Indian and Northern Affairs Canada

Internal Audit Report

Audit of the Security Program

Prepared by:

Audit and Assurance Services Branch

Project #09-79

May 2010

#3002822v1

Table of Contents

INITIALISMS AND ABBREVIATIONS

ARDG	Associate Regional Director General
BCP	Business Continuity Planning
DG	Director General
DDSM	Directive on Departmental Security Standard
DM	Deputy Minister
DRSO	Deputy Regional Security Officer
DSO	Departmental Security Officer
HRMC	Human Resources Management Committee
HRWS	Human Resources and Workplace Services
HRWSB	Human Resources and Workplace Services Branch
INAC	Indian and Northern Affairs Canada
ITSD	IT Security Division
NCR	National Capital Region
PGS	Policy on Government Security
RCM	Responsibility Centre Manager
RDG	Regional Director General
RSO	Regional Security Officer
SCDG	Security Classification and Designation Guide
SOHSD	Security and Occupational Health and Safety Division
SMF	Security Management Framework
SRCLs	Security Requirements Checklists
SSCA	Security Screening, Contracting and Awareness
SSC	Sector Security Coordinator
TB	Treasury Board
TRA	Threat and Risk Assessment

EXECUTIVE SUMMARY

Background

The most recent audit of the INAC security program was completed in 2005. A follow-up audit was included in the INAC Risk-based Audit Plan for 2010-2011, but was moved forward to 2009-2010 at the request of the Director General, Human Resources Workplace Services Branch (DG HRWSB) and Departmental Security Officer (DSO). It was generally agreed that advancing the timing of the audit was appropriate in light of the fact that the DSO is preparing to develop a plan to address the new requirements of the Treasury Board *Policy on Government Security* (PGS) which came into effect in July 2009.The new PGS emphasizes the need for departments to take a management-system approach to managing security, rather than the traditional strict compliance-based approach.

Significant progress has been made in the past two years in implementing an effective security program at INAC. The current DG HRWSB was appointed in 2007, and at that time also fulfilled the role of DSO. Shortly after her appointment, she identified underinvestment in the INAC security program and recognized a need for a dedicated full-time DSO. Thus, the Director SOHSD position was created and staffed in June 2008 and assigned the role of DSO. Since then, the DSO has worked to increase security awareness throughout the department, has initiated regular contact with regions and Regional Security Officers (RSOs). He has also received DM approval of a formal departmental security framework that is a more complete and comprehensive document than is commonly found in other social and cultural departments.

However, considerable work remains. Security reporting from regions to the DSO is incomplete and there is minimal DSO monitoring of regional security programs. RSOs, responsible for applying the PGS and departmental security procedures, are often fully occupied in their full-time, non-security regional positions. They generally do not have sufficient time to perform their security-related duties, and are not sufficiently accountable to the DSO. As a result, regional implementation of the security program is inconsistent and employee awareness of security policies and procedures is generally weak.

Objectives and Scope

The objective of the audit was to obtain assurance that: the Department's Security Program is compliant with the PGS; sufficient and appropriate resources are employed to support an efficient and effective security program, regionally and nationally; and recommendations resulting from the 2005 Audit of Security Program have been fully addressed and mitigating actions implemented.

The scope of the audit included all security functions, other than Business Continuity Planning (BCP) and IT Security, for a selection of four regions, one sector and headquarters security. The IT security and BCP functions of the Department were scoped out of the audit as they fall under the responsibility of the IT Security Division, and assurance work in these areas is planned (Audit of Business Continuity Planning) or has recently been conducted (Audit of Management of Information Technology Security).

Findings and Conclusions

Our audit found that INAC's Security Program needs improvement to meet requirements of the new *Policy on Government Security* (July 2009). Steady progress has been made in recent years in addressing recommendations of the 2005 Audit of the Security Program and in improving the breadth and effectiveness of HQ-led security activities; however significant gaps in the program remain. These weaknesses include unclear roles and responsibilities for regional and sector managers and security practitioners, low levels of security awareness amongst regional employees, inadequate information safeguarding controls, inefficient and inadequate security in contracting processes at headquarters, and insufficient monitoring and oversight of regional security programs by the DSO. Weaknesses observed are indicative of a lack of attention and resources being devoted to security by regions and sectors and the need for the DSO to refocus resources on areas of highest risk to better support regions and monitor the effectiveness of the security program.

More specifically, we found that:

- Security policy requirements and procedures outlined in the INAC Security Management Framework (SMF) are generally adequate and aligned to PGS requirements, although some work remains to ensure that policy-level roles and responsibilities are clear and operational standards are complete;

- Several key security functions prescribed in the SMF are not being performed equally by all RSOs, and as a result, regional implementation of the security program is inconsistent (i.e., some regions have implemented elements of a strong security program, while others have made little progress);

- Implementation of the security program in HQ sectors is poor. Sectors rely on SOHSD to provide all services related to the security program, and doing so has resulted in SOHSD having insufficient resources available to oversee the implementation of the broader security program and fully support RSOs in regions. Unlike regions, sectors do not have Security Officers with responsibility for supporting security program implementation;

- In keeping with the management-system approach to security, the new PGS requires that the Deputy Minister (DM) approve a departmental security plan. The DSO has undertaken to prepare such a plan in 2010-2011;

- The DSO began monitoring regional implementation of the security program in October 2009 by tracking the frequency of security incidents, awareness activities and compliance inspections, a positive and logical first step. As these are largely measures of output, the next step will be to increase focus on effectiveness of security activities and track mitigation of known gaps and risk exposures;

- Greater presence of the DSO is required in regions to guide and support RSOs and RDGs in improving their security programs and awareness of security requirements;

- Awareness of security related responsibilities among INAC employees in the regions and sector visited is generally weak, particularly as it relates to information safeguarding requirements – over the past year, the DSO has devoted considerable effort to security awareness in the HQ sectors, however limited effort has been devoted to regions;
- Controls for safeguarding information are not effective in ensuring that sensitive documents are properly identified, handled and secured in appropriate storage containers; and
- At the one sector included in the audit, controls are not effective in ensuring that contracts include appropriate security clauses and that contractors have requisite clearances prior to commencing duties.

Recommendations

Our audit report provides a number of recommendations intended to address the audit findings.

1. The DSO should update the departmental security policy to more clearly communicate the existing security related roles, responsibilities and accountabilities of the Departmental Security Officer, ADMs, RDGs, security practitioners, contracting staff, line managers and employees.
2. The DSO should further develop and communicate procedures and guidance to support implementation of the departmental security program in regions and sectors (e.g., procedures for lock-up at end of day, guidance on what to look for when conducting a security sweep, trainer's materials for delivering security awareness activities and guidance on how to establish and maintain physical security zones).
3. The ADMs responsible for regional staff and operations should work with the DSO to ensure that sufficient attention and resources are devoted to security in regions, including ensuring that RSOs have sufficient time to perform their security-related duties.
4. INAC should consider appointing Sector Security Officers in all sectors to support implementation of the security program, similar to the Regional Security Officer role. The responsibilities attached to this role and associated level of effort should be presented to INAC Senior Management when the departmental security policy is next updated.
5. The DSO should develop a strategically focused departmental security plan that outlines departmental security objectives and priorities, resource requirements, timelines for meeting baseline government security requirements, and plans for updating all required Threat and Risk Assessments (TRAs) over a five-year cycle.
6. The DSO should improve monitoring of the effectiveness of the security program in regions and sectors to support its continuous improvement (e.g. tracking implementation of recommendations from TRAs, performing random spot checks of security in contracting controls, tracking issues raised in security sweeps to ensure their timely resolution, and performing annual on-site visits to support security practitioners in regions and sectors).

7. The DSO should further develop the security awareness program to extend its reach to regional staff and improve coverage of information safeguarding and security in contracting requirements.

8. The DSO should increase focus on monitoring the effectiveness of security in contracting processes and reduce its direct involvement in the review of Security Requirements Checklists and contract clauses. To accomplish this, an organizational and functional review of the security in contracting function is required to ensure that sufficiently trained and competent contracting officers review and approve security requirements and security clauses. Furthermore, a comprehensive and effective security in contracting compliance monitoring and reporting program is required to ensure compliance is achieved and maintained across the department.

