Canadian Heritage | Patrimoine canadien

Canada

Audit of Departmental Security

Office of the Chief Audit and Evaluation Executive
Audit and Assurance Services Directorate

October 2013

THIS PAGE INTENTIONALLY LEFT BLANK

Cette publication est également disponible en français.

This publication is available in PDF format
on the Internet at http://www.pch.gc.ca/eng/1330455721434/1330456887503

Catalogue No. CH6-14/2013E-PDF
ISBN: 978-1-100-22927-0

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

Introduction

Government security is the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence, hazards, and other damaging environmental effects. The extent to which government departments can ensure their own security directly affects their ability to ensure the continued delivery of services that contribute to the health, safety, economic well-being, and security of Canadians. To support these requirements, the objectives of Treasury Board Secretariat's *Policy on Government Security* are to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management.

Within the Department of Canadian Heritage (PCH or the Department), responsibility for safety and security lies with the Human Resources and Workplace Management Branch (HRWMB). A Departmental Security Officer (DSO), reporting to the Director General of the HRWMB, has been appointed by PCH and is responsible for five core business units: Security; Security Policy and Awareness; Occupational Health and Safety (OHS); Business Continuity Planning (BCP); and Facilities Management.

The authority for this audit is derived from the Multi-Year Risk-Based Audit Plan (RBAP) 2012-13 to 2014-15 which was recommended by the Departmental Audit Committee and approved by the Deputy Minister in March 2012.

The objective of the audit is to provide senior management with assurance on the adequacy and effectiveness of governance, risk management practices, and internal controls of PCH's Security Program. The audit has five sub-objectives

1. To assess the extent to which PCH's policies and procedures related to departmental security, are in compliance with related legislation and central agency requirements;
2. To assess the extent to which departmental security policies and practices, are complied with in practice;
3. To assess the efficiency and effectiveness of management controls and procedures in place to help ensure that the continuity of PCH operations and services is maintained in the presence of security incidents, disruptions, or emergencies;
4. To assess the efficiency and effectiveness of management controls and procedures in place to: safeguard PCH's information, assets, and services from compromise; protect PCH employees against workplace violence; and effectively coordinate the management of security incidents; and
5. To assess the efficiency and effectiveness of governance and communication structures, mechanisms, and resources in place to ensure efficient and effective management of security.

The scope of this audit covered PCH's security management practices in place from April 2011 to the completion of audit work in May 2013. The audit excluded the assessment of management practices and controls related to the security of information systems and technology.

Key Findings

Throughout the audit work, the audit team observed several examples of good practices in terms of governance structures, risk management practices, and internal controls processes. This resulted in several observed strengths which are listed below:

- The importance of security within PCH is recognized and supported by senior management and is reflected in PCH's governance and oversight structures, which were found to be effective.
- The Department has implemented a number of policies and guidelines that define its expectations and requirements with respect to departmental security and safety. These policies are consistent with central agency requirements and are readily accessible to all personnel through the intranet.
- The roles and responsibilities of staff within Safety and Security Program are well-defined and understood both at Headquarters and in the regional offices.
- Safety and security matters are guided by the Departmental Safety and Security Plan which identifies the key safety and security risks PCH faces and helps focus its efforts to strengthen safety and security over a three year planning period.
- A number of security procedures have been implemented over the past few years to strengthen the consistency and rigour of PCH's security activities, such as physical security sweeps, workplace inspections, and testing of Business Continuity Plans (BCPs), both at Headquarters and in the regional offices.
- There are a number of physical access controls in place to restrict and control access to PCH premises to authorized personnel both at Headquarters and in the Regions. Physical access controls observed through the audit include access to elevators restricted by security gates that require a valid access card to be opened, the presence of security guards on main floors at Headquarters with clear views to the elevators, and secure access to offices at all locations visited using an access card system.
- PCH has implemented mandatory training sessions to increase awareness of safety and security risks and the expectations for all personnel.
- PCH has developed and implemented formal processes and procedures for the identification of critical services and the development of BCPs. Lessons learned are shared with the BCP Working Group.

The results of the audit work identified opportunities for improvement to existing governance, internal control and risk management.

