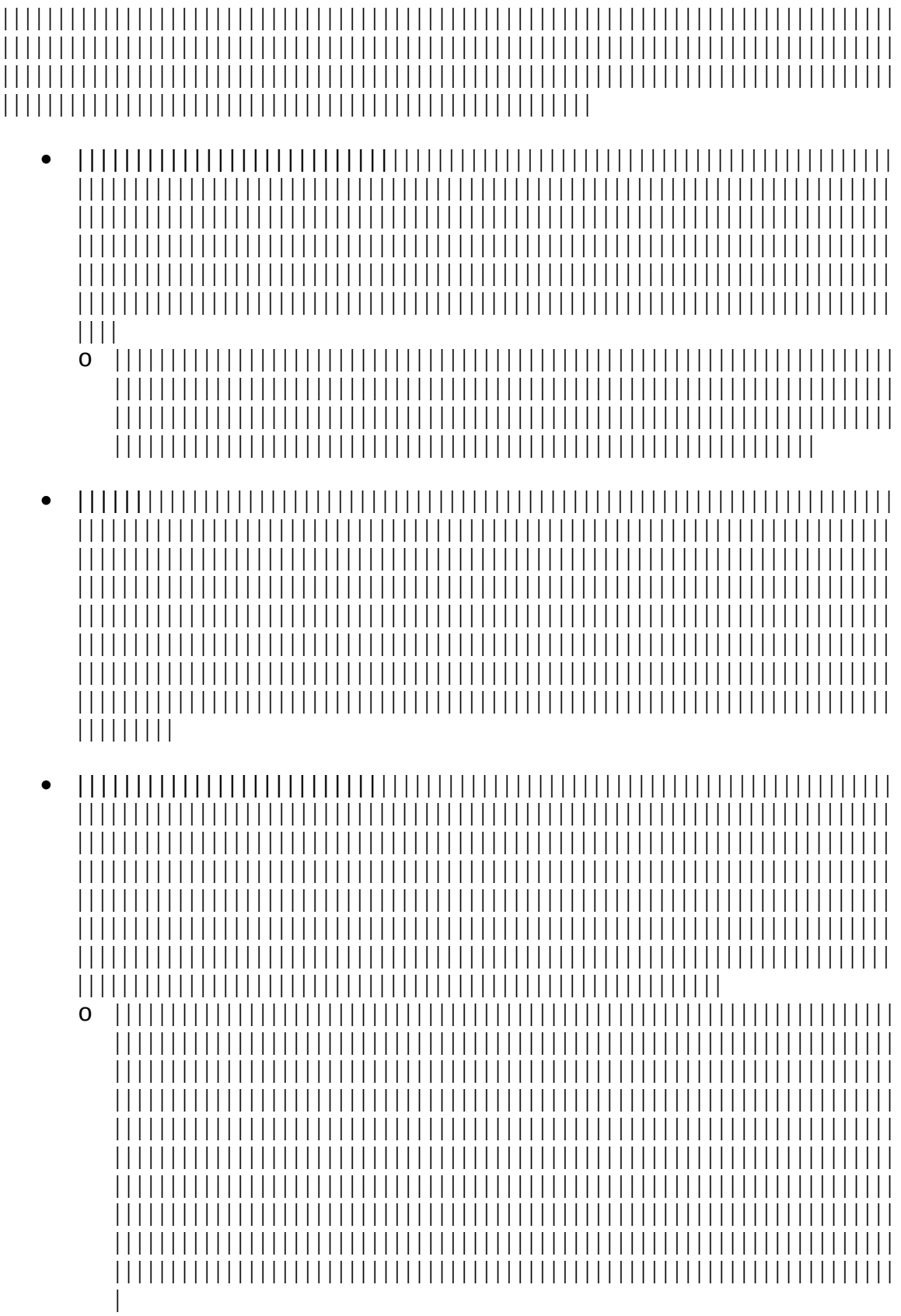
According to the NDSP 18, DPM Secur has the authority when requested by the Commanding Officer or establishment head, to grant a waiver in cases where a less formal investigation is considered as productive or the circumstances do not warrant a formal investigation. [redacted]