1. STATEMENT OF ASSURANCE

We have completed the Audit of INAC Security Program as managed by the Director General of Human Resources and Workplace Services Branch (HRWSB) and the Departmental Security Officer (DSO). The objective of the audit was to obtain assurance that:

- The Department's Security Program is compliant with the *Policy on Government Security* (PGS);
- Sufficient and appropriate resources are employed to support an efficient and effective security program, regionally and nationally; and
- Recommendations resulting from the 2005 Audit of Security Program have been fully addressed and mitigating actions implemented.

The audit was conducted in accordance with the requirements of the Treasury Board (TB) *Policy on Internal Audit* and followed the Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing.

The audit assessed the program controls against audit criteria developed from requirements outlined in the PGS, the *Directive on Departmental Security Management* (DDSM), the *Security Organization and Administration Standard*, the *Security and Contracting Management Standard*, and the *Operational Security Standard, Physical Security*.

In my professional judgment as Chief Audit and Evaluation Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on a comparison of the situations as they existed at the time of the audit and against the audit criteria. It should be noted that the conclusions are applicable only for the areas examined and the regions and sector visited.

2. INTRODUCTION

The most recent audit of the INAC security program was completed in 2005. A follow-up audit was included in the INAC Risk-based Audit Plan for 2010-2011, but was moved forward to 2009-2010 at the request of the DG HRWSB and DSO. It was generally agreed that advancing the timing of the audit was appropriate in light of the fact that the DSO is preparing to develop a plan to address the new requirements of the PGS which came into effect in July 2009.

2.1 Policy on Government Security

The INAC Security Program is governed by the PGS. This new policy replaced the *Government Security Policy (2002)* and the *Policy for Public Key Infrastructure Management in the Government of Canada (2004)*, and sets forth a list of baseline security requirements with which all departments must comply to support the safeguarding of employees and assets, and ensure the continuity of services. Specifically, the PGS requires that:

- Security management be an identifiable and integral element of departmental governance, programs and services;
- Departments adopt a systematic and consistent approach to the planning, operation and monitoring of security activities;
- Minimum controls are in place within departments to support interoperability and information exchange;
- Active management of threats, vulnerabilities and incidents support the delivery of services to Canadians and government operations; and
- Security management activities within a department do not increase risk to other departments or the government as a whole.

Included in the PGS is the requirement that Departments appoint a DSO to establish and direct a security program, and be responsible for ensuring the implementation of policy requirements and the coordination of all policy functions. A key change in the policy is a shift away from a prescriptive security compliance approach towards a management framework approach.

2.2 History of the Security Program at INAC

The 2005 Audit of the Security Program found considerable gaps in the INAC security program. Policies were outdated, roles and responsibilities were unclear, communication between headquarters and regions was poor, and the degree of implementation of the security program varied from region to region. Further, a formal security awareness program did not exist, employee security awareness was poor, particularly in regards to information safeguarding, and security staff did not perform periodic monitoring or validation of policy compliance in contracts.

The current DG HRWSB was appointed in 2007, and at that time also fulfilled the role of DSO. Shortly after her appointment, she identified underinvestment in the INAC security program and recognized a need for a dedicated full-time DSO. Consequently, the Director SOHSD position was created and staffed in June 2008 and assigned the role of DSO.

Once appointed, the new DSO set about addressing the outstanding findings of the 2005 audit and strengthening the security program by:

- Presenting of a security policy and security management framework to the DM for approval;
- Raising the visibility of the security function by proactively reaching out to senior management of regions and sectors;
- Providing leadership on regional implementation by engaging RSOs through formal and routine communications;
- Implementing a Sector Security Coordinator (SSC) pilot project in five sectors; and

- Significantly expanding security awareness activities at headquarters, particularly through increased awareness training sessions provided by DSO staff.

To further strengthen the departmental security program, the DG HRWSB has asked the DSO to prepare a strategic security plan to identify and prioritize security activities for the coming three to five years, and to investigate opportunities to further improve security training and awareness without adding resources to the security organization.

2.3 INAC Security Organization

At INAC, responsibility for security policy functions is divided between two organizational units:

- The Security and Occupational Health and Safety Division (SOHSD) of HRWSB; and
- The IT Security Division (ITSD) of CFO Sector, responsible for IT security and business continuity planning (BCP);

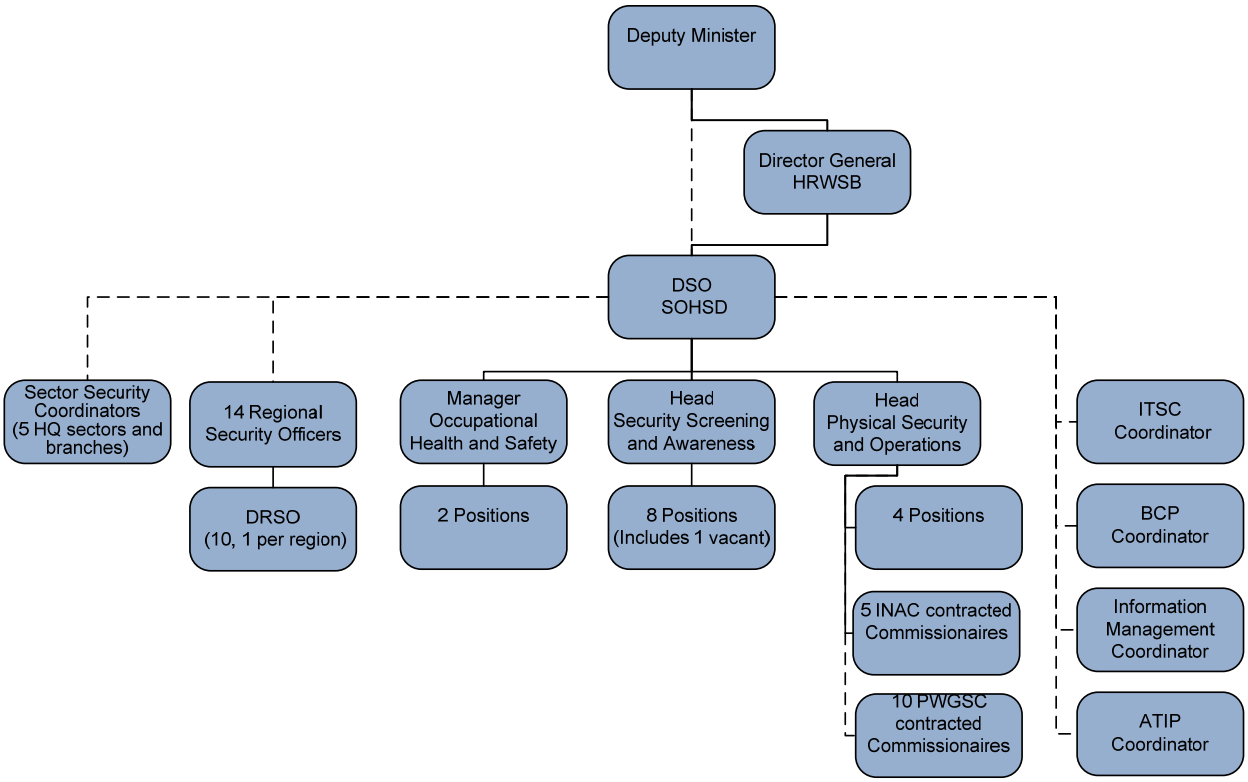
The Director, SOHSD is assigned the role of DSO, and has two units responsible for security functions, Security Screening, Contracting and Awareness, and Physical Security and Operations, and a third unit responsible for Occupational Health and Safety. The DSO reports functionally to the Deputy Minister (DM) for cause, although routine reporting is generally handled by the DG HRWSB. The Security Coordinator, ITSD has a functional reporting relationship to the DSO on security-related matters.

The Department also has other part-time security resources, Regional Security Officers (RSOs) and Deputy Regional Security Officers (DRSOs), assigned in the department's ten (10) regional offices, Adjudication Secretariat, and Indian Oil and Gas Sector. RSOs and DRSOs are responsible for delivery of security-related activities in regions, and the funding of their salaries and other costs is a regional responsibility. RSOs are generally employed within corporate services functions in INAC's regions and have other full-time roles. For any of their security-related responsibilities, RSOs are expected to report functionally to the DSO. INAC's Sectors, largely contained within the National Capital Region (NCR), are not required to appoint and fund security officers as SOHSD staff fulfill these roles.

