Department of Indian Affairs and Northern Development
Departmental Audit and Evaluation Branch

Prepared by:

Hasan Zaidi, Audit Manager
Hélène Thériault, Project Manager

Departmental Audit and Evaluation Branch

Assisted by:
Performance Management Network

Audit of Security

Project 96/06
June 1997

Table of Contents

Page

Executive Summary

Purpose

The purpose of this audit is to provide a comprehensive assessment of the management and administration of the departmental security function; and compliance with the Government Security Policy (GSP) and the Information Technology Security (IT) operational standards.

Background

The department must conduct internal audits of compliance with, and effectiveness and efficiency of the implementation of the Government Security Policy (GSP) every five years. The previous audit in 1992-1993 identified that a number of improvements were required to strengthen management and delivery practices and to comply to the requirement of the GSP.

Overall Assessment

The departmental security function has improved in comparison to conditions observed during the 1992 audit. The implementation of Threat and Risk Assessments, security awareness programs and other initiatives have strengthened the function. However, in most locations visited, the concern for security is still low, resulting in assets, particularly sensitive information, not being safeguarded adequately.

The need to further strengthening the security function to be within an acceptable level of risk will require changes to security procedures, but mostly in people's attitudes.

Key observations

The department needs to upgrade the efficiency of its annual Departmental Threat and Risk Assessment process through the use of an annual report on the security environment. Threats in today's environment are ever increasing. In one region visited, occupations/sit-ins/demonstrations were considered the most serious threat. The department does not have an efficient methodology to monitor its key threats, and adjust its key countermeasures if required, to ensure "acceptable" levels of risk are maintained.

The framework for the management of the security function is well established in two locations. However, a high level of security violations and breaches of sensitive and classified information persist in the department. "Low security concern" from employees is the root cause. As such, it is the department's key threat. Notwithstanding the efforts by the Security people and the many positive features of the existing management framework, security is still not sufficiently "valued" by employees.

Improvements can be cost-effectively established, departmentally and in the regions, to ensure the management framework is effective against all threats. A policy of sanctions and strengthening regional practices regarding annual security planning, allocation of sufficient resources, appropriately trained staff and a program of regular sweeps that are reported to the Regional Director General are key recommendations.

Compliance with the GSP has been strengthened since the 1992 audit and is now satisfactory in most respects. Liaison with external security agencies and e-mail security are areas which should be given attention in the future.

Section 1 - Introduction

Background

In June 1994, Treasury Board revised the Government Security Policy (GSP). The revision took into account the current environment of security, particularly in the Information Technology (IT) area.

The Departmental Audit and Evaluation Branch (DAEB) must conduct internal audits of compliance with, and effectiveness and efficiency of the implementation of, the GSP. These audits are required at least every five years and the DAEB carried out the previous audit in 1992-1993. This audit was conducted during the period September 1996 to March 1997.

Objectives

The objectives of the audit were to review, assess and report on:

- the security management framework, that is the policies, practices and controls in place relating to security administration; and,

- compliance with, the GSP, the ITS operational standards and all departmental security policies and procedures.

Scope

The scope of the audit includes all management policies, practices, systems and controls related to the management of the security program. In addition, the scope included compliance with the GSP covering all key areas of the security program, namely:

- Information Security;
- Physical Security;
- Personnel Security;
- IT Security; and,
- Contingency Planning.

Personal safety and security of staff were included in the scope. Liaison with security agencies outside of the department (e.g. RCMP) was also included in the scope of this project but there were no visits to external agencies.

Section 2 - Observations and Recommendations

Security Environment

The departmental methodology, to monitor its key threats and adjust key countermeasures if required, needs to be strengthened to ensure "acceptable" levels of risk are maintained.

Threats in today's environment are ever-increasing. This is driven by many factors including downsizing of public and private sector organizations coupled with persistent high unemployment and technological advancement. This makes eavesdropping equipment easily accessible to the public in retail "spy" stores found in every major city.

Two years ago the department completed detailed Threat and Risk Assessments (TRAs) in all the regions and headquarters' groups. The process took over a year to complete and the results were summarized and reported to senior management in December 1994.

The departmental TRA identified threats associated with the "human element" (i.e., non-compliance with prescribed security procedures, lack of employee awareness, etc.) as the key threats to the department. We refer to this threat as "low security concern" and it was found to still be a key threat based upon our field visits and testing.