Governance

The results of the audit indicated that governance structures have been established for the oversight of the Department's Safety and Security Program. However, there are no formal performance measures in place or regular, consolidated reporting to senior management on the results of compliance activities and the Security Program performance. This includes trends identified and best practices related to departmental safety and security.

Internal Control

The results of the audit indicate that PCH has focused on developing and implementing a number of internal controls to support the effective management of departmental safety and security. However improvement is needed in the following areas:

- Activities to identify, report, and follow up on instances of non-compliance with established security policies are not conducted in a timely manner.
- Core training on the Operational Standard of BCP for BCP leaders and alternates, as well as other training for all security personnel and PCH employees has not been provided as required.
- Moderate issues were identified in the control and usage of electronic storage devices.

Risk Management

An annual review as set out in the Department's Safety and Security Plan (DSSP) has not been done, but is planned to start in the fall 2013.

Recommendations

The Departmental Security Officer should:

In relation to Governance:

1. develop and implement a formal process to measure, monitor, and report on the performance of the Safety and Security Program.

In relation to Internal Control:

2.1 improve the timeliness, consistency, and nature of core security compliance activities;

2.2 ensure that PCH employees, security personnel and those responsible for BCPs receive all core training to fulfill their roles and responsibilities in a timely manner;

2.3 strengthen physical controls over the protection of classified and sensitive information.

In relation to Risk Management:

3. ensure that annual updates, reviews and assessments of security risks are reflected in the Departmental Safety and Security Plan (DSSP) in a timely manner.

Statement of Conformance

In my professional judgment as Chief Audit and Evaluation Executive, the audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada. A practice inspection has not been conducted.

Audit Opinion

In my opinion, the Department's Security Program is generally controlled in the areas of governance and risk management with an opportunity to improve its Performance Measurement Framework and annual Departmental Safety and Security Plan (DSSP) update. Internal operational controls have moderate issues requiring management attention.

Original signed by

_____

Richard Willan
Chief Audit and Evaluation Executive
Department of Canadian Heritage

Audit Team Members

Maria Lapointe-Savoie, Director
Miklos Horvath
Siriseng Malichanh
Catherine Yan
With the assistance of external resources

1. Introduction and Context

1.1 Authority for the Project

The authority for this audit is derived from the Multi-Year Risk-Based Audit Plan 2012-13 to 2014-15 which was recommended by the Departmental Audit Committee and approved by the Deputy Minister in March 2012.

1.2 Background

Government security is the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence, hazards, and other damaging environmental effects. The extent to which government departments can ensure their own security directly affects their ability to ensure the continued delivery of services that contribute to the health, safety, economic well-being, and security of Canadians.

To support the above requirements, the objectives of the Treasury Board Secretariat (TBS) *Policy on Government Security* are to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management. The expected results of this policy are to ensure that:

- Information, assets and services are safeguarded from compromise and employees are protected against workplace violence;
- Governance structures, mechanisms and resources are in place to ensure effective and efficient management of security at both a departmental and government-wide level;
- Management of security incidents is effectively coordinated within departments and government-wide;
- Interoperability and information exchange are enabled through effective and consistent security and identity management practices; and
- Continuity of government operations and services is maintained in the presence of security incidents, disruptions or emergencies.

In addition to the TBS *Policy on Government Security,* there are a number of other related and/or supporting policies, standards and directives, with which federal government departments must comply. These include the *Occupational Safety and Health Policy*, the Directive on Departmental Security Management, the Operational Security Standard on Physical Security, the Personnel Security Standard, the Guideline on Developing a Departmental Security Plan and, the *Canada Labour Code*.

PCH has appointed a Departmental Security Officer (DSO) who reports to the Director General (DG) of the Human Resources and Workplace Management Branch (HRWMB). Five core business units report to the DSO: Security, responsible for ensuring PCH premises and assets are safeguarded from unauthorized access and protected against

compromise; Security Policy and Awareness, responsible for the coordination of the Department's security policies and strategies; Occupational Health and Safety (OHS), responsible for the establishment and maintenance of occupational health and safety activities to reduce the incidence of occupational injuries and illnesses; Business Continuity Planning, responsible for the development and maintenance of the Department's BCP Program; and Facilities Management, responsible for coordination between PCH occupants and Public Works and Government Services Canada.

