Audit of Security

Corporate Management Branch

Final Report

May 14, 2004

Table of Contents

Executive Summary

As part of its approved Audit Plan for the 2003-2004 fiscal year, the Internal Audit and Assurance Directorate of the Corporate Management Branch of the Public Service Commission (PSC) undertook an audit of security. The audit satisfies the Government Security Policy[1] (GSP) requirement for an independent assessment of how security is implemented in the department and the degree of compliance with the GSP and Operational Security Standards[2]. The purpose of the audit was to provide assurance to the President that the PSC's management processes comply with the new Government Security Policy (GSP).

The audit sought to confirm:

- whether the PSC has put in place a security organization that meets the intent of the GSP;
- whether the department has developed and implemented an adequate management framework for the implementation and administration of security; and
- whether the security program in PSC has been effectively implemented, and is efficiently and effectively operated.

Key Findings

The President of the PSC has delegated the role of Departmental Security Officer (DSO) to the Director General, Finance and Administration, who is responsible for the development, implementation, maintenance, coordination and monitoring of the security program and ensuring its consistency with the GSP.

The Director General, Information Technology Services Directorate (ITSD), is responsible for Information Technology security and for the development and maintenance of an IT security program.

[1] *Government Security Policy, February 2002* The authority for this policy derives from Section 7 of the Financial Administration Act. This policy replaces the June 9, 1994 policy and its November 1994 and June 1995 amendments.

[2] Operational security standards approved by the Treasury Board Secretariat. They contain mandatory and recommended measures to direct and guide the implementation of the policy. Note that new standards are being produced, but some are in draft only.

The PSC operates regional offices across Canada; local staff assume responsibility for corporate services such as administration and information technology.

In this environment, the implementation of a PSC-wide security program is difficult, and is often seen by managers as a sideline to “regular business”. The risk elements in terms of security are not as high as in other organizations because of the nature of the PSC business and the related business information.

Overall the PSC has achieved the implementation of a security program and organization that meets the major requirements of the Government Security Policy.

- The PSC has implemented a framework for security and roles and responsibilities are clearly defined and assigned.

- As in other areas of security, the responsibility for physical security is split between headquarters and the regions. Most staff interviewed felt that physical security was effective in their location.

- The personnel screening process is in place and functioning as expected. As well, the process for handling employees leaving the PSC is in place and functioning.

- Contracts in PSC are the responsibility of the business manager, as is adherence to contract security guidelines. The audit concluded that managers are aware of security requirements in contracting and that they ensure the level of security required is adequate.

- The audit found that staff were aware of the procedures to follow and forms to use to report incidents.

Despite the overall positive picture, the audit concluded that there are opportunities for improvement in the following areas:

- The lack of a comprehensive awareness program has resulted in some inconsistencies among staff in the understanding and interpretation of their roles and responsibilities;

- Communication throughout the security community in the PSC is hampered by the lack of a formal and regular communications mechanisms among security partners at headquarters and in the regions;

- A comprehensive policy framework has been implemented. However, there is a lack of an approved strategic plan for the security program, without which there is a risk of important security priorities not being addressed;

- Security is seen as a management concern, but not necessarily a priority: The focus is on administrative routine. While there are elements of a security awareness program in place, it is not a proactive program and employees interviewed were somewhat complacent regarding activities that ensure the PSC environment is secure;

- Efforts are being made to ensure the use of Threat and Risk Assessments, especially in new systems development projects. Recognition of the value and importance of security risk management is growing, but improvements are required to enhance the risk assessment process;

- Given the overall increasing reliance on information technology to meet PSC business goals, IT security has taken on a more significant role. However, IT security has challenges related to: shared roles and responsibilities across ITSD, other corporate groups with IT resources (eg. Finance), and regions; resource limitations; and continuous technological change;

- While a draft business continuity plan (BCP) has been prepared, until it has been finalized, distributed and tested, the organization is at risk of not being able to provide continued services in the event of a disaster. The final BCP for all sites must reflect the reality that PSC services are not seen as mission critical. The integrity of information must be protected and information must be available, but not necessarily immediately.

1.0 Introduction

The purpose of the audit was to assess and to provide assurance to the President of the Public Service Commission (PSC), that the PSC's management processes comply with the new (February 2, 2002) Government Security Policy.

1.1 Background

The PSC is the independent agency responsible for safeguarding the values of a professional Public Service: competence, non-partisanship and representativeness. It does this by administering the *Public Service Employment Act* (PSEA) and a merit-based system and, inter alia, being responsible for the appointment of qualified persons to and within the Public Service; by providing recourse and review in matters under the PSEA; by delivering training and development programs; and by carrying out other responsibilities as provided for in the PSEA and the *Employment Equity Act* (EEA). The mission of the PSC is, through its statutory authorities, to: maintain and preserve a highly competent and qualified Public Service in which appointments are based on merit; and to ensure that the Public Service is non-partisan and its members are representative of Canadian society.