At the DSO's recommendation, five sectors have recently appointed Sector Security Coordinators (SSCs) as a pilot project to assist with security activities in their sectors. Thus far, SSCs have assumed little to no involvement in the implementation of the security program, acting solely as a liaison between SOHSD staff and the sector. SOHSD staff remain responsible for providing all security-related services to HQ sectors.

The INAC security organization is depicted in Figure 1. Functional relationships are represented by dotted lines.

Figure 1 – INAC's Security Organization



3. Audit Objectives and Scope

The objectives of the audit were to provide assurance that:

- The Department's Security Program is in compliance with the PGS;
- Sufficient and appropriate resources are employed to support an efficient and effective security program, regionally and nationally; and
- Recommendations resulting from the 2005 Audit of Security Program have been fully addressed and mitigating actions implemented.

The audit examined the adequacy (design), efficiency and effectiveness of the Department's Security Program and management controls intended to provide assurance that INAC is in compliance with the PGS, and that key security issues are identified and communicated for timely and appropriate decision-making.

Audit work included an assessment of the Security Program's capacity to deliver a security program in compliance with applicable legislation, the security function's organizational

structure, including governance frameworks and roles and responsibilities, from both a regional and national perspective.

The scope of the audit included all security functions, other than BCP and IT Security, at a selection of regions and one sector. The IT security and BCP functions of the Department were scoped out of the audit, with the exception of their governance framework and linkages to the Security Program. This is because they fall under the responsibility of the IT Security Division, and assurance work in these areas is planned (Audit of Business Continuity Planning) or has recently been conducted (Audit of Management of Information Technology Security).

4. Approach and Methodology

Our audit was led by Orbis Risk Consulting and conducted in accordance with the requirements of the TB *Policy on Internal Audit* and followed the Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing. Sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinions provided and contained in this report.

Audit criteria were developed from requirements outlined in the PGS, the DDSM, the Security Organization and Administration Standard, Security and Contracting Management Standard, and the Operational Security Standard, Physical Security. These criteria served as the basis for developing the audit approach and detailed audit program for the conduct phase.

During the planning phase, interviews were conducted with security personnel at INAC headquarters, and with RSOs from five regional offices. Program documentation was also reviewed and analyzed. This work was performed in support of the preliminary risk assessment process. The first step in the process identified the significance of each control activity (in relation to each audit criteria), considering both the level of resources assigned to the activity and its importance in supporting an effective control system. The second step assessed the level of residual risk associated with each control activity. A risk score was then assigned to each control activity and used to confirm its inclusion in the audit and determine the audit procedures to be performed in the conduct phase. The planning and risk assessment phase concluded with the completion of a detailed risk assessment, audit strategy, and audit program.

The conduct phase of the audit included the completion of audit procedures at regional and sector offices, as well as at SOHSD. Specifically, Yukon, Alberta, Ontario (Toronto and Thunder Bay), and Quebec regional offices were visited, as were the Treaties and Aboriginal Government Sector offices located in the NCR. The selection of four regions and one sector included consideration of the size of the organization, scope of activities and maturity of security programs. Our audit only provides assurance on the adequacy and effectiveness of controls for the regions and sector included in scope and for the responsibilities of SOHSD.

The principal audit procedures completed by the audit team included:

- *Documentation Review and Analysis* – Documentation was reviewed to assess whether the security program was implemented in accordance with the requirements of the PGS. Documentation reviewed included, but was not limited to: policy and program authorities;

departmental security policies, procedures, standards and directives; security awareness documentation and records of attendance; security classification and designation guides; managers security handbook; RSO terms of reference; security training plans, courseware, and records of attendance; committee minutes; security incident and investigation reports; threat and risk assessments (TRAs); reports on security activities and operations including sweeps and inspections; job descriptions for select security-related positions; organization charts; and Memoranda of Understanding, service-level agreements, and contracts for the provision of security-related services.

- *Transactional Review* – A sample of transactions were reviewed for the regions and sector visited to ascertain that:
    - Personnel security clearances were granted prior to the employee's commencement of duties, clearances requirements were commensurate with the nature of the position, and employees were provided with a security briefing by a security practitioner;
    - Security Requirement Checklists (SRCLs) were completed for contracts with security requirements, security requirements identified in SRCLs appeared reasonable, and security requirements were included as contractual clauses; and
    - Combinations to secure storage containers were changed in accordance with policy requirements, and that individuals with knowledge of the combinations met all requirements for accessing the information contained within.
- *Analysis of Resource Capacity* – A review of the security organization was performed to assess the level of resources devoted to the security function relative to that of similar departments. An assessment of resource competencies was also performed to assess if appropriate and sufficient resources have been applied to the security function.
- *Observation of Task Performance* – Walkthroughs were conducted at each of the regions and sector visited to verify the extent to which key physical security controls were implemented in facilities in accordance with requirements and policy. Walkthroughs also included questioning of employees to assess the extent to which they understood their security-related obligations.
- *Interviews* – Interviews were conducted with management and staff at SOHSD and at the regions and sector visited. Interview guides were developed for the interviews conducted, taking into consideration the objective of the audit and the audit criteria.
- *Survey* – A survey of INAC employees to assess their general awareness of security policies, procedures and activities was planned but not conducted, as it was determined that sufficient audit evidence was obtained during interviews and walkthroughs.

Audit fieldwork was conducted between January 2010 and March 2010.

5. CONCLUSIONS

Our audit found that INAC's Security Program requires improvement to meet requirements of the new PGS (July 2009). Although steady progress has been made in recent years in

addressing recommendations of the 2005 Audit of the Security Program and in improving the breadth and effectiveness of HQ-led security activities, significant gaps in the program remain. These weaknesses include unclear roles and responsibilities for regional and sector managers and security practitioners, low levels of security awareness amongst regional employees, inadequate information safeguarding controls at HQ and in regions, inefficient and inadequate security in contracting processes, and insufficient monitoring and oversight of regional security programs by the DSO. Weaknesses observed are indicative of a lack of attention and resources being devoted to security by regions and sectors and the need for the DSO to refocus resources on areas of highest risk to better support regions and monitor effectiveness of the security program.

6. OBSERVATIONS AND RECOMMENDATIONS

The observations of our audit are provided in three sub-sections. The first addresses audit observations at the program level, including program design, implementation and monitoring. The second addresses specific audit observations related to compliance with the PGS, including security awareness, information safeguarding, protection of employees and assets, personnel screening, security in contracting and administrative investigations. The third address INAC's compliance with recommendations from 2005 Audit of the Security Program.

6.1 Security Management Program

6.1.1 Security Management Framework

Security policy requirements and procedures outlined in the INAC Security Management Framework (SMF) are generally adequate and aligned to PGS requirements, although some work remains to ensure that policy-level roles and responsibilities are clear and that operational standards are complete.

The PGS makes deputy heads responsible for establishing a security program for the co-ordination and management of departmental security activities. This security program must include a governance structure with clear accountabilities and have defined objectives that are aligned with departmental and government-wide policies, priorities and plans.

2005 Audit Key Findings

- Security accountabilities need clarification.
- The INAC security manual has not kept pace with government-wide policy changes.
- There are gaps in departmental security policy and incident reporting procedures.

INAC's SMF was approved by the DM in June 2008, establishing the department's security policy objectives, roles, responsibilities and accountabilities, and monitoring framework. Our audit found the SMF and policy requirements contained within to be generally adequate as a high-level security document, and well aligned to PGS requirements and departmental objectives, priorities and plans. INAC's SMF is a more complete and comprehensive document than is commonly found in other social and cultural departments.

However, our audit found that the roles and responsibilities of INAC managers, staff, RSOs, and Sector Security Coordinators are not clearly understood or defined in the actual INAC Security Policy. In essence, employees find the SMF document to be a confusing mix of policies, standards and procedures.

Under the direction of the new DSO, SOHSD staff and some regions have made good progress in the past two years developing and communicating security procedures. However, additional work is required to ensure that all directives, standards and procedures are complete and disseminated throughout the organization, particularly as they relate to lock-up at end of day (clean-desk), guidance on what to look for when conducting a security sweep, trainer's materials for delivering security awareness activities and the establishment and maintenance of physical security zones.

Recommendations:

1. The DSO should update the departmental security policy to more clearly communicate the existing security related roles, responsibilities and accountabilities of the Departmental Security Officer, ADMs, RDGs, security practitioners, contracting staff, line managers and employees.