[redacted][17]

- [redacted]
  - [redacted]
  - [redacted]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

[17] [redacted]



Reporting Security Incidents to External Organizations

The GSP and associated standards identify specific circumstances under which security incidents must be reported to organizations outside the Department. For example, incidents suspected of constituting criminal offences must be reported to the appropriate law enforcement authority, and incidents involving threats to the national interests must be reported to the Canadian Security Intelligence Service (CSIS).

[redacted]

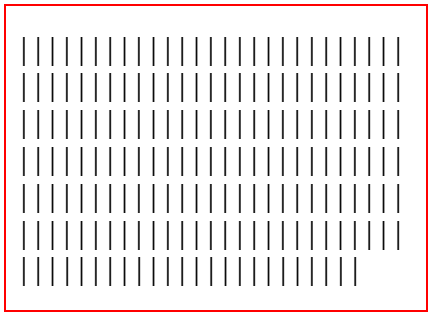
- [redacted]
- [redacted]
- [redacted]

[18]

[18] [redacted]

-
-
-

Conclusion—Prevent Recurrence



Recommendations

It is recommended that:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

OPI: VCDS/DSO

Annex A—Management Action Plan

Security Incident Management

CRS Recommendation

1. [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] [illegible]

Annex A

CRS Recommendation

2. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

CRS Recommendation

3. [redacted]

[redacted]

[redacted]

[redacted] [redacted]

Annex A

CRS Recommendation

4. [redacted]

[redacted]

[redacted]

[redacted]

CRS Recommendation

5. [redacted]

[redacted]

[redacted]

[redacted]

Annex B—Audit Criteria

Objective

1. To assess whether security incidents are reported to the DSO and required external organizations, whether the incidents are investigated, and whether measures are taken to minimize damage and/or prevent recurrence.

Criteria

- The DSO is informed of all security incidents reported to the IHA;
- Damage assessments are conducted and there is a commitment by management to take remedial action;
- Security investigations are conducted and coordinated in order to obtain all necessary information in a timely manner, and there is a commitment by management to take appropriate action;
- IHA undertake activities (i.e., trend analyses) to minimize the risk of recurrence; and
- Security incidents are reported to external organizations when required according to the GSP and DND/CF policies.

Annex C—Key Security Incident Policies

Government of Canada Security Policies

Government Security Policy, Treasury Board of Canada Secretariat, 2002

Operational Standard: Security Organization and Administration, Treasury Board of Canada Secretariat, 1995

Operational Standard for the *Security of Information Act*, Treasury Board of Canada Secretariat, 2003

Operational Security Standard: Management of Information Technology Security, 2004

IT Security Directives: Directives for the Application of Communications Security in the Government of Canada (ITSD-01), Communications Security Establishment of Canada, 2005

IT Security Guidance: COMSEC Material Control Manual (ITSG-10), Communications Security Establishment of Canada, 2006

New (July 2009) Government of Canada Security Policies

Policy on Government Security, Treasury Board of Canada Secretariat, 2009

Directive on Departmental Security Management, Treasury Board of Canada Secretariat, 2009

DND/CF Security Policies

National Defence Security Policy, Chapter 18: Breaches & Violation—Investigations & Reporting, 2007

National Defence Security Policy, Chapter 19: Damage Assessment, 2004

National Defence Security Policy, Chapter 20: Disciplinary & Administrative Responses to Breaches, 2004

Queen's Regulations & Orders, Chapter 21: Summary Investigations and Boards of Inquiry, 1999

Defence Administrative Orders and Directives 7002 Series: Boards of Inquiry and Summary Investigations, 2002

COMSEC Material Control Instructions (Infosec 2B), 2007

DND Information System Security Incident (ISSI) Reporting and Handling, CANFORGEN 138/02 ADM IM 007/02, 2002