At the time of the audit, the PSC operated five business lines.

The **Resourcing** business line works with federal departments and agencies to ensure a resourcing system that provides a highly competent Public Service that is non-partisan and representative of Canadian society. The business line encompasses activities in support of delegated and non-delegated staffing. These include: program development; administration of staffing delegation; establishment of tests and standards for selection; administration of staffing priorities; recruitment and promotion; and diversity and employment equity initiatives. The PSC is also responsible for the delivery of the employment equity initiatives and corporate development programs.

The objectives of the **Learning** business line are to improve the professional competence of federal public servants and to enable them to meet the language proficiency requirements of their positions. The business line is composed of two main service lines: language training; and professional development for non-executives.

The objectives of the **Recourse** business line are to protect public interest and to promote the application of merit, fairness, equity and transparency. It provides independent recourse processes including appeals by public servants against alleged breaches of the *Public Service Employment Act* and Regulations on matters such as appointment and promotion. Recourse is also responsible for the investigation of complaints and irregularities in the resourcing process that are not subject to appeal, for the investigation of complaints of harassment in the workplace and for conciliating settlements where complaints are upheld.

The **Oversight and Outreach** business line provides knowledge, intelligence, insight and advice to support the PSC's ability to help build an professional and representative Public Service. This business line provides the capacity to measure, report, provide advice, and deliver policy in areas within the PSC's mandate. It provides strategic analysis and research, environmental scanning, and liaison with stakeholders, on issues related to the PSC's role as guardian of the integrity of the appointment process.

Corporate Services business line provides the PSC with central services and systems in support of corporate management and all PSC program activities. It includes the activities of the President and Commissioners, business planning, management systems and policies, finance, human resources management, information technology, internal audit, and other administrative and support services.

The PSC's annual budget is approximately $123M with some 1,600 staff, of whom 900 are located in the National Capital Region.

The Administrative Services Division of the Finance and Administration Directorate provides the lead for the Security Program, with policies, procedures and standards to ensure that the prescribed levels of security are maintained throughout the PSC.

1.2 Objectives

The overall objective of the audit was to meet the Government Security Policy (GSP) requirement for an independent assessment of how security is implemented at the PSC, and to measure the degree of compliance with the GSP and Operational Standards.

In February 2002, the GSP was updated to become more rigorous in terms of required action on the part of departments and agencies. It now places more emphasis on the management framework and accountability structure within the departments and agencies.

Specifically, the audit's objectives were:

- to determine the compliance of the PSC in implementing the security standards of the GSP and its operational standards; and
- to assess the efficiency and effectiveness of PSC's security program.

1.3 Scope

The following areas were included in the scope of the audit.

Security Organization:

This included an assessment of the structure of security management at the PSC in order to verify if security responsibilities are well defined, established and assigned to personnel whose position description includes security responsibilities.

Security Management:

This included an assessment of the security program, the security education and training programs, the handling of breaches and violations of security and other security-related incidents, and the protection measures taken for external communications.

Physical Security:

This included an examination of the location and layout of some PSC installations, the identification and application of protection measures in the installations, and the examination and controls of physical security measures.

The following were examined in detail using the site inspection questionnaire: national headquarters (L'Esplanade Laurier) and three regional offices (National Capital and Eastern Ontario Region, Central and Southern Ontario Region, and Quebec Region).

Personnel Security:

This covered personnel security investigations, the authorization, refusal and revocation of security levels, and the measures required at employees' termination of employment.

Security and Management of Emergency Cases:

This included an assessment of whether managers throughout the PSC have taken the necessary action to protect sensitive information, assets and employees, and to provide for the resumption of essential business operations following an unplanned interruption.

Information Technology Security:

This included physical, personnel, hardware/software and communications security assessments of whether necessary actions are taken to: ensure that the IT security structure and its relationship and coordination with the overall security structure in PSC meet GSP requirements; provide Threat and Risk Assessment reviews of IT assets and procedures for product development, maintenance and operation; and control electronic information, IT and communications assets.

The 2002 Audit of Records Management covered: classification and designation of sensitive personal information, declassification and disposal, and the measures of protection for sensitive personal information. The audit indicated that the physical security processes were a key element of the protection of records - this was followed up as part of the security audit work.

The 2002 Audit of Contract Management assessed the contracting function. Security is one requirement for contracts. The Audit of Security conducted a brief review of contracting to ensure the level of security required is adequate and managers are aware of security requirements.

1.4 Audit Approach

The audit approach included an extensive review of documented policies, procedures and guidelines, interviews with approximately 63 individuals at various levels both corporately and regionally, as well as the completion of detailed site inspection checklists.