There are other threats that are now becoming more serious for the department. For example, in one region visited, **occupations/sit-ins/demonstrations** were considered a more serious threat than low security concern. Countermeasures, including reduction of reception areas and card access controls, were being adjusted to offset the increased seriousness of the threat. These countermeasures were not completed at the time of this audit such that the region was not yet within an "acceptable" level of risk.

This same region also identified employee dissatisfaction as a key threat, but a slightly less serious one than occupations/sit-ins/demonstrations. In another region, theft was considered a key threat along with its most serious threat of low security concern.

Low security concern remains the main key threat across most departmental locations. However, as other threats become as/more serious, the department is at risk by not having a more efficient method to assess and summarize key threats. The present TRA process is lengthy and complex without providing the flexibility that would allow the department to adjust their key countermeasures.

Exhibit 1, on next page, has been prepared as a sample one-page Security Environment Annual Report regions and headquarters' groups could use to efficiently assess and report on their key threats, key countermeasures, etc.

Exhibit 1

PROTECTED (when completed)

SECURITY ENVIRONMENT ANNUAL REPORT

Branch/Region: _____

Key Protection Needs	Key Threats
☐ Personnel ☐ Sensitive Information ☐ Classified Information ☐ Assets ☐ Cash, negotiables ☐ Equipment ☐ Blank Status Cards ☐ Other _____ (specify)	☐ Occupations/SIHs ☐ Public Access ☐ Low Security Concern ☐ Employee Dissatisfaction ☐ Bomb Threats ☐ Natural Disasters (flood, fire, etc.) ☐ Electronic Eavesdropping ☐ Other _____ (specify)

Key Countermeasures	
☐ TRA Updated Annually	☐ Contingency Plans
☐ Guarding	☐ Business Resumption Plans
☐ Card Access System	☐ Security Sweeps
☐ Key Registry/Combinations	☐ IT Security Sweeps
☐ Cabinets/Containers	☐ All Violations reported to ADM/RDG/HQ
☐ Screening/Clearances Required	☐ Liaison with external Law Enforcement Agencies
☐ Training	☐ Other _____ (specify)
☐ Back-Ups Appointed	

Compliance to Prescribed Security Procedures

☐ Completely Satisfactory ☐ Satisfactory in Most Respects ☐ Unsatisfactory

Overall Risk Assessment

☐ Minimal Risk ☐ Acceptable Risk ☐ Unacceptable Risk

Action Plans

Actions Plans (where required):

_____

_____

_____

_____ _____

ADM/RDG (name & initial) Date DSO/RSO (name & initial) Date

The Security Environment Annual Report would be prepared annually by the Regional Security Officer (RSO) or Departmental Security Officer (DSO) for headquarters' groups. It would then be reviewed and signed by a Regional Director General (RDG) or Assistant Deputy Minister (ADM).

The Security Environment Annual Report would ensure senior management is well-informed about changes in threats and allow timely action to be taken to ensure acceptable levels of risk are being maintained.

Recommendation 1: The Assistant Deputy Minister, Corporate Services should ensure the department upgrades the efficiency of the Departmental Threat and Risk Assessment process through the use of an annual report on the security environment.

Management Framework

The framework for the management of the security function is well established in two locations. However, the efforts by the Security people and the many positive features of the existing management framework have not been effective against the "low security concern" threat, which is contributing to a persistently high level of security violations and breaches of sensitive and classified information.