2. Objective

The objective of the audit is to provide senior management assurance on the adequacy and effectiveness of governance, risk management practices, and internal controls of the Department's security program. The audit has five sub-objectives:

1. To assess the extent to which PCH's policies and procedures related to departmental security are in compliance with related legislation and central agency requirements;
2. To assess the extent to which departmental security policies and practices are complied with in practice;
3. To assess the efficiency and effectiveness of management controls and procedures in place to help ensure that the continuity of PCH operations and services are maintained in the presence of security incidents, disruptions, or emergencies;
4. To assess the efficiency and effectiveness of management controls and procedures in place to: safeguard PCH's information, assets, and services from compromise; protect PCH employees against workplace violence; and effectively coordinate the management of security incidents; and
5. To assess the efficiency and effectiveness of governance and communication structures, mechanisms, and resources in place to ensure efficient and effective management of security.

The results have been reported under governance, internal control, and risk management.

3. Scope

The scope of this audit covered PCH's security management practices in place from April 2011 to the completion of audit work in May 2013. The audit excluded the assessment of management practices and controls related to the security of information systems and technology, as these areas were examined through the Audit of Information Technology (IT) Security.

4. Approach and Methodology

All audit work was conducted in accordance with the Treasury Board Secretariat's *Internal Auditing Standards for the Government of Canada,* and the *Policy on Internal Audit.*

Audit criteria were developed based on the Treasury Board Secretariat's Core Management Controls, policies and directives related to departmental security and safety. These criteria identify the standards against which an assessment is made and form the basis for the audit work plan and the conduct of the audit. The criteria are specific to each audit's objectives and scope. The detailed audit criteria for the audit objectives for the Audit of Departmental Security are provided in Appendix A.

The audit methodology included:

- Reviewing PCH's documentation, guidelines and procedures, policies and processes relevant to departmental security and safety, occupational health and safety, and general security;
- Conducting site visits to three regional offices to observe and examine the safety and security practices in place;
- Conducting interviews with 23 representatives from the HRWMB, the Chief Information Officer Branch, and PCH regional offices;
- Reviewing a sample of security compliance activities, personnel security clearance files, business continuity plans, business impact analysis documents, management and governance reporting, memoranda of understanding, committees and working groups meeting minutes, and other documentation of relevance to key controls identified for fiscal year 2011-12 to May 2013; and
- Analyzing information obtained through documentation review and interviews.

5. Findings and Recommendations

This section presents the detailed findings and related recommendations of the Audit of Departmental Security. The findings are based on a combination of the evidence gathered through the examination of documentation, analysis, file testing, and interviews conducted for each of the audit criterion. Appendix A provides a summary of all findings and conclusions for each of the criteria assessed during the audit. Details of the audit's observations and recommendations are provided below.

5.1 Governance

The results of the audit indicate that governance structures have been established for the oversight of the Department's safety and security program. The importance of security within PCH is recognized and supported by senior management and is reflected in the PCH governance and oversight structures. In this regard, a number of oversight committees have been established to oversee, advise upon, and respond to matters of security, and employee safety. These committees, which include the Crisis Management Team, Human Resource and Workplace Management Advisory Committee, BCP Working Group, and Occupational Health and Safety National and Local Committees, have senior representation and meet regularly to discuss PCH security and safety matters. The Crisis Management Team (CMT) consists of PCH's senior management team and is

responsible for all decisions, direction, and the approval of funding for handling specific crisis events. The audit team understands that the composition of the CMT was recently reviewed to help identify the core members required in crisis situations; this has reduced the committee's size.

Roles and responsibilities for departmental security are well-defined and understood both at Headquarters and in regional offices. Responsibilities are documented in various forms, including job descriptions, policies such as the Department's *Business Continuity Planning (BCP) Program Policy* and *Security Policy*, and through formal guidelines and standards.

The audit team identified one area for improvement in relation to governance and is discussed below:

5.1.1 Reporting on Safety and Security Program Performance

There are no formal performance measures in place or regular, consolidated reporting to senior management on the results of compliance activities and Security Program performance. This includes trends identified and best practices related to departmental safety and security.