2. The DSO should further develop and communicate procedures and guidance to support implementation of the departmental security program in regions and sectors (e.g., procedures for lock-up at end of day, guidance on what to look for when conducting a security sweep, trainer's materials for delivering security awareness activities and guidance on how to establish and maintain physical security zones).

6.1.2 DSO and the Security Organization

The DSO is appropriately positioned within the organization to fulfill all security responsibilities and sufficient mechanisms exist to ensure that senior executives are kept apprised of security matters. However, our audit found that regions are not sufficiently accountable to the DSO for implementing regional security programs and sectors have not appointed Security Officers to support their security-related obligations.

The PGS stipulates that the DSO be functionally responsible to the deputy head or to the departmental executive committee to manage the departmental security program. Our audit found the DSO to be appropriately positioned within the organization to fulfill all security responsibilities and to provide security advice to the organization. Senior executive is kept apprised of security matters through frequent reporting by the DSO to the Human Resources Management Committee (HRMC). The DSO also reports directly to the Deputy Minister on an as-required basis, while Reporting to the DM on routine matters is generally handled by the DG HRWSB.

At INAC, responsibility for security policy functions is divided between two units: The ITSD, responsible for IT security and BCP; and SOHSD, whose Director is appointed as the DSO. SOHSD has two units responsible for security functions (Security Screening, Contracting and Awareness, and Physical Security and Operations), and a third responsible for Occupational Health and Safety. The Security Coordinator, ITSD has a functional reporting relationship to the DSO on all security-related matters. The DSO has a direct line reporting relationship to the DG HRWSB, who also serves as his Deputy Departmental Security Officer.

2005 Audit Key Findings

- Communication between headquarters and regions is lacking because there is no effective framework for it.
- Implementation of departmental security standards is often inconsistent.
- There is no central training budget for all security staff, and training budgets do not adequately reflect training requirements.

Although common in other government departments, this division of security responsibilities adds complexity to the management of the security program, as security efforts must be coordinated between two groups. Strong and routine communication is required between the two divisions to ensure the successful implementation of the security program. Our audit did not include an assessment of IT security and business continuity planning controls but did look at governance and communication between these functions and the DSO. The audit found that effective communication is being achieved through the Departmental Security Committee, whose mandate is to provide advice, guidance, and recommendations concerning departmental security and to ensure that the departmental Executive Committee is appropriately engaged on the management of security in the department. The Departmental Security Committee is chaired by the DSO, meets monthly, and has a membership that ensures adequate coverage of the security organization to facilitate the implementation of the security program.

Regional Security Officers (RSOs)

Supporting the DSO in implementing the security program in regions are RSOs and DRSOs, who are funded by regions, and have full-time positions outside of the security organization, generally within regional corporate services functions. While functionally responsible to the DSO, RSOs are primarily accountable to the regional management team. Consequently, security matters are generally handled on a reactive basis when workload permits or when urgent issues arise. Our audit found that the DSO does not have sufficient influence over the level of effort devoted to the security program in regions. Several key security functions prescribed in the SMF are not being performed equally by all RSOs, and as a result, regional implementation of the security program is inconsistent (i.e., some regions have implemented elements of a strong security program, while others have made little progress). Examples of security functions that are performed satisfactorily in some regions, but poorly in others, include: security awareness activities; conduct of monthly security sweeps; reporting on security program implementation to the DSO; control over keys and combinations for secured storage containers; and other preventive security activities.

Security Implementation in Sectors

Implementation of the security program in sectors is weak. We believe this stems from: Sectors not having sufficient focus on security; Sectors not having appointed Security Officers who perform duties similar to RSOs in regions; and SOHSD having been too preoccupied with implementing sector security activities to provide appropriate oversight and advice to ADMs. Although some sectors have appointed Sector Security Coordinators, their roles have not been defined and their involvement in the implementation of the security program has been minimal.

The absence of Sector Security Officers has also adversely affected the departmental security program, as a significant portion of the corporate security function's resources have been devoted to performing these duties. This has left SOHSD with insufficient time to develop and oversee the implementation of the security program, and to provide support to regions and sectors.

Best practice among government departments is for all organizational units to appoint Security Officers, consistent with the security principle of centralized control and decentralized execution.

Training of Security Practitioners

Our audit found that resources devoted to training security practitioners are insufficient and that the DSO lacks a process to formally assess security-related training needs of RSOs so that individual training plans can be developed.

The DSO has a $5,000 budget to meet training needs of 15 staff, at an average of less than $350 per staff member. While security training provided by INAC was deemed insufficient, two thirds of DSO staff interviewed reported having received adequate training at other departments prior to joining INAC, and thus felt sufficiently trained to perform their duties to the required level. In contrast, our audit found that two thirds of the regional security practitioners were not sufficiently trained to perform their duties to the required level. The DSO, aware of this shortcoming, is addressing the issue by conducting an annual week-long RSO training session at headquarters in March of each year, holding monthly conference calls with RSOs to improve communications and improve guidance on security-related duties, and offering RCMP training courses free of charge.

Security Organization Resources

The new PGS requires annual planning to establish goals and allocate resources based on the unique needs of each department. Our audit included a review of the reasonableness of resources currently assigned to the INAC security program. In performing this review, we analyzed the resources and levels of security personnel in other departments with comparable programming and security needs. Our audit was unable to reach an audit conclusion on the adequacy of resources due to the lack of benchmarking information and the fact that many other departments are not yet in compliance with the requirements of the PGS.

Although we are not able to provide an audit conclusion on the adequacy of resources, our review has identified some areas requiring management attention, including:

- SOHSD resources are dedicated to reviewing all SRCLs with security requirements and contract security clauses to compensate for inadequate contracting security controls within CFO Sector, sectors and regions;
- Inadequate training and reference materials for departmental contracting staff on security in contracting requirements;
- Inadequate training available to security practitioners;
- Underinvestment in security resources in sectors; and
- Underinvestment in some regions in the role of RSO.

Recommendations:

3. The ADMs responsible for regional staff and operations should work with the DSO to ensure that sufficient attention and resources are devoted to security in regions, including ensuring that RSOs have sufficient time to perform their security-related duties.

4. INAC should consider appointing Sector Security Officers in all sectors to support implementation of the security program, similar to the Regional Security Officer role. The responsibilities attached to this role and associated level of effort should be presented to INAC Senior Management when the departmental security policy is next updated.

6.1.3 Security Planning

A formal departmental security plan does not exist, but is planned for 2010-2011.

The new PGS requires that the Deputy Minister approve a departmental security plan that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security and supporting its implementation. Given that this requirement only came into effect in July 2009, INAC does not yet have a formal departmental security plan.

The DSO reports on departmental security matters at HRMC and maintains a quarterly plan of DSO priorities and activities that is reported to the DG HRWSB. This plan does not sufficiently address regional security program gaps. The Departmental Security Committee's mandate includes ensuring that security is integrated into the department's strategic planning process. However, overall monitoring of the implementation of the security program in regions is minimal, with little in the way of performance

2005 Audit Key Findings

- Security planning is limited to an annual work plan established by headquarters security for Security and Emergency Measures Division staff, and a national report on security activity that projects this activity into the future.
- Some regions do not participate fully; therefore the completeness of the annual national report is suspect.
- INAC's policy and planning framework were deemed to be ineffective.

measurements to assess program effectiveness (discussed in section 6.1.4). Systemic security risks are not being identified at the departmental level, and current informal planning does not consider the whole of the security program.

At a regional level, security risks are addressed on an ad-hoc basis. RSOs report on emerging security risks to Regional Operations Committees as issues arise, and regional managers are generally responsive to items requiring immediate attention. However, security risks are generally not formally prioritized, nor are annual security plans prepared for or by regions.

The DSO and DG HRWSB have committed to preparing a formal security plan in 2010-2011, and intend to base the plan on the findings from this audit.

Recommendation:

5. The DSO should develop a strategically-focused departmental security plan that outlines departmental security objectives and priorities, resource requirements, timelines for meeting baseline government security requirements, and plans for updating all required Threat and Risk Assessments (TRAs) over a five-year cycle.