Through the use of an integrated methodology and drawing from the Treasury Board Secretariat's (TBS) Guidelines for the Audit of Security, the audit team undertook a comprehensive analysis of the issues.

2.0 Audit Findings

The audit scope included an examination of six major and two related areas. Based on the results of the audit work finding are grouped into three major areas, as follows.

2.1 Security Organization

In examining the organization of security at PSC the audit team sought to determine whether PSC has put in place an organizational regime that meets the intent of the GSP. A formal accountability framework with suitable communications capabilities must be evident.

2.1.1 Roles and Responsibilities

Security responsibilities have been defined, established and assigned to specific personnel.

Finding

The GSP states that the President as “the head of the department”, is accountable for safeguarding employees and assets within the PSC, and for implementing the GSP. Under the policy, departments/agencies must appoint a Departmental Security Officer (DSO) to establish and direct a security program that ensures coordination of all policy functions and implementation of policy requirements.

The President has delegated the role of Departmental Security Officer (DSO) to the Director General, Finance and Administration, who is responsible for all aspects of the PSC security program. The DSO has delegated the management of the program to the Director, Administration, who is the Deputy Departmental Security Officer (DDSO). The DDSO is responsible for the development, implementation, maintenance, coordination and monitoring of the security program and for ensuring it is consistent with the GSP.

Reporting to the DDSO is the Chief, Security Services, who is supported by three full-time employees. This group develops, implements and monitors physical and personnel security.

The Director General, Information Technology Services Directorate (ITSD) is responsible for information technology security, which concerns the security aspects of information, hardware, software, data communications and operations in the information technology environment. Supporting the DG is an Information Technology Security

Coordinator (ITSC), who is responsible for the development and maintenance of an IT security program. The ITSC provides functional direction on IT security and co-ordinates IT security activities throughout the PSC. There are several staff in various sections of ITSD who carry out specific security activities. The IT security activities are integrated with the operational role of IT.

Responsibility centre managers are responsible for the protection of the employees, assets, information, services and facilities under their jurisdiction. Regional Directors have the same responsibilities plus physical security and business resumption and disaster recovery planning. Depending on the size of the regional office, the individual responsible for administration activities is usually also responsible for security.

Staff and contractors are responsible for safeguarding assets and information in their possession against theft, damage, unauthorized access, interruption or modification. Like many other government departments, the roles and responsibility for security are strategically, functionally and operationally distributed in PSC. Except for staff in Security Services with exclusive security responsibilities, security is always a shared role.

Conclusion

The accountability framework for security is in place and roles and responsibilities are clearly defined and assigned.

2.1.2 Communications and Linkages

A more formal framework to sustain a dialogue within the PSC security community would enable the PSC to meet the standard security policy compliance objectives efficiently and effectively over time.

Finding

The GSP indicates that part of the DSO role entails the coordination of GSP activities. The DSO should be positioned strategically within the organization so as to be able to provide organization-wide advice and guidance to members of the senior management team. Two key elements of a successful security organization are effective communication across the organization and linkages to promote the coordination of an organization-wide security program.

At headquarters, in response to 9/11 an Incident Management Team for L'Esplanade Laurier was created by the Deputy Ministers of Finance, TBS and PSC to deal with security issues. The PSC is an active participant. In addition at L'Esplanade Laurier Steering Committee there is an ADM level steering committee that meets monthly to discuss security issues. Physical and employee security is managed jointly with TBS and Finance. Furthermore, there are active health and safety committees in all PSC locations.

Interviews with the security community revealed a general lack of communication between regions and headquarters and within headquarters. Communication and coordination of security matters are weakest between the regions and headquarters (HQ).

Regions share mutually beneficial tools or techniques applicable to regional security management. However, with security being only a minor role for staff in some regions, many find it difficult to be experts; receiving central expertise from HQ is important. Many of those interviewed indicated that HQ could provide more functional direction, advice and leadership, thus improving the sharing of processes, procedures and standards.

Although there is ongoing communication between Security Services and the Information Technology Security Coordinator, a more formal linkage to assess the security program and to share information would be useful.

Conclusion

With security being the responsibility of many areas in the organization, communication and linkages are important to ensure consistent implementation of the security program and protection of staff and assets. While many communication venues are available and used, there is room to improve the overall framework and the dialogue amongst PSC security community members.

Recommendation

1. It is recommended that the Vice President, Corporate Management Branch:

- establish formal and regular communication mechanisms between regional and headquarters partners and among headquarter partners to facilitate the coordination and implementation of security program components.

2.2 Security Management

In determining whether the PSC has developed and implemented an adequate management framework for the implementation and administration of security, the audit looked for the components of such a framework, including an established policy, an active planning element, appropriate training and awareness, and a risk management approach.