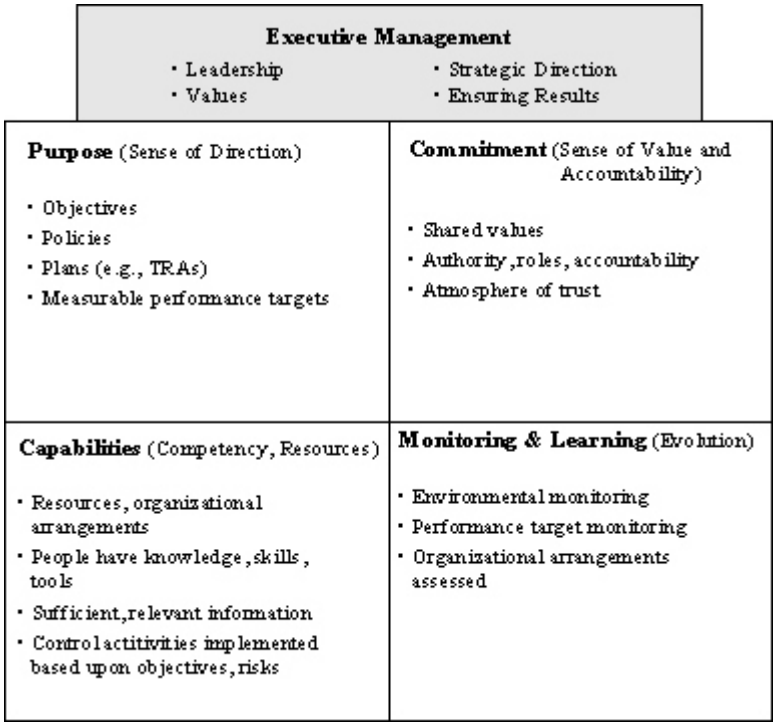
Improvements can be cost-effectively established, departmentally and in the regions, to strengthen the "value" placed on security.

We examined the department's overall management practices based upon the Management Control Framework illustrated on the following page in **Exhibit 2**.

The framework for the management of the security function departmentally includes: a comprehensive TRA process to support security planning; clear roles, responsibilities and lines of reporting for the DSO, RSOs, managers and employees, etc.; and a Departmental Security Manual which includes a Classification and Designation Guide. In addition, security staff were generally well-trained, albeit the need for training of security staff was identified in some regions visited.

The many positive features of the existing management framework have not been able to adequately address the threat of "low security concern". This threat has been identified as a key threat at headquarters and in the three regions visited. It is the direct cause of the persistently high level of security violations and breaches of sensitive and classified information. This high level of security violations was confirmed during silent hour sweeps.

Exhibit 2: Management Control Framework



At best, violations were found in 50% of work units visited — in one region it was 100% of work units swept.

In some regions, recommendations to strengthen management framework practices were made specifically to address the low security concern threat. Using the TRA methodology in annual security planning, allocating sufficient resources, establishing a program of security sweeps, reporting the results to the RDG and establishing sanctions for security violations were the major recommendations. These management framework features should be in place across the department.

Sound protection practices need to be developed as a "value" of the organization. Demonstrated senior management action is the key to illustrating the organization values security. Funding for physical access controls, support of ongoing security awareness programs and the TRAs all signal that security is valued. A policy to provide sanctions where expected practices are not taken seriously is the next concrete action senior management can take to enhance the value of security within the department. The issue of sanctions is particularly important. We also observed some documents were over-classified SECRET in the interest of ensuring their protection. Protection of a document is not assured by its marking, even a SECRET marking.

The sanctions policy, and other recommendations highlighted above can be cost-effectively implemented to strengthen the management framework. Without these changes, future violations and breaches will likely create "unacceptable" risks to the achievement of departmental objectives.

Recommendations 2: The Assistant Deputy Minister, Corporate Services should ensure:

a) a departmental policy of sanctions that may be imposed in the event of a security violation or breach is developed and communicated to all staff, and enforced;

b) the Departmental Security Officer assesses effectiveness of the sanctions policy one year after implementation; and

c) the results of the regional and headquarters' security activities and incidents are summarized annually and reported to senior management.

Recommendation 3: The Assistant Deputy Minister, Corporate Services, in consultation with Regional Director Generals should ensure the management framework for security include use of the TRA methodology in their annual security planning, allocation of sufficient resources, appropriately trained security personnel and a program of regular sweeps that are reported to the Regional Director General.

Security Program

Compliance with the GSP has been strengthened since the 1992 audit and is satisfactory in most respects. The main areas that remain of particular concern are Information Security and Contingency Planning.

Threat and Risk Assessments, Business Resumption Plans, Personnel Security, Informatics Security and Information security were all identified as requiring strengthening by the 1992 audit.

A TRA process has been developed and implemented and a project to establish Business Resumption Plans is underway at headquarters and in the regions. The Security and Emergency Measures Section at headquarters also issued guidance on contingency plans covering fire, demonstrations, bomb threats, medical emergencies and other threats in July 1997. However, in two of the three regions visited, regular liaison had not been established with external security agencies. This is an important feature of contingency planning for all regions.