Analysis

The Canadian Heritage Departmental Safety and Security Plan requires that the safety and security program`s success be evaluated through a performance measurement strategy. PCH's security program includes five core components: Emergency Management and Business Continuity Planning; Policy, Planning and Awareness; Occupational Health and Safety; Physical Security; and Facilities Management. The performance strategy is expected to include performance indicators to enable analysis of mitigation measures and the development of annual security priority actions. Updates on the program`s results are expected to be provided annually or as required to the Deputy Minister and the Executive Committee.

The audit team identified that governance committees receive updates on various aspects of the safety and security program through regular committee and working group meetings. These updates include reporting of the number of workplace inspections performed, major repairs in progress for the premises, the status of security activity and courses being developed, BCP crisis management activities, and approval for changes to security guidelines and standards. However, there was no evidence of formal reporting on the overall results of safety and security activities and related trends and best practices in a consolidated report to the Deputy Minister or to any of the governance committees in place.

Although a formal performance measurement strategy is required as part of the Departmental Safety and Security Plan (DSSP), as of the end of the audit work, this had not been developed. There was no evidence to support regular consolidated reporting to

senior management against pre-defined performance indicators on the progress and results of PCH `s Safety and Security Program.

The absence of consolidated reporting is due in part to the limited tools in place for recording and analyzing the results of security activities, such as physical security sweeps and workplace inspections, in a centralized and consolidated manner. Currently, each operating unit (Security, OHS, and BCP) separately maintain their records and results of activities through individual Excel worksheets and manual paper trails, which does not enable the consolidation and analysis of results in a cost-effective or timely manner. Improvements can be made to strengthen reporting in order to support oversight and decision-making by senior management.

Risk Assessment

The absence of formal, regular, and consolidated reporting on the progress and results of the safety and security program, including trends and best practices identified, may limit the ability of management to monitor and respond to emerging and systemic safety and security issues. The absence of consolidated analysis and reporting on the performance of PCH's safety and security program further limits the extent to which management can readily identify and respond to priority areas in order to optimize the allocation of PCH resources and effort.

Recommendation

1. The Departmental Security Officer should develop and implement a formal process to measure, monitor, and report on the performance of the safety and security program.

5.2 Internal Control

PCH has implemented a number of policies that define its expectations and requirements with respect to departmental security and safety, including the Department *Security Policy, BCP Program Policy*, and *Occupational Health and Safety Policy*. These policies are consistent with central agency requirements and are readily accessible to all personnel through the intranet. Overall, safety and security matters are guided by the PCH Safety and Security Plan, which provides an important roadmap to focus PCH's efforts on strengthening safety and security over a three-year planning period.

PCH has developed and implemented formal processes and procedures for the identification of critical services and development of BCPs. A number of security procedures have been implemented over the past few years to strengthen the consistency and rigour of PCH's security activities, including physical security sweeps, floor inspections, and testing of BCPs both at Headquarters and in regional offices. There are a number of physical access controls in place to restrict and control access to PCH premises to authorized personnel.

The results of the audit identified four areas for improvement in terms of internal control and are discussed below:

5.2.1 Compliance Activities

Activities to identify, report, and follow up on instances of non-compliance with established security policies are not conducted in a timely manner.

Analysis

PCH has implemented procedures to monitor and report on compliance with established policies on security and safety, including security sweeps and workplace inspections. Random security sweeps are required to be conducted by Safety and Security Services at Headquarters and by designated security coordinators in the regions. The sweeps are designed to identify any instances in which classified or protected information and valuable assets are left unsecured, and any positive practices or deficiencies identified through the sweeps are expected to be reported to the DSO or regional management. The DSO is expected to report on the results of the sweeps to the DG HRWMB. Workplace inspections to identify physical workplace hazards are expected to be conducted annually by occupational health and safety (OHS) officers. There is a Workplace Inspections Checklist which provides a list of potential workplace hazards that OHS officers should look for during the inspection.