2.2.1 Policy and Planning

A comprehensive policy framework for security has been implemented in the PSC. A strategic plan for the security program would help to ensure its ongoing effectiveness and efficiency and the continuous addressing of security risks.

Finding

The Government Security Policy addresses the need to manage security risk at a strategic, senior management level. The strategic nature of the policy drives the need for an integrated, strategic-level security plan and related policies to be put in place by departments and agencies.

The PSC Security Policy is up to date with government-wide policy changes made in the last few years. The policy is available to all PSC staff and contractors through the PSC intranet. It includes roles and responsibilities of all staff with respect to security. It is a comprehensive document that incorporates policy statements on all aspects of security, and it references available standards, directives, handbooks and additional information. Policies in areas such as information technology, records management and contracting that have specific security elements are also available to all staff. The intranet site is used as a repository for PSC security policy and procedural material and it provides consistent, adequate and up-to-date material to staff.

The PSC has established the role of DSO to address the strategic-level direction for security. Planning has been focussed on the immediate operational needs of security and the implementation of the program. Security planning is at present limited to an annual work plan established for the Deputy DSO and Security Services staff. In the regions, security initiatives exist as part of individual work plans. IT security plans are part of the ITSD annual work plan. Consequently, security elements are not brought together within a comprehensive security plan at a strategic level that is formally integrated across the PSC.

While the DSO and Security Services have managed all events giving rise to enhanced security such as the G8 summits, blackouts, demonstrations, water contamination, false alarms, etc., the creation of updated security policies and integrated plans is a key output of a well-defined strategic vision for security. In order to secure the investment needed to implement appropriate standards, the security function must be able to present its strategic vision and influence senior managers. This is achieved through the formulation and submission of a comprehensive security plan. It must include all aspects of security - physical, personnel, information technology and assets.

Conclusion

The PSC has developed and implemented a comprehensive policy framework for security. The matrix character of PSC means that security receives only as much attention as the assigned individuals can afford in competition with other priorities in terms of both time and budget. Without an integrated pan, there is a risk of important security priorities not being addressed.

Recommendation

2. It is recommended that the VP, Corporate Management Branch:

   - establish a multi-year strategic plan for security (personnel, physical and information technology) and identify critical security priorities; and

   - establish an integrated, annual security plan with milestones, and monitor and review security deliverables on a periodic basis in conference with their administration, regional, program and information technology partners.

2.2.2 Training and Awareness

While elements of a security awareness program are in place, it is not proactive program; employees and assets are at risk of not being adequately protected as a result of complacency regarding security issues.

Finding

The GSP requires departments and agencies to have a security awareness program. An awareness program should include the following elements:

- orientation sessions for new employees (security as one of many topics);

- ongoing reminders of responsibilities (locking up sensitive information), updates on issues and areas of concern (e.g. notification of viruses or an increase in thefts); and
- monitoring (security sweeps and identification of problems).

The GSP requires that individuals be briefed on the access privileges and prohibitions attached to their screening level prior to commencement of duties. The PSC has an orientation program for new employees that contains a security component. However, it is only available at HQ and not all new staff are required to attend the sessions. Two regional offices have also developed orientation programs for new employees which cover security. As most of the security topics are the same, it is not effective or efficient for regions to develop their own program.

On a weekly basis all staff is required to accept their responsibility for use of information technology services and equipment. A screen is automatically generated when the employee signs on. Employees must indicate that they accept accountability for using the services and equipment in compliance with the various PSC policies and are aware there are potential sanctions if privileges are abused. While this safeguard is an excellent first step, the process is set up so that an employee does not have to actually read the terms and conditions. Over time there is a risk that employees will not pay attention to the reminder and its intent.

The Records Management unit has developed and offered to HQ and regions a training session on safeguarding sensitive information, that included security as an important element. Participants came away with an understanding of the levels of information (top secret, secret, confidential and Protected A, B and C) and the requirements for marking, transmission, protection and destruction of information. The initiative did not reach across the entire organization and not all staff attended the course. As well, the contracting group provides training, and security is covered.

The GSP requires departments to monitor adherence to security policy; this in turn promotes the security awareness of employees. ITSD monitors network use and compliance with PSC Policy. Security Services has funded, through partnership with the RCMP, security training and awareness courses for PSC employees across Canada. Monitoring of physical security is usually accomplished through security sweeps of facilities. Security Services does not do any security sweeps to identify areas of concern or problems.

The PSC does not have a formal requirement for managers who are responsible for security to receive training. Heads of administration in the regions are, in general, delegated responsibility for the day-to-day activities related to local security. Many have not had any security training and are provided minimal guidance from corporate security. This is exacerbated by the lack of a standard, department-wide program or plan for employee security awareness. Although staff are aware of emergency procedures in case of specific threats such as fire emergencies, and evacuation exercises have been conducted, it was evident during interviews that the level of awareness with respect to security varied significantly among staff.

