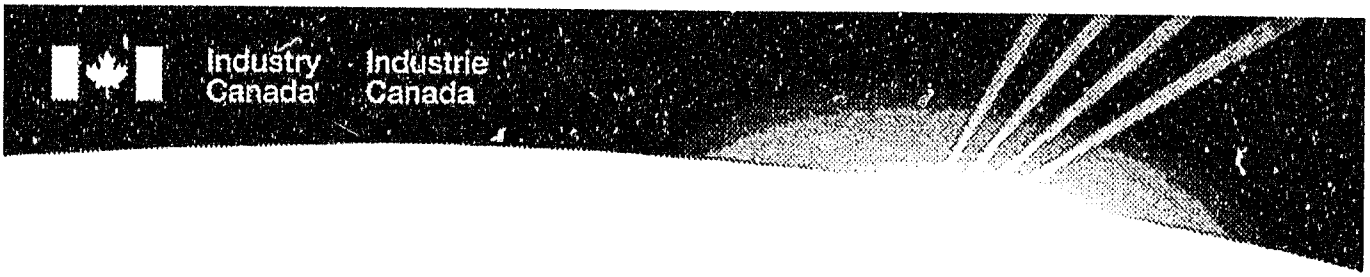

Audit of Security Function
Report on Preliminary Phase

Audit and Evaluation Branch

January 2000

Canada

TABLE OF CONTENTS

1.0 Audit Objectives

The purpose of the preliminary phase of this audit was to evaluate the efficiency of Industry Canada's security function and to identify key aspects of this function which should be subject to a further audit.

The objectives of the preliminary phase were to:

- Evaluate the management framework used by the Security Services Division (SSD), including the efficiency of the departmental security policy and its level of compliance with Treasury Board's security policy; and
- Evaluate the effectiveness and efficiency of security function delivery within the Department.

2.0 Audit Scope and Approach

The preliminary phase covered all the departmental sectors, including a summary assessment of security function in the Pacific/Yukon, Quebec and Atlantic Regions through telephone interviews. The following elements were audited:

- Security organization;
- Security administration;
- Physical security;
- Personnel security;
- Emergency security and management; and
- Contract security and management.

The information technology security component, which is now part of the Chief Information Office, was excluded from this audit due to its distinct nature. However, the functional relationships between the informatics security officer and the SSD was assessed.

A total of 15 interviews were conducted with managers and employees related to the security function. Treasury Board's Guide to the Audit of a Security Function (July 1996) was used as a reference tool during the interviews and the review of appropriate documentation.

3.0 Security Function Management Framework

3.1 Security Organization

All managers are responsible of ensuring security within the Department, whereas the Security Services Division is responsible for the management of the various security function elements.

The Security Services Division (SSD) reports to the Director, Compensation, Security and Management Services of the Human Resources Branch. The Director has seven full-time employees, as well as 27 employees under contract with the Corps of Commissionaires and one with Pinkerton

The Director of SSD acts as the Departmental Security Officer (DSO), whose mandate is to develop, implement, maintain, coordinate and control Industry Canada's security program. For security matters, departmental sectors report directly to the DSO with the exception of the Canadian Research Council (CRC), the Canadian Intellectual Property Office (CIPO) and Measurement Canada. In these cases the DSO assumes a functional reporting role.

The DSO is assisted by three managers: one for personnel security, one for physical security and contingency planning, and one for cost recovery management and security awareness. Since October 1999, the security function related to information technology falls under the responsibility of the Chief Information Office. According to the manager responsible for this function, the transfer has not led to any negative changes for the SSD, as he must keep the DSO informed of all important information concerning information security. The Human Resources Branch is about to revise the work description for the DSO as a result of this transfer.

The DSO plays a functional reporting role with regard to regions. In all regional offices, officers have been appointed for personnel security, as well as physical security and contingency planning. The latter are responsible for applying adequate security measures, but must share the time assigned to security with other administrative tasks.

During the preliminary phase of this audit, the SSD told auditors that the position of the agent responsible for the electronic integrated system of access control and the identification system is presently occupied by a contract employee. However this position is in process of being staffed. Staffing of this position will help to ensure the continuity of this service.