6.1.4 Monitoring of the Security Program

The DSO has developed performance measures to monitor levels of security activities in regions. Improvement is required to monitor the effectiveness of the security program in regions and sectors to support continuous improvement (e.g. tracking implementation of recommendations from TRAs, performing random spot checks of security in contracting controls, tracking issues raised in security sweeps to ensure their timely resolution, and performing annual on-site visits to support security practitioners in regions and sectors).

The PGS requires that periodic reviews be conducted to assess whether the departmental security program is effective, whether the goals, strategic objectives and control objectives detailed in the departmental security plan are being achieved, and whether the departmental security plan remains appropriate to the needs of the department and the government as a whole.

2005 Audit Key Findings

- There is no central authority to review the security impact of change actions for accommodations, which makes it difficult to assess INAC's exposure from an overall facilities' security risk.

In October 2009, the DSO began monitoring the regional implementation of the security program by tracking the frequency of security incidents, awareness activities and compliance inspections in regions and sectors. This represents a positive and logical first step in establishing a monitoring and oversight regime. As these are largely measures of output and not sufficient to meet PGS requirements for monitoring the program, the next step will be to refine measures to focus on assessing the effectiveness of the security program.

Current monitoring activities performed by the DSO include:

- Identification of TRAs completed in regions and sectors – next step will be to track findings and recommendations from TRAs to ensure that they are addressed;
- Reviewing all SRCLs for professional services contracts and security clauses in contracts prior to contract signing;
- Performing spot checks on SRCLs and contracts to verify if security requirements were properly identified, contractor clearances were performed, and the required contractual clauses included. Due to workload pressures, the only spot check thus far was performed in November 2009. In the future, SOHSD intends to conduct them monthly;
- Monitoring the screening of individuals to ensure that security clearances are in place before a letter of offer is issued;
- Collecting Security Incident Reports for all incidents disclosed in the department (started in April 2009); and
- Directing RSOs to conduct monthly security sweeps. Our audit found that sweeps are not being conducted in all regions and that DSO staff are not tracking identified gaps and monitoring to ensure effective resolution. RSOs generally reported having insufficient time to conduct monthly sweeps.

The DSO has personally met with most senior managers of regions and sectors and occasionally travels to regions to discuss security matters. This management-level interaction is important. Additional on-site visits from SOHSD staff would be very beneficial to support RSOs in identifying security risks and gaps in their regional security programs.

Recommendation:

6. The DSO should improve monitoring of the effectiveness of the security program in regions and sectors to support its continuous improvement (e.g. tracking implementation of recommendations from TRAs, performing random spot checks of security in contracting controls, tracking issues raised in security sweeps to ensure their timely resolution, and performing annual on-site visits to support security practitioners in regions and sectors).

6.2 Compliance with Policy on Government Security

Our audit also examined compliance with specific sections of the PGS, including security awareness, information safeguarding, protection of employees and assets, personnel screening, security in contracting, and administrative investigations.

6.2.1 Security Awareness

The DSO has developed security awareness materials and has begun rolling out activities within the NCR, yet awareness of security related responsibilities among INAC employees remains weak, particularly as it relates to information safeguarding.

Awareness levels in regions visited ranged from very poor to satisfactory, and was largely a function of activities initiated by regions. Regions visited were not utilizing the awareness materials prepared by SOHSD to provide formal security awareness sessions to employees.

The objective of a security awareness program is to focus the attention of employees on maintaining the confidentiality, integrity, and availability of information assets and to encourage compliance with all security policies, standards and procedures. An effective awareness program is critical to the success of any departmental security program.

2005 Audit Key Findings

- Although communication efforts are evident, a formal security training and awareness program does not exist.
- The inadequacy of security training and awareness is exhibited by a lack of pervasive knowledge of security within INAC.
- There is no mandatory orientation program for new employees that includes security.

The DSO has made some progress over the past two years in improving security awareness levels of employees in HQ by significantly increasing the frequency of formal security awareness sessions in the NCR and by bolstering other aspects of the security program (e.g., security awareness week, posters, and periodic email / INAC Express reminders). The same cannot be said for regional staff where very little has been undertaken. Although these are important and positive improvements, it was evident during interviews and site walkthroughs that the majority of employees remain unaware of many of their security-related responsibilities, and that sustained effort is required to improve security awareness levels.

A total of 56 security awareness sessions were offered in the NCR in 2009-2010, and attended by 1,029 employees. In contrast, the audit did not find evidence of similar awareness presentations being provided to employees in any of the regions visited, although RSOs did report providing a brief 5-10 minute session for new employees. In November 2009, the DSO distributed a security awareness presentation to RSOs with the instruction that it could be customized for delivery in their region. RSOs reported not having sufficient time to customize and deliver the training sessions to regional staff. Further, while new employees are provided with a brief introduction to security as a part of the INAC orientation program, a review of the documentation from these sessions indicated that only a cursory overview of document classification and categorization procedures was covered. Thus, new employee security awareness training is neither comprehensive nor sufficient.

Finally, the audit found that attendance at awareness sessions is not mandatory, thus mechanisms do not exist to ensure that all employees receive sufficient security awareness training on a regular and ongoing basis.

Recommendation:

7. The DSO should further develop the security awareness program to extend its reach to regional staff and improve coverage of information safeguarding and security in contracting requirements.

6.2.2 Information Safeguarding

Information safeguarding policies and procedures are not consistently implemented throughout the department, and employee awareness of information safeguarding requirements is generally poor.

A key requirement of the PGS is that information, assets and services be safeguarded from compromise. The DSO has prescribed security measures and processes in the SMF and the Security Classification and Designation Guide (SCDG) to ensure the proper safeguarding of information. However, these policies and procedures are not consistently implemented throughout the department due to: documented guidance being fragmented, incomplete, and insufficiently prescriptive; poor employee security awareness; and insufficient oversight by the DSO.

2005 Audit Key Findings

- Document designation, classification and control is a problem within the department.
- Employees do not understand document classification procedures and its implementation is inconsistent across the department.

Documented guidance is fragmented and incomplete with information safeguarding policies and procedures spread across the SMF, SCDG, and a two-page SCDG summary poster, as well as other Government of Canada security policy and procedure documents. Portions of the SMF relating to information safeguarding are incomplete, and reference other policies and procedures, adding complexity for users who are not familiar with their security obligations. For example, the SCDG poster most often referenced by employees prescribes that PROTECTED B information be stored in an approved security container with approved combination padlock in operational zones. No description of what constitutes an approved security container or approved combination padlock is provided. The SMF is also incomplete in this area, as it includes a placeholder which notes that an appendix on Security of Information will be inserted at a future point. The audit found that the majority of RSOs were unaware of what constituted an approved storage container or combination padlock, and the audit found inappropriate storage containers in use in all regions and the one sector visited.

Poor observation of clean desk policies was identified as a concern in all regions and the one sector visited. PROTECTED A and PROTECTED B information was commonly found unsecured on both unattended and vacant desks, in unlocked storage containers, or in boxes left on the floor in operational and public zones. In one site visited, SECRET documentation was found in unlocked cabinets temporarily stored in hallways, on bookshelves in operational zones, and on unattended desks. In two regions, employee HR files (PROTECTED A and PROTECTED B) were stored in cabinets in high-traffic walk-through areas. Although the types

of cabinets in use were appropriate, they were left unlocked and unmonitored during the day, allowing for easy and unnoticed access by any passerby. In both instances, RSOs and managers were unaware of the inappropriateness of these storage locations.

No standards are prescribed in the SMF or elsewhere on how to transport, transmit or destroy sensitive information, and a general lack of awareness was observed amongst employees. Inappropriate shredders, storage containers for third-party shredding, or disposal procedures were observed at all sites visited, and RSOs were unaware of this non-compliance.

The audit also found there to be generally poor key control and poor combination management practices in the regions and sector visited. Records of changes in storage container keys and combinations were not kept at any of the sites visited, and only one site reported appropriately changing keys and combinations as required. Finally, we found that individuals with knowledge of combinations or who were provided with keys for secure storage containers were generally appropriately screened and authorized to access the information.

A specific recommendation is not provided for the findings identified in this section as they are addressed by recommendations 1 through 7.

6.2.3 Physical Security - Protection of Employees and Assets

Physical security controls were generally adequate in all regions and the one sector included in the scope of our audit.

2005 Audit Key Findings

- General physical security varies from site-to-site. A standardized approach to implement physical security across the department would improve results.
- Not all systems and at-risk areas have had TRAs prepared, and those that have been conducted have not been kept up-to-date. Better central guidance for the TRA process is required.