The Security Services Information System (SSIS) has been implemented since the previous audit. It enables efficient processing and tracking clearances requiring updating. We also observed effective IT Security procedures in two of the three regions visited. No one had been assigned IT Security responsibility in the other region visited. (IT Security was not within the scope of our audit of headquarters security practices.)

Information Security practices observed included adequate cabinets, containers and registry arrangements in all locations visited. However, staff were consistently showing a low security concern in not ensuring sensitive and classified information was secure in silent hours. Several recommendations to address the persistent Information Security violations were made in the previous observation on management practices.

E-mail is an area of concern for Information Security. The department was pilot testing a software program to enable the e-mailing of classified and sensitive information at the time of this audit. With or without the software in place, e-mailing is becoming the transmission mode of choice and there is a need to place emphasis on e-mailing protocols in security awareness training.

The distribution of the Department's Security Manual which includes the Classification and Designation Guide is limited to a few select managers at headquarters and in the regions. The extent of this distribution may be a contributing factor to the information security deficiencies. At the time of this audit, the Security and Emergency Measures Section was considering electronic dissemination of the Security Manual to improve employee access to prescribed requirements such as those for information security.

Recommendations 4: The Departmental Security Officer should ensure:

a) security policies and procedures, including the Classification and Designation Guide, are made more accessible to employees through electronic communications; and,

b) security awareness training about the use of e-mail is given particular attention.

APPENDIX I

AREAS OF AUDIT ACTIVITY

GOVERNMENT SECURITY POLICY

Main components to assess:

- organizational structure;
- administrative procedures; and
- all sub-systems; for example:
  - Physical Security;
  - Information Technology Security;
  - Personnel/Information/Assets Security; and
  - Communications Security.

INFORMATION TECHNOLOGY SECURITY

Main components to assess:

- organizing and administering;
- personnel security;
- physical security;
- hardware security;
- software security;
- communications security; and
- operations security.

SECURITY MANAGEMENT & ADMINISTRATION FRAMEWORK

Terms of Reference

TERMS OF REFERENCE

AUDIT OF SECURITY

BACKGROUND:

In June 1994, Treasury Board revised the Government Security Policy (GSP). The revision takes account of the current environment of security, particularly in the Information Technology (IT) area.

DEPARTMENTAL SECURITY ORGANIZATION

- the Departmental Security Officer (DSO), who is appointed by the Deputy Minister, is responsible for the administration of the departmental security program consistent with the Security policy and standards;

- each Regional Security Officer (RSO) is responsible for the overall effectiveness of the security program and compliance with the GSP, the ITS standards and all the departmental policies and directives, for his/her respective region; and

- each Regional Informatics Manager (RIM) is responsible for the technical aspect pertaining to security of informatics and telecommunications within his/her region.

NEED:

The Departmental Audit and Evaluation Branch (DAEB) must conduct internal audits of compliance with, and effectiveness and efficiency of the implementation of, the GSP. These audits are required at least every five years. The Treasury Board also monitors compliance with GSP.

SCOPE:

The scope of the audit includes all management policies, practices, systems and controls related to compliance with the GSP and to the organization, management and administration of security including physical and personnel security. The areas of audit activity are listed in Appendix I.

The audit will be conducted at corporate headquarters and at British Columbia, Manitoba and the Quebec Regions.

SCOPE EXCLUSION:

The proposed audit will exclude Informatics Security at Corporate headquarters. It has been covered in the audit of Informatics and EDP Consolidation in 1995-1996 (Project 94/10).

OBJECTIVES: The objectives of this audit are to review, assess and report on:

- compliance with, the GSP, the ITS operational standards and all departmental security policies and procedures; and
- the Security management framework, that is, the policies practices and controls in place relating to security administration.

APPROACH: The audit will be conducted in the following three phases:

- Preliminary Survey and Evaluation;
- Fieldwork and Analysis; and
- Reporting.

RESOURCES: The project will be implemented using contracted resources and will be managed by DAEB.

COST: It is estimated that the contracted resources will cost between $55,000 and $66,000.

TIMEFRAME: The audit planning will commence in August 1996 and the report will be completed by March 1997.