The audit team identified that, in the case of security sweeps, expected procedures are well documented in guidelines and standards. We understand, based on interviews with management that PCH's goal is to conduct sweeps in all locations over a three-year period. However, this expectation is not formally documented and there is no defined schedule to ensure this is achieved over the three-year time frame. As a result, it was not possible to determine if security sweep activities are being conducted in all locations in a timely manner, and instances of non-compliance remaining undetected for some time. As of the end of the audit work, 11 security sweeps had been conducted at Headquarters and one sweep had been conducted at a regional office between November 2012 and January 2013. The sweeps at Headquarters revealed 94 incidents of non-compliance, most of which related to instances of unsecured protected information. Minor instances of unsecured keys, passwords, and assets such as laptop computers and BlackBerry devices were also identified. Within the regional office, 47 instances of non-compliance were identified, the majority of which related to unsecured information. Five reports had been formally issued to management out of the 11 sweeps conducted at Headquarters, and a preliminary report had been issued for the regional sweep. Informal follow-up was undertaken by the Security team for three of the five instances, but there was no formal follow-up on management's actions to address the instances of non-compliance.

With respect to workplace inspections, the audit identified weaknesses and inconsistencies in the documentation supporting the inspection process. Based on a sample of workplace inspection logs reviewed, the audit team noted that in many cases, the date of the inspection was not recorded or identifiable, there was no documented

evidence to show that an inspection had been conducted, and there was no formal sign-off on the review or approval of inspection results. The majority of issues identified through these inspections related to the presence of unauthorized electrical appliances, cluttered offices, and overloaded shelves. There was limited evidence of any formal reporting or follow-up on the results of workplace inspections.

In addition to strengthening identification, reporting, and follow-up on compliance activities, implementing a more consistent and defined approach with formal accountability for conducting compliance activities would help allocate resources to ensure that all of the required compliance activities are completed in a timely manner. Strengthening the supporting documentation for inspections would provide greater assurance that all of the required procedures have been conducted, and would improve future planning, since more complete records would be kept of the results of past events and issues identified. It would also enable management to report on workplace hazards and security issues on a consolidated basis and to identify and respond to trends.

Risk Assessment

There is a risk that all required security procedures cannot be conducted in a timely manner and that incidents of non-compliance may go undetected for a long period of time. Current tools to support the analysis and consolidation of the results of compliance activities are limited.

The absence of timely and formal reporting and follow-up with management on instances of non-compliance (identified through security activities) further limits the extent to which management can be confident that appropriate remedial action is taken to address and resolve instances of non-compliance.

Recommendation

2.1 The Departmental Security Officer should improve the timeliness, consistency, and nature of core security compliance activities.

5.2.2 Training

Core training on the Operational Standard of BCP for BCP leaders and alternates, as well as other training for all security personnel and PCH employees has not been provided as required.

Analysis

A number of mandatory training sessions are provided to PCH staff members to increase their understanding and awareness of security risks, policies, and expectations. These sessions include orientation sessions for new employees and new managers with the security portions; hazard prevention activities targeted to specific employees at risk based on their location of work and responsibilities; and an annual security refresher course that

is mandatory for all PCH employees. As of the end of the audit fieldwork, the audit team was informed by management that approximately 65% of all employees had received this refresher training titled "Annual Security Briefing". In addition, a new Workplace Violence Prevention Program is to be delivered to all PCH employees but has not yet been deployed; it is expected to be approved in fall 2013.

PCH's *BCP Program Policy* requires BCP leaders to take the course on Operational Standard for Business Continuity Planning offered by the Canada School of Public Service. However, the Canada School of Public Service has not offered the BCP training course for the past year. As a result, the majority of BCP leaders and alternates (18 of 22) have not received the required training. While the BCP Manager has been maintaining the required designation of Certified Business Continuity Professional (CBCP), there have been a number of new personnel with BCP responsibilities who have not received the required training to help them fulfill their roles and responsibilities.

Based on the results of interviews and testing, individual training needs for safety and security personnel are identified annually during the performance review process. There was no evidence to support the monitoring and tracking of training which security personnel actually received for the audit period.

Risk Assessment

The absence of core BCP training provided over the past year may increase the risk that personnel may not be able to fulfill all of their required roles and responsibilities since they have not been provided with sufficient training and expertise in the subject matter area.

Recommendation

2.2 The Departmental Security Officer should ensure that PCH employees, security personnel and those responsible for BCPs receive all core training to fulfill their roles and responsibilities in a timely manner.

5.2.3 Protection of Information Assets

Moderate issues were identified in the control and usage of electronic storage devices.