The PGS defines baseline physical security requirements to counter threats to government employees, assets and service delivery and to provide consistent safeguarding for the Government of Canada. The audit team performed walkthroughs at each of the regions and sector visited to assess compliance with this standard. While physical security practices varied from region to region, overall it was found that appropriate and generally adequate physical security controls were in place.

At all sites visited, employees felt safe, emergency measures were in place and practiced, and proper zoning procedures and access controls were generally implemented, with some minor exceptions noted. Although non-compliant practices or controls were noted in all regions visited, none were indicative of systemic problems. Exceptions were generally one-offs, resulting from employees circumventing existing policies and procedures, such as a failure to wear identification passes in a visible manner; the inappropriate storage of keys to secure storage containers; and doors to operational zones from public areas being left open or unlocked. These infractions were more indicative of a weak security awareness program and a lack of oversight by RSOs, than inadequate policies or procedures.

All regions visited had recently performed TRAs in support of the Secure Card of Indian Status (SCIS) project, covering the primary offices in each region. However, TRAs did not exist for all assets and operations in the sites visited, and as a result, DSO staff are unable to fully assess the appropriateness of implemented security safeguards. A review of all available TRAs found that current TRAs were not available for nearly half of all INAC buildings. As prescribed in the SMF, TRAs must be conducted for all assets and operations and be kept current annually. Government security standards require that TRAs be completed or updated for all assets and operations at least once every five years.

A specific recommendation is not provided for the findings identified in this section as they are indirectly addressed through recommendation 5 (prioritized completion of TRAs) and recommendation 7 (improved security awareness program).

6.2.4 Personnel Screening

Our audit found that security screening of employees is consistently performed prior to the commencement of duties. However, RSOs are not providing employees with proper security briefings when security clearances are granted or when their duties change.

The PGS requires that all individuals who will have access to government information and assets be security screened at the appropriate level prior to the commencement of their duties. This process usually involves reference inquiries, verification of qualifications, criminal records checks and, as required, credit checks. At INAC, security screening for employees and contractors is performed centrally by SOHSD. RSOs are responsible for submitting screening requests to SOHSD, and for coordinating the collection of information at the regional level.

2005 Audit Key Findings

- Instances were found of regional staff beginning duties prior to receipt of official clearance.
- No reconciliation has been attempted to determine if staff have been cleared appropriately, or if positions have been appropriately classified.

The audit team was advised by security staff that, in the past, some individuals began their duties without a proper screening in place. In 2009, the DSO implemented a process requiring that a security screening be in place before a letter of offer could be issued. As a part of this process, the HR department was provided with access to the security screening system to ensure that security clearances have been granted prior to issuing letters of offer. The audit found this new process to be functioning effectively.

The second element considered in the audit was whether the designated security levels of positions were appropriate for the nature of work and information handled. Overall, security levels were appropriate. However, at one site visited, multiple instances were found where the designated security level of positions was insufficient given the nature of the information and assets requiring protection. In these instances, the personnel in the position were screened to the appropriate higher level, or managers were aware of the shortcoming and were in the process of obtaining proper clearance for the individual.

The third element assessed was whether RSOs provided security briefings to employees at the time they were granted their clearance. Security clearance forms require that the employee and a security professional both sign confirming that a briefing has been provided. The audit found that all briefing forms were properly signed; however, interviews and site walkthroughs indicated that many employees had not received these formal briefings and simply been asked to sign the form.

A specific recommendation is not provided for the findings identified in this section as they are indirectly addressed through recommendation 3 (strategy to ensure sufficient investment in regional security programs) and recommendation 7 (improved security awareness).

6.2.5 Security in Contracting

The process for identifying contract security requirements at INAC headquarters is inadequate, ineffective and inefficient.

2005 Audit Key Findings

- Security staff does not engage in periodic monitoring or validation of security policy compliance in contracts.

Our audit found that controls at all four regions visited were effective in ensuring that SRCLs were properly completed and contract security clauses were appropriate. Our audit only covered one sector in headquarters, and therefore we cannot draw conclusions on the adequacy and effectiveness of controls at all sectors. At the one sector visited, we concluded that Responsibility Centre Managers (RCMs) and sector contracting administrators are not adequately trained to use SRCLs to properly identify security requirements.

Significant non-compliance was identified at the one sector visited, where a large proportion of contracts are for professional services. Our audit found that 23 of 25 contracts reviewed had security related requirements, but only 3 of these 23 contracts were accompanied by properly completed SRCLs. Additionally, only 6 of 23 contracts requiring security clauses had clauses that were appropriate for the work being performed.

To date, SOHSD had dedicated two full-time resources and one part-time resource to reviewing Security Requirements Checklists (SRCLs) and developing contract clauses. SOHSD informed us that, in 2009-2010, only 10% of all contracts (400 of approx 4,000) were being routed through them. It is expected that this workload will double or triple in 2010-2011 if a planned process change is implemented to ensure that all SRCLs with security requirements are routed through SOHSD.

At INAC, Responsibility Centre Managers (RCMs) are required to identify when a proposed contract has security requirements and complete an SRCL. Completed SRCLs are generally reviewed for completeness and accuracy by region and sector security staff and/or contracting staff. RCMs are then required to forward SRCLs directly to SOHSD for approval, before being sent to contracting. With this process, a large portion of contracts (mainly low-dollar value contracts) that should include security clauses are not being proactively directed to SOHSD by RCMs and do not contain appropriate security clauses. If this planned process change is

implemented, SRCLs would be sent directly to CFO Sector Contracting Officers with contract requests and then routed to SOHSD for review and approval.

When SRCLs arrive at SOHSD, they are reviewed by a Security Officer who also develops security clauses for the contract. Prior to being sent back to the Contracting Officer, all SRCLs and security contract clauses are reviewed and signed-off by the Head, Security Screening, Contracting and Awareness (Head SSCA), and SOHSD processes any required contractor security screening.

Although an improvement in terms of security-related compliance, we believe that this new process would continue to be inadequate, ineffective and inefficient. More specifically, we believe that:

- Considerable delays in the contracting process are likely to result as SOHSD's two Security Officers attempt to adjust to reviewing much higher volumes of SRCLs;
- Low-dollar value (LDV) contracts will likely continue to bypass the security function entirely, the most significant concern identified in our audit testing;
- SOHSD will have less time to provide awareness training to the RCMs and contracting personnel in sectors who are already inadequately trained and equipped to identify when security requirements exist and complete SRCLs;
- SOHSD Security Officers will have less time available to perform spot checks of contracts that have not been identified as containing security requirements; and
- The Head SSCA will be fully occupied with the routine administrative duties of reviewing and signing relatively uncomplicated SRCLs and have little to no time to devote to security screening and security awareness responsibilities; and
- It is not efficient or necessary to have the corporate security organization performing review and approval of all SRCLs with security requirements – in almost all government departments, this function is performed by security-trained contracting officers who are co-located with the contracting function and have a functional reporting relationship to the DSO.

To improve the efficiency of the contracting process, other government departments that have high volumes of contracts have developed standardized pre-populated SRCLs and accompanying contract clauses. A decision tree is prepared to guide RCMs in identifying when a standard SRCL and security clause can be employed and when input is required from security practitioners. In addition to driving efficiency, this process can reduce errors and improve the speed of the contracting process.

Recommendation:

8. The DSO should increase focus on monitoring the effectiveness of security in contracting processes and reduce its direct involvement in the review of Security Requirements Checklists and contract clauses. To accomplish this, an organizational and functional review of the security in contracting function is required to ensure that sufficiently trained and competent contracting officers review and approve security requirements and security clauses. Furthermore, a comprehensive and effective security in contracting compliance monitoring and reporting program is required to ensure compliance is achieved and maintained across the department.

6.2.6 Administrative Investigations

Administrative investigations are generally conducted in accordance with the requirements of the PGS, although some exceptions were noted.

The conduct of administrative investigations is an important component of security monitoring and oversight and serves to identify risk exposures so that safeguards can be amended accordingly. The audit found that administrative investigations are generally conducted in accordance with the requirements of the PGS.

2005 Audit Key Findings

- Security incidents were often informally reported and investigated with little result.
- Security incidents are often not reported to the DSO until an incident proves to be more serious than originally thought and the impact becomes greater.