The audit team also discovered that most of the security function elements are covered by SSD positions. However, the following weaknesses were identified in the security organisation within the Department:

- The SSD provides services to external organizations, among which the most important ones are Citizenship and Immigration Canada (CIC) and the Office of the General Auditor. (This is explained, in part, by the Department's acquisition of the control centre located at the Jean Edmond building where these external organizations are located). However it is

difficult to understand the rationale for this situation, since a higher level of security for the operations of CIC is needed, and that the Department is not the main tenant of the building.

- Some regional officers were not able to state accurately their role and their task definition with regards to security. The DSO argued that the lack of personnel and capital explains why the Division is not fully involved in the regions, particularly for the follow-up of security measures.

On the other hand, the SSD seems to maintain close links with functions related to health and safety at work, property and equipment management, and staffing. External links with organizations such as RCMP (physical security) and PWGSC (contract security), appeared to be satisfactory.

Recommendation

It is recommended that the Director, Compensation, Security and Management Services, evaluate the relevancy of providing security (and other) services to other government organizations. This assessment could include a comparative analysis of common security services for other government buildings occupied by different departments.

3.2 Security Plan and Policy

Through our preliminary assessment, we found that the Department does not have a formal security plan in place. Although several future initiatives were presented by the SSD staff, they do not seem to be part of a comprehensive plan with short, medium and long-term goals and objectives. Moreover, regional security operations are excluded. This plan should also be integrated in the departmental strategic plan and approved by the senior management. The DSO indicated that efforts are being made to convince senior management to establish a department-wide security plan.

The interviews with security officers in regional offices revealed that some regions do not have a planning process or a program for security. While the Pacific/Yukon Region seems to be more proactive in the application of various measures and in the overall security management for their offices, the Atlantic and Quebec Regions have a rather reactive approach.

It was also noted that the Department does not have an overall security policy. There are some old policies derived from the departments that were part of the amalgamation leading to the creation of Industry Canada. These policies are available on the Intranet site of the Human Resources Branch. However, these policies must be revised to remove any references to the old departments and to reflect the 1994 revised security policy of the government. There does not seem to be any formal agenda for the revision of these policies or the development of a department-wide security policy.

Recommendations

The Director, Compensation, Security and Management Services should develop a complete security program, that is a plan which includes all the elements of the security function in all departmental sectors and regions.

The Director, Compensation, Security and Management Services should develop and implement a plan to create a department-wide security policy or to update existing policies.

3.3 Cost Recovery for Security Services

The SSD Management Director is responsible for the cost recovery of security services. The Administration Officer, Administrative Services, Human Resources Branch (HRB) does the invoicing and the fund recovery.

There are two types of cost recovery: 1) services offered for other government departments and agencies, and 2) services offered within the Department.

Services offered for other government departments and agencies

Presently the Department has service agreements with five organizations: the Millennium Bureau of Canada; Citizenship and Immigration Canada; the Canadian Intellectual Property Office; the Canada Industrial Relations Board; and the Public Service Staff Relations Board. These agreements vary from one to three years with an automatic renewal clause. The agreements are relatively different from each other. Coverage of service levels vary from one part of the security function to the overall corporate services. As well, the recovery terms vary from one agreement to the other (e.g., from a rate per service (ID card, access, etc.) to cost-sharing (Corps of Commissionaires)).

The Administration Agent, Administrative Services, HRB, issues invoices on a quarterly basis.

Auditors also observed that the Department provides services to other organizations without any formal agreement, including the Office of the Auditor General of Canada (ID cards, information desk, basic building service); Human Resources Development Canada (emergency system); and the Canadian Space Agency (emergency system).

Preliminary analysis revealed that the basis used for invoicing is not appropriate. No cost analysis has been carried to determine the actual and absorbed costs for service rates and cost-sharing. Costs are presently based on estimates and no annual analysis is conducted to increment costs depending on the increase of incurred expenses. Moreover, it was noted that the cost-sharing for commissionaires does not include overhead costs (supervision, etc.).

Services within the Department

Since 1995, the same services are offered within the Department on a cost-recovery basis. This approach has been implemented to meet a resource shortage within the HRB. The SSD has presently has a $337,000 budget for salaries and $66,000 for operating expenses. It also receives a

budgetary transfer of $400,000 from the Deputy Minister's Office for the Corps of Commissionaires. Through cost-recovery, the SSD has a surplus of approximately $1.2 M.