Occasionally, e-mails about security are sent to all staff; but they are mainly focussed on information technology - in particular about new viruses or worms. In addition, no mechanism exists to ensure all staff actually read the broadcast e-mail.

Conclusion

Even though the PSC has not established a formal awareness program, elements of a program are in place. Security is seen as a management concern but not necessarily a priority, and the focus is on administrative routine. Without an active awareness program, staff can get complacent about security or not understand the implications of certain actions.

Areas of importance that should be included in the awareness program that reminds all senior managers and their staff about security requirements are:

- personnel security clearances are completed prior to appointment;
- contracts have requirements for the appropriate level of clearance;
- all employees and contractors who leave the department have returned departmental assets and information, as per departmental security guidelines;
- steps for handling sensitive information and assets; and.
- the protected ABC regime is implemented properly.

Recommendation

3. It is recommended that the VP, Corporate Management Branch:

- ensure a security education program for all employees, and a training plan for security staff, be formalized in the annual security plan to include metrics for effectiveness, efficiency and compliance; and

- ensure that security sweeps are conducted on a regular basis.

2.2.3 Risk Management

While some Threat Risk Assessments have been completed, they have not been completed for all systems, services and facilities, making it difficult to determine whether sufficient safeguards have been implemented to protect all staff and assets.

Finding

The Public Service of Canada is moving toward a risk management approach to the work environment. The government's policy makes it incumbent on managers to be informed about the security threats, vulnerabilities, impacts and risks to which their business operations may be subject. The standard approach to assessing risk is the use of the Threat and Risk Assessment (TRA).

Certain areas within PSC are familiar with the TRA process - in particular IT. All new information systems development projects operating under the PSC IT Project Management Framework are required to do TRAs at the various stages of development. However, not all information systems at the PSC have had TRAs completed. For example, some older legacy systems were not assessed when it was determined that the effort was not cost-effective as documentation was poor or the systems were being phased out. For the most part, TRAs for systems development projects are contracted out, as the PSC does not have the expertise and it is more cost effective to use experienced contractors.

A number of TRAs have been done on sites occupied by the PSC. These are normally done in conjunction with the other tenants of the building. A number of these were done through Public Works and Government Services Canada (PWGSC), especially if they were the building owner or manager. Not all regional sites have had a completed or up-to-date TRA.

Managers interviewed during the audit pointed out that the PSC is an organization that, due to the nature of its work, is not considered to be a high risk for threats. The PSC relies on physical security systems and IT security. However, the organization is moving in the direction of risk management. To date, TRAs carried out at the PSC seem to be focussed on specific IT applications and services, and not on overall business delivery. Audit interviews demonstrated a varied understanding of risk management and threat risk assessments. It was not evident what the Security Services role was in completing TRAs.

Conclusion

Overall, PSC managers are primarily concerned with the impact of negative security incidents and see physical controls as the primary means to a secure environment. Although the department is moving toward security risk management, improvements are required in the application and coverage of the process.

Recommendation

4. It is recommended that the VP, Corporate Management Branch

- ensure a review of the security risk assessment process and initiate improvements to expand and broaden coverage to align with the PSC risk management framework.

2.3 Security Operation

The GSP identifies security policy functions - in addition to the security management framework - which together comprise the departmental Security Program. These elements are examined in order to assess whether the Security Program has been effectively implemented, and is efficiently and effectively operated.

2.3.1 General Physical Security/Protection of Assets and Employees

Finding

Physical security at the different sites varies to some degree and depends on many factors, including awareness, local management priorities, resources, and the other building tenants (private or public sector). In many cases the PSC is not the primary tenant and often has lesser security requirements. As a result building security meets the more stringent requirements of the other tenants.

Security Services is responsible for physical security at HQ and provides functional direction to the PSC. Regional Directors are responsible for managing all aspects of physical security at their sites. Those interviewed indicated that little functional direction is provided to regional and district offices. PWGSC usually provides the functional direction locally, with respect to physical security.

At HQ the PSC relies on the security guards on the main floor for limiting access to the floors it occupies. Staff of the other tenants (TBS and Finance) have access to all floors, including those occupied by the PSC. There are cipher locks on PSC floors but in many cases the codes have not been changed recently or are known by many staff from other floors and former employees. During core hours many floors leave these doors open. All floors have cipher locks and they are all closed during non-core hours.

The PSC has had few reported incidents of assets being lost or employees put at risk. Staff interviewed did not feel at risk. Information is at minimal risk. Secret information was stored in the proper cabinets with the approved locks.

Conclusion

As in other areas of security, the responsibility for physical security is split between HQ and the regions. Most staff interviewed felt that physical security was effective in their location. The risk was seen as higher in sites where the tenants included the private sector. At HQ for the most part there is a dependency on security guards for controlling physical access to the building. They do look at ID cards but the pictures and expiry dates are small and when it is very busy it is hard to examine them carefully. There is the risk of unauthorized individual getting onto PSC floors.