Complex administrative investigations at SOHSD are contracted to appropriately qualified third-party investigators and are conducted in accordance with the requirements of the PGS. Routine and less complex investigations are handled by DSO and regional staff, and were found to not always have been conducted in accordance with the requirements of the PGS. While DSO staff are sufficiently equipped to handle these types of investigations, not all RSOs are adequately trained to do so. As a result, not all RSOs maintain proper records of investigations conducted, or provide complete reporting on these investigations to the DSO. Further, it was found that “minor” incidents (theft of personal property, visitors escorted without visitor passes) occasionally go unreported by employees. Greater awareness of security practices is required among employees to ensure that all security incidents are reported so that they may be properly investigated.

Issues regarding administrative investigations will be addressed through improved training programs for RSOs to result from ensuring sufficient investment is allocated security in regions (Recommendation 3).

6.3 Progress in Addressing the Recommendations of the 2005 Audit of the Security Program

Steady progress has been made in recent years in addressing recommendations of the 2005 Audit of the Security Program and in improving the breadth and effectiveness of HQ-led security activities; however, significant gaps in the program remain. These weaknesses include unclear roles and responsibilities for regional and sector managers and security practitioners, low levels of security awareness amongst regional employees, inadequate information safeguarding controls, inefficient and inadequate security in contracting processes at headquarters, and insufficient monitoring and oversight of regional security programs by the DSO.

Detailed accounts of steps taken to address the 2005 recommendations follow.

2005 Recommendation:

1. It is recommended that the Departmental Security Officer, in consultation with other departmental areas at headquarters and within the regions, review, define and assign/implement operational and functional roles and responsibilities related to all areas of security, including but not limited to: physical security, information/assets security, personnel security, Information Technology (IT) Security, communication security, awareness / education; ensure that all personnel assigned a security role/responsibility are provided with the required training and tools; and ensure a formal framework is implemented to strengthen effective communication mechanisms between regional and national headquarters' partners.

Progress to date:

INAC has made a considerable investment in resources in the security function, appointing a full-time DSO (the DSO previously fulfilled multiple roles in addition to security duties) and assigning dedicated resources to physical security, personnel security, security in contracting, and security awareness functions. The DSO sought and received DM approval of the SMF, a comprehensive document that defines operational and functional roles and responsibilities related to all areas of security, and a RSO Terms of Reference document to outline RSO roles and responsibilities within the security program. The DSO has made significant progress towards achieving the intent of the recommendation to review, define and assign/implement operational and functional roles and responsibilities related to all areas of security, although some work remains to ensure that policy-level roles and responsibilities are clear.

Security training was identified as an issue in 2005 and since that time, the DSO has implemented a one-week training session at Headquarters to educate RSOs on their roles and responsibilities. The DSO has also made RCMP security courses, primarily in physical security, available to all security practitioners free of charge. Despite this progress, security training remains insufficient for both RSOs and DSO staff. A majority of RSOs were found to be insufficiently trained to perform their security-related duties, and the budget for DSO staff training was determined to be inadequate. Further work is required to ensure that RSOs and security personnel are adequately trained, and that their security knowledge is kept current.

Communication within the security organization has improved considerably since 2005. In 2008, the DSO introduced formal monthly teleconferences with RSOs, and all parties have noted that communications between SOHSD and regions have improved significantly. All regions visited indicated that DSO staff provides timely responses to their inquiries. However, work remains to formalize and improve reporting from regions to SOHSD on security activities and incidents.

To improve communication across security functions, the DSO implemented the Departmental Security Committee. This committee provides a formal communication forum for all security functions, and has served to improve communications and coordination of security activities between the DSO and the IT and BCP functions.

2005 Recommendation:

2. It is recommended that the Departmental Security Officer, in collaboration with other departmental areas, at headquarters, and within the regions, review, revise/develop and implement a formal risk assessment and planning framework including: a risk assessment of the departmental security program, physical and Information Technology (IT) threat and risk assessments, a multi-year strategic plan, an annual operational security plan with milestones, a process to monitor and review security deliverable, and update/publish departmental security policies; and review and revise the Departmental Business Continuity Plan (BCP).

Progress to date:

A formal risk assessment of the departmental Security Program has not been performed. TRAs have been conducted for some facilities but not all, and the results have not been aggregated, analyzed, or tracked departmentally by the DSO.

Security planning remains a largely informal process, and a multi-year strategic plan has not yet been developed. An annual operational security plan integrating regional and corporate activities with milestones also does not yet exist, although the DSO does report on SOHSD activities and milestones through the quarterly review process. Work remains to integrate regional security activities, and the DSO has committed to completing a strategic plan in 2010-2011. The DSO has expressed that the results of our audit will be used to identify gaps that will be addressed in the plan.

Monitoring and review of the security program also remains a largely informal and incomplete process. While some mechanisms for the monitoring and review of security deliverables have been defined in the SMF, these mechanisms have not been implemented and are not comprehensive. Current monitoring includes only measures of activity and does not evaluate the effectiveness of the security program. Further effort is required to improve the existing oversight regime to include measures of security program effectiveness.

Although BCP was excluded from the scope of our audit, it was observed that a Departmental Business Continuity Plan was completed, and each of the regions visited had recently updated their regional business continuity plans as a part of the H1N1 exercise.

2005 Recommendation:

3. It is recommended that the Departmental Security Officer (DSO), in collaboration with other departmental areas, at headquarters, and in the regions, review, revise/develop, implement and monitor security procedures related to: physical security, security of personnel, information/assets security, Information Technology (IT) Security, contract security and others as required or as they are released by Treasury Board Secretariat; and review, revise/develop, implement and monitor an awareness/education program to inform employees and senior management on these and other security procedures and their roles/responsibilities.

Progress to date:

Considerable progress has been made in developing procedures to implement the security program. The SMF includes procedures for many security functions, and improvement since 2005 has been noted in several areas, particularly personnel screening. Effort has also been invested in improving security in contracting, although significant issues remain. Security procedures requiring further development include lock-up at end of day (clean-desk), security awareness program, information safeguarding, conduct of security inspections/sweeps, and establishment and maintenance of physical security zones.

Some improvement has been achieved in security awareness in headquarters, although overall awareness remains insufficient in regions. The DSO has worked to increase the frequency of awareness activities, and has conducted numerous awareness sessions in the NCR. This increased activity has not been replicated at a regional level, and considerable work remains to design and implement a formal and comprehensive security awareness program.

7. Recommendations

The recommendations from our audit are:

1. The DSO should update the departmental security policy to more clearly communicate the existing security related roles, responsibilities and accountabilities of the Departmental Security Officer, ADMs, RDGs, security practitioners, contracting staff, line managers and employees.

2. The DSO should further develop and communicate procedures and guidance to support implementation of the departmental security program in regions and sectors (e.g., procedures for lock-up at end of day, guidance on what to look for when conducting a security sweep, trainer's materials for delivering security awareness activities and guidance on how to establish and maintain physical security zones).

3. The ADMs responsible for regional staff and operations should work with the DSO to ensure that sufficient attention and resources are devoted to security in regions, including ensuring that RSOs have sufficient time to perform their security-related duties.

4. INAC should consider appointing Sector Security Officers in all sectors to support implementation of the security program, similar to the Regional Security Officer role. The responsibilities attached to this role and associated level of effort should be presented to INAC Senior Management when the departmental security policy is next updated.

5. The DSO should develop a strategically focused departmental security plan that outlines departmental security objectives and priorities, resource requirements, timelines for meeting baseline government security requirements, and plans for updating all required Threat and Risk Assessments (TRAs) over a five-year cycle.

6. The DSO should improve monitoring of the effectiveness of the security program in regions and sectors to support its continuous improvement (e.g. tracking implementation of recommendations from TRAs, performing random spot checks of security in contracting controls, tracking issues raised in security sweeps to ensure their timely resolution, and performing annual on-site visits to support security practitioners in regions and sectors).

7. The DSO should further develop the security awareness program to extend its reach to regional staff and improve coverage of information safeguarding and security in contracting requirements.

8. The DSO should increase focus on monitoring the effectiveness of security in contracting processes and reduce its direct involvement in the review of Security Requirements Checklists and contract clauses. To accomplish this, an organizational and functional review of the security in contracting function is required to ensure that sufficiently trained and competent contracting officers review and approve security requirements and security clauses. Furthermore, a comprehensive and effective security in contracting compliance monitoring and reporting program is required to ensure compliance is achieved and maintained across the department.