The cost-recovery operation presents some problems for the organization. First, as security within the Department is a critical function, the SSD and HRB staff indicated that the maintenance of an invoicing system adds work. Moreover, it was noted that:

- The invoicing for each ID card and each access modification request application discourages responsibility centres from requesting the service and creates a situation where longer and more risky periods are requested for the sole purpose of minimizing costs;
- According to the interviews, it is likely that some managers refrain from conducting security audits on temporary employees and consultants in order to avoid the associated costs; and
- The invoicing of SSD staff time leads to the transfer of responsibility centres' operating expenses to cover SSD salary expenses. These transfers between operating expenses and salary distort expenditure report within the Department.

In conclusion, cost-recovery is required for services provided to the other organizations external to the Department. However, it is crucial to have an adequate system which reflects actual and absorbed costs. With regard to internal recovery, this does not seem to be a method any more complicated than a simple budget transfer between responsibility centres.

Recommendations

The Director, Compensation, Security and Management Services should develop a system to evaluate actual costs related to SSD operations and should revise these rates on an annual basis.

The Director, Compensation, Security and Management Services should review the internal invoicing policy and use the information derived from the assessment of real costs to establish, at the beginning of each year, a budgetary transfer from other responsibility centres to cover security services according to the number of employees per sector.

4.0 Effectiveness and Efficiency of Security Function Delivery within the Department

4.1 Security Function Administration

4.1.1 Education and Training on Security

There is no formal security awareness program for departmental employees. Awareness training is conducted on an "as requested" basis. The Intranet site of Human Resources Branch includes also a page dedicated to security which includes departmental security policies as well as information of common use about the services. The regions do not have any awareness programs, except that sometimes reminders are sent electronically to staff in the British Columbia and Quebec.

The background paper on the security function, which was prepared for a colloquium with the Industry Sector, has recently been reproduced on a large scale in order to try to implement a more proactive program. The officer of staff awareness also indicated that the documents should be customized for each sector and region to reflect distinct features. Auditors noticed that the content of this document pertains more to practical information about security services, rather than to developing awareness in the true sense of the term.

The SSD staff wants to have more time and budget for the training of employees related to the security function. The same problem was raised in the Quebec Region where the lack of security training adversely affects managers because of limited knowledge in the field. The representatives of the Quebec and Atlantic Regions also reported that central services provided little support for information and awareness services.

Recommendation

It is recommended that the Director, Compensation, Security and Management Services put in place a formal security awareness program, which would encompass regions as well as Headquarters.

4.1.2 Classification and Designation of Sensitive Information and Assets

Presently, three classification guides from the old departments constituting Industry Canada are being used for the classification and designation of information. However, a new guide for the Department is in process of being developed and should be available by the end of February 2000.

The audit with managers responsible for file rooms shows that classified and protected information is labelled with the required security markings (i.e., protected, secret or top secret). On the other hand, the Department does not assign the A, B, C ratings for protected documents, as is specified in the TB policy. At the same time, in the absence of a sole classification guide reflecting ongoing departmental activities, the manager in charge of records management for the NCR does not perform any controls to verify if some documents are over or under classified.

There are no procedures or controls in place to ensure that documents required to be declassified after a certain period of time are, in fact, declassified systematically, at the request of managers. This situations increases the risk of over classification, and creates a congestion in file rooms during peak periods. On the other hand, the Department's records retention and disposal schedule seems to be followed and is compatible with TB policy. In regions, security officers reported that they are not aware of all the procedures for records classification and protection.

Recommendation

The Director, Compensation, Security and Management Services should ensure that the Department's new classification guide is part of the awareness program, that it ensures a follow-up and that it prompts managers to advise file rooms when documents are declassified.

4.1.3 Threat and Risk Management Method

The preliminary audit revealed that there is no Department-wide method for threat and risk management. There is presently no documentation which describes risks by sector, by business type or by location, and which is based on one method of assessment. However, it was noted that the risks associated to the Department are well known by the SSD staff concerning the main buildings (such as C.D. Howe and Jean Edmond) and some other secondary locations.

The assessment of threats and risks is a central component in the risk management method. However, threat and risk assessments have not been conducted in Industry Canada buildings at Headquarters or in the regions since the creation of Industry Canada.. The SSD recently engaged a consultant to conduct such an assessment in the C.D. Howe building. According to the TB policy, this type of assessment - which in principle could be performed by departmental employees - should be conducted in all buildings where the frequency of reported incidents and infringements and where the nature of assets and information seem to justify it.