2.3.2 Personnel Screening

Finding

All employees and contractors must be screened to the highest level of information and assets that they will access as part of their job duties. This screening must be completed before they have physical access to the work environment and access to information or other assets. Upon termination, all employees and contractors must return all assets; in addition they have a continuing responsibility for the confidentiality of information.

For most positions at the PSC, “Reliability” is the maximum level required. There are a number of senior level positions whose incumbents have access to information at the “Secret” level; this requires a secret level. Some of the information technology staff have recently been upgraded to Secret because of their extensive access to information. Contractors require, as a minimum, the “Reliability” level.

Security designation is part of the PSC classification process. Each position has an established level of security based on the responsibility centre manager’s decision, with Enhanced as the minimum. The staffing process includes obtaining personnel security screenings before an individual is offered a position. Similarly, in the contracting process the responsibility centre managers define the security requirements. The security level must be obtained before the contractor is allowed on site. Security

Services is responsible for arranging for the screenings and notifying the hiring manager, so that a letter of offer can be sent or other contracting mechanism can be completed.

Termination procedures and forms exist for the timely and complete separation of terminated individuals and the retrieval of assets, such as ID cards. These procedures are readily available through the intranet. Everyone interviewed during the audit were aware of the procedures and forms.

Conclusion

The personnel screening process is in place and functioning as expected. As well, the termination process is place and functioning.

2.3.3 Information Security

Finding

The unauthorized disclosure of information, with reference to specific provisions of the *Access to Information Act* and the *Privacy Act*, is a risk that is intended to be managed by the provision of information security safeguards. When such disclosure could reasonably be expected to cause injury to the national interest, the PSC is required to classify and mark such material as "Confidential", "Secret" or "Top Secret", depending on escalating potential impacts. When the expected injury from disclosure is to private and other non-national interests, such information is considered protected and must be categorized and marked "Protected A", "Protected B" or "Protected C".

Managers generally agree that PSC is not a “high-risk” government agency when compared to other departments and agencies. The PSC has adopted the “Protected A/B/C” regime and the majority of its information is classified at “Protected B” or lower.

Within the last two years training sessions have been conducted by Records Management on the designation and classification of information. Staff have been provided with a laminated sheet that summarizes the requirements for safeguarding sensitive information.

A minimal amount of information at the PSC could be classified “Secret” or higher. The audit reviewed areas where this information was located. In all cases, it was stored in appropriate containers with the approved style of locks that were properly engaged. Sensitive information such as tests and test results are protected by a special set of controls over access, distribution and storage.

The electronic transmission of sensitive information is of some concern throughout the PSC, as the electronic network is limited to "Protected A" level information or less. Staff have been advised not to send sensitive information across the network. The policy and guidelines on the use of electronic mail and network are clear on staff responsibilities.

The PSC is in the process of developing an information management strategy and vision. This will include both electronic and paper-based information and its security. It is recognized that the classification and archiving of electronic information are an area that needs to be addressed within this process.

Conclusion

Information security, while important, is not crucial to program operation in the PSC. However, the personal nature of the information means its protection and security is important to maintain the integrity of the business processes and the reputation and integrity of the PSC.

2.3.4 Information Technology

Finding

Information management (IM) and information technology (IT) within the PSC are evolving as a result of an increasing commitment to policies and standards for the delivery of IT services.

The IT Security Coordinator (ITSC), the Director of Technical Services, is responsible for developing and maintaining an IT security program. The ITSC provides functional direction on IT security and co-ordinates IT security activities throughout the PSC. There are several staff in various sections of ITSD who carry out specific security activities (e.g. network). IT security activities are integrated with the operational role of IT. Regional LAN managers who are also involved in IT security get functional direction from the ITSC via regular teleconferences.

The ITSC has significant operational responsibilities in addition to IT security responsibilities. From a budgetary perspective IT security is not funded as a distinct activity and IT security activities are resourced within various areas of ITSD. Consequently, specific needs are not addressed. Historically, a position was dedicated to IT security but budgetary pressures have resulted in the position not being filled after the departure of the most recent incumbent.

The PSC has adopted a corporate approach to the development, maintenance and operations of systems. A committee structure is in place for the approval and management of IT development and maintenance. A project management framework based on TBS's Enhanced Management Framework has been implemented. It institutes standardized development processes that include a requirement for sensitivity statements, threat and risk assessments, and an impact assessment to test coexistence with the PSC's technical infrastructure. A test laboratory is available. A change management process has been implemented and applications must be accredited before going into production. The ITSC is involved in conducting TRAs for new projects.