Analysis

PCH has a number of policies and standards to help ensure compliance with federal government security requirements and to protect the integrity of PCH information. These include (a) the *Departmental Network Storage Policy* which specifies encryption requirements for the storage of information on PCH networks; (b) the *PCH Security Policy*, which describes the minimum requirements for physical security measures to be applied to sensitive information; and (c) the IT Removable Media Protection and Disposal Standard, which describes requirements for the protection and destruction of

data on all portable electronic media and devices. In addition to formal policies and procedures, departmental broadcasts are issued to remind all PCH employees of their duty to protect information, including the requirements to properly secure USB keys containing Protected or Classified information.

The audit work determined that electronic documents at a level of Protected B and above were being stored on removable electronic media, including USB keys. Removable electronic storage media, such as USB keys, external drives, memory cards, and compact discs can be easily misplaced or lost, putting at risk any information stored on them. For example, although the USB key might be properly used to transfer information from one secure electronic media to another, the data may not be properly deleted from the key. These media were not always properly stored in a locked area. There is currently no mechanism in place to control the issuance of USB keys and the destruction of data on electronic media.

Risk Assessment

There is a risk that by not communicating PCH's expectations and policies on a regular basis regarding the proper storage and disposal of sensitive information to all personnel, information may be accessed by unauthorized individuals, thereby compromising the reliability of access to PCH information. This risk is increased given the fact that devices used to transfer soft copy information do not contain basic security protection, such as passwords and restricted functionality for editing and printing.

Recommendation

2.3 The Departmental Security Officer should strengthen physical controls over the protection of classified and sensitive information.

5.3 Risk Management

An annual review, as set out indicated in the Department's Safety and Security Plan, has not been done, but is planned to start in the fall 2013.

Analysis

The audit examined whether risks to the achievement of safety and security objectives are properly identified and assessed, and whether effective and efficient controls are implemented to mitigate risk to an acceptable level.

In 2009, the Management Accountability Framework (MAF) and the new Treasury Board Secretariat (TBS) *Policy on Government Security* introduced more stringent requirements for security management. To comply with these requirements, the Department put a Departmental Safety and Security Plan (DSSP) in place, for the first time, which was approved by the Deputy Minister in August 2012. The DSSP identifies the key safety and

security risks facing PCH, controls to mitigate these risks, key actions required to strengthen mitigation activities, and accountabilities for implementing action plans. The Plan provides an important roadmap to focus PCH's efforts to strengthen security and safety over the three-year planning period based on the risks identified and the expectation is that it will be reviewed and updated on an annual basis.

As a component of the DSSP and at an operational level, Business Impact Assessments (BIAs) have been developed every three years to determine critical services and priorities, the potential impact of disruptions on the organization that may impact these critical services, and key actions required to address these impacts. These documents are a critical element of the Business Continuity Planning (BCP) Program, as they help to focus efforts on areas of highest potential risk to PCH. However, as for the other areas of the Safety and Security Program, for instance employee safety and security or work place hazards and violence, there is limited evidence that a formal update has performed annually to capture emerging issues or risks.

During the audit, it was indicated that the DSSP has not been updated but that the exercise will be launched in the fall 2013.

Risk Assessment

When risk assessments for all areas of safety and security are not performed in a timely manner, it is likely that the unknown safety and security risks in the Department are not considered. There is a risk that emerging issues or risks may not be addressed thus undermining the efforts put into the DSSP.

Recommendation

3. The Departmental Security Officer should ensure that annual updates, reviews and assessments of security risks are reflected in the Departmental Safety and Security Plan (DSSP) in a timely manner.

Appendix A – Audit Criteria

The conclusions reached for each of the audit criteria used in the audit were developed according to the following definitions.

Numerical Categorization	Conclusion on Audit Criteria	Definition of Conclusion
1	Well Controlled	• Well managed and effective, no material weaknesses noted.
2	Controlled	• Well managed and effective, but minor improvements are needed.
3	Moderate Issues	Has moderate issues requiring management focus (at least one of the following two criteria need to be met): • Control weaknesses, but exposure is limited because likelihood of risk occurring is not high; • Control weaknesses, but exposure is limited because impact of the risk is not high.
4	Significant Improvements Required	Requires significant improvements (at least one of the following three criteria need to be met): • Material Financial adjustments to line item or area or to the department; or • Control deficiencies represent serious exposure; or • Major deficiencies in overall control structure. Note: Every audit criteria that is categorized as a **"4"** must be immediately disclosed to the CAEE and the appropriate Director General or higher level for corrective action.