Recommendation

It is recommended that the Director, Compensation, Security and Management Services establish a priority list of buildings, including those in the Regions, for which the Director considers appropriate to conduct a threat and risk assessment and establish a timeline for these assessments.

4.1.4 Offense, Infringement and Other Security-Related Incidents

Auditors observed that there is a process within the Department to deal with cases of offense, infringement and other security-related incidents. When one of these cases is reported to the Security Services Division, a standard report is used to enter all relevant data.

A part of the information from reports is usually entered in a computer program "Lotus Approach". Entires have not been made since September 1999 due to technical problems. The SSD wants to modify this database in order to make it more compatible with their needs. Auditors noticed that this database is not presently used to analyse the overall incidents and infringements (types, locations, periods), although it represents an interesting tool to assess threats and risks

In principle, all infringement and incident cases should be reported to the SSD. However, it was mentioned that some sectors or regions do not always report these cases because they do not want to call attention on their potential lack of efficient security measures. We observed that for the period of March 1996 to August 1999, on a total of 261 cases, only four incident or infringement cases came from regions. When asked to comment on these infringement and incident cases, regional officers did not provide any clear answers regarding the procedures to be followed and reported few known cases, but they admitted that there is no guarantee that all incidents and infringements have been reported.

There is an internal policy on infringements and incidents, but like all the other policies, it needs to be revised.

Recommendations

It is recommended that the Director, Compensation, Security and Management Services reinforce awareness efforts among regions to ensure that any type of infringement, offense or incident is reported to the SSD.

It is recommended that the Director, Compensation, Security and Management Services change the infringement and incident database so as to use it as an analysis tool in order to measure threats and risks associated to types of events, locations, period of year, etc.

4.2 Physical Security

4.2.1 Site and Accommodation of Facilities Enabling Risk Reduction or Elimination

Through our review of the Department's physical security, we observed that security requirements were, in general, taken into account during the choice of a site, the acquisition or the construction of a new accommodation, or a simple renovation. Facilities management services staff communicate to the SSD any new construction or new accommodation plans. The division then reviews these plans, makes recommendations and makes site visits at the end of the projects to ensure compatibility,

However, according to the SSD, regions do not follow this procedure. As the Quebec and Atlantic Regions reported the lack of security training and the lack of support from the head office (especially for aspects related to physical security), there is no evidence that all important criteria are taken into account during new construction or moves.

Recommendation

It is recommended that the Director, Compensation, Security and Management Services develop a list of steps to be followed as a control tool to help regional security coordinators and senior managers in ensuring that all significant security elements are considered during new construction or moves.

4.2.2 Physical Protection Measures

In the NCR, the Department has offices in 15 locations. The SSD offers these locations an arra of services related to physical protection and emergency measures, including camera surveillanc guards, ID cards, electronic access control and patrols. Our visit to the security control centre located at the Jean Edmond building revealed that the Department was equipped with a modern system, including an integrated access system (Level) and a security information management system (ID cards).

Auditors found that physical protection measures are satisfactory for several departmental offices. However, some weaknesses were identified in ensuring this protection, especially in some secondary locations in the NCR and in the regions.

For the main buildings in which the Department occupies office space, we were told that most of the areas at risk, such as the file rooms and the computer control rooms, are well protected,. But the SSD could not ascertain whether measures are adequate for buildings where the Department has a low number of employees, especially since a security system audit has not been conducted. On the other hand, we observed that access to offices of the C.D. Howe building is well protected in the evening and during week-ends, but often open to public during regular work hours. According to the DSO, most of the reported infringements/incidents related to theft of personal belongings are the consequence of this open access. However, this weakness should be addressed in the threat and risk assessment being conducted for the C.D. Howe building.

According to the DSO, departmental employees are aware of the appropriate measures to protect classified and protected documents. However, there are no security "sweeps" (control measures) undertaken outside regular work hours to verify if employees have placed documents in locked cabinets. This might increase the possible access of classified or protected documents by employees who do not have the corresponding security ratings or by the public in the case of C.D. Howe building.