As we reported in Training and Awareness, staff in the PSC are required to acknowledge security responsibilities weekly by accepting an appropriate use statement for access to networks and government supplied computer equipment at log-in. Processes are in place to ensure passwords are changed regularly and that they cannot be reused.

The ITSC participates in the development of IT policies and standards (e.g. wireless, use of e-mail). The PSC has very specific standards in terms of the network, hardware and software that will be supported by ITSD. The IT environment is managed and monitored centrally. The PSC uses common firewalls, virus software and access control software.

A change management process is in place and is followed for the certification of new systems and changes to existing systems. There are areas, such as Finance, that have the ability to change data without going through a standard change management process, although it is discouraged. This brings into question the degree to which IT operational standards are met, including such IT security concerns such as access management, emergency planning, user account management and removal of sensitive information from storage media.

Most staff interviewed indicated they receive information in terms of IT security risks such as viruses and worms.

Conclusion

IT security administration is complicated by shared responsibilities across the IT environment. A document detailing the various elements and who is responsible would be useful to ensure all elements are in place and understood. All changes to data or software should go through the change management process.

2.3.5 Contingency Planning

While a draft Business Continuity Plan (BCP) has been prepared, until it has been finalized, distributed and tested, the organization is at risk of not being able to provide continued services if there is a disaster.

Finding

Federal government policy requires departments and agencies to establish a business continuity planning program to provide for the continued availability of critical services and assets within the context of the Security Program. The BCP Program must include a governance structure, monitoring of overall readiness, and continuous review, testing and audit of the Program. The specific operational standards in support of the GSP have yet to be finalized by TBS.

Like most departments and agencies, the PSC developed a BCP for IT as part of its Year 2000 business resumption planning. More recently a draft BCP has been prepared and discussed at Executive Management Committee. PSC is now waiting for TBS standards to be produced in order to create a final version.

Security Services is responsible for coordinating emergency procedures for headquarters and has done a good job during infrequent events such as last year's blackout. Numerous e-mails and voice-mail messages are left on employee phones and computers to address emergency situations such as L'Esplanade Laurier water contamination, blackout, mould, air quality status, etc. The DSO and Security have been complimented in the past, in particular, for managing the L'Esplanade Laurier water contamination situation; all the employees in Security who were involved were given a Recognition Award by the former President at an EMC meeting.

Regional and district offices have current emergency plans, developed in conjunction with the other tenants in their buildings - particularly for specific threats, incidents, thefts, follow-ups on summits, demonstrations. Information and advisories are received from the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). For example, in the case of the Vancouver area, earthquake disaster simulation was coordinated with the municipal, provincial and federal authorities. Earthquake kits were replaced in 2001-02. As well, in the Vancouver area a joint US Sponsored counter-terrorism exercise was conducted in May 2003. However, regional and district offices do not have BCPs and they do not have the expertise to develop them.

Events such as the power outage and ice storm have further focussed the need for contingency planning and security preparedness. However, it was evident during these events that PSC services are not deemed essential. Business processes and information do not need to be available immediately, but the integrity and availability of the information are important for the longer term. ITSD has implemented a backup process that includes off-site storage and provides for the managed shut down of equipment to ensures damage to information is minimized. Events like the blackout have resulted in improvements. An example is the importance of knowing who the crucial contacts are and how to contact these individuals.

Conclusion

The PSC requires a final BCP for all sites, but it must reflect the reality of the PSC not having mission-critical services. The integrity of information must be protected and available, but not necessarily immediately.

Recommendation

5. It is recommended that the VP, Corporate Management Branch:

- pending finalization of government-wide standards, ensure that updated plans for all business operations at all sites are in place to provide for the continued availability of services and assets.

2.3.6 <u>Contracts</u>

Finding

The GSP applies to the contracting process as it does to internal operations. Since contracting authority is subject to the PSC's delegation of financial authority, it is incumbent on the contracting manager to ensure that security specifications are appropriate.

The PSC's contracting system requires managers to complete statements of work and contracting forms, and the system includes a mandatory field for the security screening level required. The intranet site contains a detailed contract guide to assist managers with contracting procedures. In addition, the contracting group asks managers questions with respect to where the contractor will be working and what information will be accessed to ensure that the level of screening is neither too low nor high and that any risks are considered. The majority of contracts require a "Reliability" level. No contracts are issued until the clearances have been verified by Security Services.

Interviews with managers confirmed their awareness of their responsibilities for defining contracting requirements, including security. Contractors do not comet on site until the clearance has been confirmed.

Conclusion

Contracts in PSC are the responsibility of the business manager, as is adherence to contract security guidelines. The audit concluded managers are aware of security requirements in contracting and they ensure the level of security required is adequate.

2.3.7 Breach Response

Finding

Effective security incident reporting is a key feedback mechanism, which together with incident investigation, allows important information to be gathered on security vulnerabilities that may predict future trends. Without a robust reporting and investigation system or an incident repository, management cannot take effective preventive or corrective action.