8. Mangement Action Plan

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
1. The DSO should update the departmental security policy to more clearly communicate the existing security related roles, responsibilities and accountabilities of the Departmental Security Officer, ADMs, RDGs, security practitioners, contracting staff, line managers and employees.	• SOHSD will: o In consultation with other federal departments, develop a Statement of roles and responsibilities to be incorporated in the Departmental Security Policy. o Present the draft to ADMs, RDGs and security practitioners for their review and comments. o Implement the Statement of roles and responsibilities.	Departmental Security Officer (DSO)	2010-DEC 2010-DEC 2011-JUN
2. The DSO should further develop and communicate procedures and guidance to support implementation of the departmental security program in regions and sectors (e.g., procedures for lock-up at end of day, guidance on what to look for when conducting a security sweep, trainer's materials for delivering security awareness activities and guidance on how to establish and maintain physical security zones).	• SOHSD will: o Review, identify and prioritize gaps in the existing procedures. • Pending HR and Financial resources, expertise and new PGS Standards, SOHSD will: o Update existing procedures and develop new ones to be included in the Security Management Framework. o Communicate updated procedures to those who need them.	Departmental Security Officer (DSO)	2011-MAR 2012-MAR 2012-MAR

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
3. The ADMs responsible for regional staff and operations should work with the DSO to ensure that sufficient attention and resources are devoted to security in regions, including ensuring that RSOs have sufficient time to perform their security-related duties.	• Following recommendation no 1, DSO to obtain buy-in from ADMs responsible for regional staff and operations: o To ensure their engagement towards the security program in their respective region. o To refocus the Regional Security Officers (RSOs) responsibilities to ensure sufficient time for security duties. o To ensure that RSOs undergo mandatory training related to their duties. o To ensure that the security awareness program is active in their respective region.	Departmental Security Officer (DSO) in collaboration with ADMs responsible for regional staff and operations. (ADM NAO, ADM ROS)	2011-MAR
4. INAC should consider appointing Sector Security Officers in all sectors to support implementation of the security program, similar to the Regional Security Officer role. The responsibilities attached to this role and associated level of effort should be presented to INAC Senior Management when the departmental security policy is next updated.	• Define role and responsibilities for Sector Security Officer as per Recommendation # 1, and determine the associated level of effort the position will require. • DSO to seek approval from Senior Management for the introduction of the Sector Security Officer role.	DSO in collaboration with Sector Managers	2010-DEC 2011-MAR
5. The DSO should develop a strategically focused departmental security plan that outlines departmental security objectives and priorities, resource requirements, timelines for meeting baseline government security requirements, and plans for updating all required Threat and Risk Assessments (TRAs) over a five-year cycle.	• DSO will develop a 3 year Departmental Security plan as per the Policy on Government Security: o To include departmental security strategies, objectives, resource requirements, priorities and timelines. o To include a prioritization of the TRAs nationwide in a 5 year cycle.	Departmental Security Officer (DSO)	2010-AUG

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
6. The DSO should improve monitoring of the effectiveness of the security program in regions and sectors to support its continuous improvement (e.g. tracking implementation of recommendations from TRAs, performing random spot checks of security in contracting controls, tracking issues raised in security sweeps to ensure their timely resolution, and performing annual on-site visits to support security practitioners in regions and sectors).	• Implementation of recommendation no 3 will include specific reporting requirements. • DSO to request regional input to extend beyond NCR the collection of additional statistical data. o Note: Since October 2009, at the DSO's request, regions are providing statistical data on incident reports, sweeps and TRAs which are compiled for trend analysis purposes. • RSOs to address known risks and to report to DSO. • DSO to conduct trend analysis from information obtained nationwide. • DSO to conduct annual regional and sector visits. • DSO to report performance data to HRWSMC	RSOs DSO DSO DSO	2011-APR 2011-MAY 2011-MAR 2011-JUN

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
7. The DSO should further develop the security awareness program to extend its reach to regional staff and improve coverage of information safeguarding and security in contracting requirements.	• SOHSD: o To staff the security training and awareness position o To review existing awareness material. o To identify gaps with the existing awareness program o In synch with Actions described in #3, to review awareness presentations including speaking notes for the RSOs use. o To obtain feedback from the RSOs for analysis and improvement purposes. o To ensure added focus is placed on classification, handling and disposal of information, as well as requirements for security in contracting (completion of SRCLs). o To produce an online security awareness training session.	Departmental Security Officer (DSO)	2011-MAR 2011-JUN 2011-JUN 2011-JUN 2011-JUN 2011-DEC 2011-DEC

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
8. The DSO should increase focus on monitoring the effectiveness of security in contracting processes and reduce its direct involvement in the review of Security Requirements Checklists and contract clauses. To accomplish this, an organizational and functional review of the security in contracting function is required to ensure that sufficiently trained and competent contracting officers review and approve security requirements and security clauses. Furthermore, a comprehensive and effective security in contracting compliance monitoring and reporting program is required to ensure compliance is achieved and maintained across the department.	• DSO to consult with the CFO to: o Revise existing procedures and to develop new ones for the completion and review of SRCLs and inclusion of security clauses in contracts. o To develop training modules for RCMs and contracting administrators for the management of the SRCL process. o To develop training modules for Security Officers responsible for compliance of contract security requirements. • DSO: o To increase focus on monitoring the effectiveness of security in contracting processes. • CFO: o To identify contracting officers to review and to process SRCL forms and to liaise with SOHSD. Note: Checklists and security clauses include this shared activity (DSO/CFO) in the Statement of Roles and Responsibilities as per recommendation no 1.	Departmental Security Officer (DSO) in collaboration with the Chief Financial Officer (CFO)	2010-SEP 2011-MAR

Appendix A: Audit Criteria

Although this audit has three audit objectives, Objective 1 is ostensibly the overall objective of the audit, while Objectives 2 and 3 are subsumed under security program management. The Audit Criteria are derived from the Treasury Board PGS or PGS, (July 2009) and the associated standards and guidelines, in particular, the Directive on Departmental Security Management (DDSM) – Appendix C, Security Control Objectives (July 2009).

Audit Criteria	Reference
Security Management Framework	
1. A security management program is in place with appropriate and clearly defined objectives, roles, responsibilities and accountabilities.	PGS 6.1.1
2. The DSO and security organization ensure that managers at all levels integrate security and identity management into plans, programs, activities and services.	PGS 6.1.4
3. An effective departmental security awareness program is in place.	DDSM App C.
4. The department's risk management program contains processes to formally identify and assess security related risks and select appropriate safeguards.	SOA 9.1
5. The management of security risks is incorporated into departmental practices to systematically adapt to changing needs and threats.	PGS 6.1.7
6. Sufficient and appropriate personnel are assigned to support implementation of the security management program, regionally and nationally.	DDSM App C.
7. Administrative investigations related to security incidents are conducted in accordance with the requirements of the PGS.	PGS 6.1.7 DDSM App C. SOA 16
8. The security management program is monitored and assessed to measure achievement against expected results.	PGS 6.1.1 DDSM App C.
Personnel Security	
9. Security screening is conducted for all individuals who access government information and assets prior to commencement of their duties.	PGS 6.1.5
Security in Contracting	
10. Security requirements for contractors are identified, documented, addressed and monitored in the procurement process.	DDSM App C.
Physical Security	
11. Appropriate physical security controls are in place at facilities to provide for the protection of personnel and safeguarding of information and assets.	DDSM App C.
Information Safeguarding	
12. Information is protected from unauthorized access, use, disclosure, modification, disposal, transmission or destruction throughout its lifecycle	DDSM App C.
13. Information is identified and categorized based on the degree of injury that could be expected to result from the compromise of its confidentiality, availability or integrity.	DDSM App C.
14. Appropriate security management measures are in place for ensuring the authorized disposal of information.	DDSM App C.

Acronyms related to TBS references

PGS: Policy on Government Security (PGS), issued July 2009
DDSM: Directive on Departmental Security Management, issued July 2009.
OSS-PS: Operational Security Standard, Physical Security, 2004
SCMS: Security and Contracting Management Standard 1996
SOA: Security Organization and Administration, 1995
PSS: Personnel Security Standard