Interviewees noted that there is no guarantee that regional offices have all the necessary physical protection measures, both for assets and employees. The SSD believes that there are gaps in several areas, such as easy access to work space from the reception area.

Finally, the audit indicated that since the creation of Industry Canada, the SSD has inspected some departmental offices in the NCR. In the case of regions, only the regional administration offices of Place Ville-Marie in Montreal have been subject to an audit of physical security by the SSD, after which remedial actions were brought by the regional officer. In the Atlantic Region, advisory meetings were also held by the SSD. However, we observed that there is no periodic review or control program of physical security measures for all of the locations of Industry Canada.

Recommendations

Given the uncertainty related to the absence of controls performed outside regular work hours (sweeps) to verify if employees have placed documents in locked cabinets, it is recommended that the Director, Compensation, Security and Management Services ensure that this gap is addressed in the threat and risk assessment for C.D. Howe building.

Given the uncertainty with regard to physical protection measures in regional offices, it is recommended that the Director, Compensation, Security and Management Services inform all regions of the measures to take to ensure a physical security in their offices, and conducts a follow-up.

It is recommended that the Director, Compensation, Security and Management Services establish a periodic review and control program of physical security measures for all the locations occupied by the Department.

4.3 Personnel Security

The SSD is responsible for the administration of security and reliability rating of all employees reporting to Industry Canada's Deputy Minister. The Department's policy is to require, at a minimum, an enhanced level of reliability as soon as a permanent employee or a term employee has access to Industry Canada's offices.

The audit found that the Department has a security investigation program which is relatively compatible with the government security policy and with the personnel security standard. The interview with the manager in charge of security revealed the existence of a clear and well-established process, both for offices in the NCR and in the regions. The regions must, in fact, use the security investigation service offered by Headquarters.

The SSD conducts periodic audits of sample of files for personnel security. These audits verify, for example, if signatures of individuals have been obtained for their consent to be subject to an investigation, if dates show that the individual began work after the result of the investigation, etc. However, we observed that, despite these audits and the awareness efforts, including a guide made available to managers, there are still some weaknesses:

- The government security policy stipulates that a permanent employee or a term employee should hold office only once the result of the security/reliability investigation is obtained. The manager of personnel security indicated that this condition is generally respected in the case of permanent positions, but a contract worker or a trainee often has access to the departmental offices without knowing the result of the inquiry or, even worse, without initiating an inquiry request. Awareness campaigns for managers in the NCR and in some regions have helped to improve the situation, but there is still room for improvement according to the manager. In the Quebec Region, auditors were told that to offset this trend, regional informatics services will henceforth give a computer access account only when an employee receives the result of his or her security inquiry, as prescribed by the Treasury Board's informatics security policy.

- The government security policy requires that the security/reliability ratings be updated every ten years, except for the very secret level which must be updated every five years. According to the manager of personnel security services, the update of security ratings can extend up to eleven years.

With regard to the disposal of security files, the SSD mentioned that this is done in compliance with the records retention and disposal schedule of National Archives of Canada.

Recommendations

It is recommended that the Director, Compensation, Security and Management Services enhance the awareness among managers, including regional managers, in order to avoid that contract workers and trainees having access to the departmental offices or beginning to work before obtaining their security/reliability ratings.

It is recommended that the Director, Compensation, Security and Management Services ensure that the period of updating security/reliability ratings is compliant with Treasury Board recommended level.

4.4 Security and Management of Emergencies

The audit showed that necessary measures have been followed to protect sensitive information and assets, as well as employees, during any type of emergency, for all the locations where the Department has many employees. Procedures are available for both security staff and employees. For locations where the Department occupies a small portion of the available space, the SSD reports that they have assessed the measures taken by the owners or the main tenants of the buildings and that these measures are compatible with Treasury Board's policy.

5.0 Conclusion

This preliminary audit demonstrated that, despite a few weaknesses identified, the security function within the NCR does not present any major problems, especially for the key locations.

The most important recommendations refer to the organization and administration of security function. Since these recommendations will prompt the SSD to take many significants actions in the Department's locations in the NCR and in the regions, it would not be advisable, at this point, to conduct a further audit of security function. However, it would be appropriate to conduct a follow-up of the status of implementation of recommendations in one to two years time. This follow-up could include a visit to one or two regional offices, if deemed appropriate.