The following are the audit criteria and examples of key evidence and/or observations noted which were analyzed and against which conclusions were drawn.

Audit Objective 1: To assess the extent to which PCH's policies and procedures related to Departmental security, are in compliance with related legislation and central agency requirements.			
Criteria #	**Audit Criteria**	**Conclusion**	**Examples of Key Evidence / Observation**
Internal Controls			
1.1	PCH has developed and implemented policies, guidelines, and procedures that are aligned with government-wide policies.	**1**	• Formal policies and guidelines have been documented and are consistent with central agency policies and directives.
1.2	Mechanisms are in place to identify and monitor changes to relevant federal policies and legislation and align operating directives, procedures, and guidelines with relevant federal policy requirements.	**1**	• Management is kept apprised of changes in federal policies and legislation via various mailing and e-mail distribution lists. • PCH policies are consistent with current federal policy requirements.
1.3	Responsibility for monitoring compliance with relevant legislative requirements is clearly communicated and followed in practice.	**1**	• Roles and responsibilities for monitoring compliance are clearly defined in job descriptions and in policies, guidelines, and the Departmental Safety and Security Plan.
Audit Objective 2: To assess the extent to which departmental security policies and practices, are complied with in practice.			
Criteria #	**Audit Criteria**	**Conclusion**	**Examples of Key Evidence / Observation**
Governance and Internal Control			
2.1	Monitoring of compliance with policies and procedures is conducted on a regular basis and reported to management.	**3**	• There are a number of documented procedures to monitor and report on compliance with established policies on security and safety, including security

			sweeps. • Issues were identified with respect to the timeliness with which the results of compliance activities are reported to management and the extent to which compliance activities are consistently documented.
2.2	Mechanisms are in place for sweeps, workplace inspections and departures to ensure approved policies and procedures are identified and remediated in a timely manner.	**3**	• Limited evidence was available to support follow-up on management's action plans to address issues and weaknesses identified through compliance activities.
2.3	Roles, responsibilities, and accountabilities for security procedures (including BCP) are clearly defined, communicated, and understood.	**1**	• Roles and responsibilities are clearly defined in job descriptions, policies, and guidelines.
2.4	Employees are provided with the tools and training they require performing their duties effectively with respect to security, including BCP.	**3**	• Mandatory training sessions are provided to PCH staff to increase their understanding and awareness of security risks, policies, and expectations. • A number of BCP leaders have not received the required core BCP training due to the fact that the course was not offered over the past year by the service provider. • There was no evidence to support the monitoring and tracking of training actually received for the period under the scope of the audit.
Audit Objective 3: To assess the efficiency and effectiveness of management controls and procedures in place to help ensure that the continuity of PCH operations and services are maintained in the presence of security incidents, disruptions, or emergencies.			

Criteria #	Audit Criteria	Conclusion	Examples of Key Evidence / Observation
Governance and Risk Management			
3.1	Business continuity activities, plans, and program are comprehensive, documented, approved, and based on business impact analysis.	**1**	• The audit confirmed that BIAs and BCPs had been completed by all required units for all critical services identified. BCPs for Headquarters were last reviewed in the fall of 2012, and BCPs for the regional offices were last reviewed in January of 2012.
3.2	Responsibilities, procedures, and performance expectations with respect to departmental security, including BCP, have been documented and clearly communicated.	**2**	• Roles and responsibilities for security procedures are clearly defined in job descriptions, policies, and guidelines. • However, there are no formally defined performance measures to enable tracking and reporting on the security program's actual performance.
3.3	The activities, schedules and resources required to implement the departmental security plans, including BCP, in an effective, efficient, and fiscally responsible manner have been identified and integrated into business plans and budgets.	**2**	• The Departmental Safety and Security Plan identifies the key safety and security risks facing the Department and helps focus PCH's efforts to strengthen safety and security on areas with the highest risk and priority. • BCPs have been developed based on BIAs that identify critical services, priorities and areas of highest potential risk to the Department. • There is limited evidence that a formal updated was performed annually to capture emerging issues or risk for other areas of safety and security.
3.4	Results of performance against stated objectives are documented,	**2**	• There is no formal document report to support the consolidation, analysis, and