APPROVED BY:

B. DiBartolo
Assistant Deputy Minister
Corporate Services
August 16, 1996

Action Plan

AUDIT AND EVALUATION / VÉRIFICATION INTERNE ET ÉVALUATION

REQUEST FOR ACTION PLAN / DEMANDE DE PLAN D'ACTION

PROJECT / PROJET : 96/06
DATE SENT / DATE D'ENVOI : 97-05-12
DATE DUE / ÉCHÉANCE : 97-05-23

PROJECT TITLE / TITRE DU PROJET : Audit of Security
REGION OR BRANCH / RÉGION OU DIRECTION GÉNÉRALE : Corporate Services

(1) RECOMMENDATIONS / RECOMMANDATIONS	(2) REPORT / RAPPORT PAGE NO.	(3) ACTION PLAN / PLAN D'ACTION	(4) RESPONSIBLE MANAGER / GESTIONNAIRE RESPONSABLE (TITLE / TITRE)	(5) PLANNED COMPLETION DATE / DATE PREVUE DE MISE EN OEUVRE
1. The Assistant Deputy Minister, Corporate Services should ensure the department upgrades the efficiency of the Departmental Threat and Risk Assessment process through the use of an annual report on the security environment.	4	The proposed Annual Report will be adopted as part of the departmental security procedures and the RDGs will be requested to update the TRAs for their respective regions. A call letter will then be forwarded to all RDGs annually to request an update of the regional TRAs. The NCR TRAs will be updated in the same fashion.	Chief, SEMD	November 1, 1997
2. The Assistant Deputy Minister, Corporate Services should ensure:	6			
a) a departmental policy of sanctions that may be imposed in the event of a security violation or breach is developed and communicated to all staff, and enforced;		a) Security policy/procedures related to sanctions currently in draft; revisions still required based on recent concerns. Further consultation with Staff Relations will be initiated and security chapter will be revised/issued accordingly.	Chief, SEMD	October 31, 1997
b) the Departmental Security Officer assesses effectiveness of the sanctions policy one year after implementation; and		b) The DSO will review the impact of sanctions in one year after implementation by consulting with Staff Relations and analyzing records of violations and breaches.	Chief, SEMD	October 31, 1998
c) the results of the regional and headquarters' security activities and incidents are summarized annually and reported to senior management..		c) An annual report to the DM (c.c. Executive Committee) will be prepared based on input from all regions and will outline major security concerns and achievements during the fiscal year.	Chief, SEMD	June 30, 1997

PROJECT TITLE / TITRE DU PROJET : Audit of Security
REGION OR BRANCH / RÉGION OU DIRECTION GÉNÉRALE : Corporate Services

(1) RECOMMENDATIONS / RECOMMANDATIONS	(2) REPORT / RAPPORT PAGE NO.	(3) ACTION PLAN / PLAN D'ACTION	(4) RESPONSIBLE MANAGER / GESTIONNAIRE RESPONSABLE (TITLE / TITRE)	(5) PLANNED COMPLETION DATE / DATE PREVUE DE MISE EN OEUVRE
3. The Assistant Deputy Minister, Corporate Services, in consultation with Regional Director Generals should ensure the management framework for security include use of the TRA methodology in their annual security planning, allocation of sufficient resources, appropriately trained security personnel and a program of regular sweeps that are reported to the Regional Director General.	6	The DSO will consult with the RDGs, Directors of Corporate Services and RSOs in an attempt to develop a departmental approach that could improve the management framework and participation/involvement in the regions. The DSO will also solicit their full support/participation in developing and implementing a departmental plan.	Chief, SEMD	January 31, 1998
4. The Departmental Security Officer should ensure:	7			
c) security policies and procedures, including the Classification and Designation Guide, are made more accessible to employees through electronic communications; and,		a) Intranet site to be used for this purpose, when available. SEMD will contact the Intranet Coordinator to determine departmental plan/time frame and requirements. If time frame acceptable, SEMD will pursue this initiative separately in consultation with the Departmental Intranet Coordinator.	Chief, SEMD	December 31, 1997
d) security awareness training about the use of e-mail is given particular attention.		b) Transmission of designated/classified information by e-mail has been addressed through the Network Security Strategy recently approved by IMC.	Chief, SEMD and IMB	2 year implementation (June 30, 1999)
		The regular use of e-mail and associated security concerns are currently being presented during the security briefings. Briefing material will formally be revised to address this issue.	Chief, SEMD	September 30,1997
		An article will also be included in the next Security Bulletin	Chief, SEMD	July 31, 1997