At HQ incidents are reported to the Commissionaires and/or Security Services. The Chief, Security Services makes the decision whether or not to investigate an incident and what corrective action to take. Major incidents are reported to senior management and investigated through appropriate channels, which can include the police.

In the regions, the individuals assigned security responsibility at each site are informed of any breaches. These individuals make the decision whether or not to investigate and what corrective action to take. Major incidents are brought to regional management for further action and are reported to Security Services who provide assistance if required. Investigations are taken to various levels, depending on the nature of incident. Security Services keeps a record of incidents/concerns and uses it to identify any trends.

Regions provide asset loss reports to Security Services, who ensure they are reported through the Public Accounts. Year-end security reports are submitted by regions to HQ and include a summary report of incidents. Null reports are also submitted. All sites indicated that there have been few incidents over the last few years.

We found that reported incidents were mostly loss of assets (e.g. theft). Verbal abuse and other security related events were not always seen as an incidents and were not necessarily reported.

Conclusion

The audit found that staff were aware of the procedures to follow and forms to use to report incidents. For the most part, the reporting of incidents is left up to the manager and staff involved. As part of the security awareness program, staff could be made aware of all types of incidents and the need to report and track them.

3.0 Management Response and Action Plan

Recommendations	Responsibility	Management Action Plan
1. It is recommended that the Vice President, Corporate Management Branch: • establish formal and regular communication mechanisms between regional and headquarters partners and among headquarter partners to facilitate the coordination and the implementation of security program components.	DG, FAD	Management supports this recommendation. The PSC is in the process of establishing a new Finance and Administration Committee with regional representation. This Committee will be chaired by a Vice-President and be comprised of Directors General. Given that security will be within the mandate of this Committee, this will provide an ideal vehicle for regular communication between headquarters and the regions with respect to security matters. Moreover, sub-committees of this group can be struck as required, to provide a greater focus on security. Care will be taken to ensure the terms of reference for this committee achieve these objectives. Target Date: Sept. 2004.
2. It is recommended that the Vice President, Corporate Management Branch: • establish a multi-year strategic plan for security (personnel, physical and information technology) and identify critical security priorities; and • establish an integrated, annual security plan with milestones, and monitor and review security deliverables on a periodic basis in conference with their administration, regional, program and information technology partners.	VP, CMB	Management supports this recommendation. To accomplish this, the PSC is working towards establishing an integrated corporate planning function, and corporate security planning will become an integral part of this broader process. The new Finance and Administration Committee will also play a important role in this regard. Target date: Nov. 2004

Recommendations	Responsibility	Management Action Plan
3. It is recommended that the Vice President, Corporate Management Branch: • ensure that a security education program for all employees, and a training plan for security staff, is formalized in the annual security plan to include metrics for effectiveness, efficiency and compliance; and	DG, HR	Management supports this recommendation. The new PSC learning plan will contain a number of mandatory training modules to ensure PSC staff are well equipped in all basic areas of management (e.g. finance, human resources, security). Essential security training will be included. Additionally, security issues will continue to be part of orientation for new employees. Further steps will be taken to ensure orientation training is taken by new employees and made a mandatory requirement.
• ensure that security sweeps are conducted on a regular basis.	DG, FAD	A program is currently being put in place to conduct ad hoc security sweeps. Target Date: Sept. 2004
4. It is recommended that the Vice President, Corporate Management Branch: • ensure a review of the security risk assessment process and initiate improvements to expand and broaden coverage to align with the PSC risk management framework.	VP, CMB DG, FAD DG, ITSD	Management supports this recommendation. CMB is currently undergoing significant transformation and reorganization and needs to adjust its business lines in order to support a smaller organization. The implementation of risk management will be one of the key techniques used to identify priority areas for targeted action. Our security program will be evaluated in this context in the future. Completing ongoing and periodic Threat and Risk Assessments in the informatics domain is a first priority. Target date: Sept. 2004

Recommendations	Responsibility	Management Action Plan
5. It is recommended that the Vice President, Corporate Management Branch: • pending finalization of government-wide standards, ensure that updated plans for all business operations at all sites are in place to provide for the continued availability of services and assets.	DG, FAD	TBS sent to Deputy Heads on April 6, 2004 the approved Operational Standard Business Continuity Planning (BCOS) which supplements the Government Security Policy. The Director General, Finance and Administration will begin work in this domain in the near future. The proposed action plan is as follows: - overview of BCOS to the Executive Management Committee (EMC) - establishment of a BCOS team with representation from ITSD/branch/rRegions - BCOS training for all team members - development of BCOS action plan/milestone/costs - approval of BCOS action plan by EMC - implementation - monitoring. Target date: Sept. 2004