	communicated and reported to the required authority levels and are acted upon.		reporting of the results of BCP testing.
Audit Objective 4: To assess the efficiency and effectiveness of management controls and procedures in place to: safeguard PCH's information, assets, and services from compromise; protect PCH employees against workplace violence; and effectively coordinate the management of security incidents.			
Criteria #	**Audit Criteria**	**Conclusion**	**Examples of Key Evidence / Observation**
Governance, Internal Control and Risk Management			
4.1	Procedures have been implemented to restrict access to and safeguard physical assets as well as data and information.	**2**	• Physical access controls, such as restricted access cards and security gates, are in place, at PCH offices. • Security sweeps are conducted to identify instances of unsecured information and assets.
4.2	Policies and procedures have been developed and implemented to safeguard the health and safety of employees, including protection against workplace violence.	**2**	• Workplace inspections are conducted annually to identify workplace hazards. Policies on Risk Prevention and Violence Prevention are still in draft form. • Management should expedite the approval of these policies as well as the implementation of the Hazardous Prevention and Workplace Violence Prevention training activities.
4.3	Mechanisms are in place to track security incidents, communicate and report to the proper delegated authorities on a regular and timely basis, and take corrective action as necessary.	**3**	• There is no centralized and consolidated log of all incidents nor is there documentation supporting the reporting and follow-up of management action plans. • Electronic storage media, such as USB keys, are not consistently stored securely within the Department.
4.4	The activities, schedules and resources required to implement the departmental security plans to protect PCH	**2**	• The Departmental Safety and Security Plan identifies the key safety and security risks facing the Department and helps focus PCH's efforts to

	assets, information, and employees in an effective, efficient, and fiscally responsible manner have been identified and integrated into business plans and budgets.		strengthen safety and security areas with the highest risk and priority. • As indicated in the Department's Safety and Security Plan (DSSP), an annual review has not been done, and is planned to start in the fall 2013.
Audit Objective 5: To assess the efficiency and effectiveness of governance and communication structures, mechanisms, and resources in place to ensure efficient and effective management of security.			
Governance, Internal Control and Risk Management			
5.1	An effective governance structure is in place where roles, responsibilities, and accountabilities are clearly communicated and understood to enable strategic oversight of the Department's security program, including BCP.	**1**	• A number of oversight committees have been established to oversee, advise upon, and respond to matters of security, and employee safety.
5.2	Sufficient information related to departmental security, including BCP, is provided to the oversight bodies, management, and partners on a timely basis to enable effective decision making.	**2**	• Governance committees receive updates on various aspects of the safety and security program through regular committee and working group meetings. However, there are no formal performance measures in place and no regular, consolidated reporting is provided to senior management.
5.3	Mechanisms are in place to identify, develop, and manage effective partnerships with other organizations with complementary objectives and goals to improve overall efficiency and effectiveness.	**1**	• The agreement for security with PWGSC is provided under the blanket federal government agreement.

Appendix B – Management Action Plan

Project Title: Audit of Departmental Security

Management Action Plan			
Governance			
Recommendation	**Actions**	**Who**	**Target Date**
1. *The Departmental Security Officer should develop and implement a formal process to measure, monitor, and report on the performance of the Safety and Security Program.*	Agree DSO will develop and implement the Departmental Safety and Security Plan (DSSP) performance measurement strategy, which will include defining key performance indicators to measure the results of the program on a regular basis. DSO will develop a mechanism to consolidate safety and security program activities and report to senior management.	D/DSO	February 2014
Internal Controls			
Recommendations	**Actions**	**Who**	**Target Date**
2.1 *The Departmental Security Officer should improve the timeliness, consistency, and nature of core security compliance activities.*	Agree DSO has developed a mechanism, as outlined in the approved Departmental Safety and Security	D/DSO	August 2013

	Plan (DSSP), to ensure that compliance activities (security sweeps and workplace inspections) are undertaken consistently and in a timely manner. Workplace inspections occur once every twelve months while security sweeps occur monthly.		
2.2 The Departmental Security Officer should ensure that PCH employees, security personnel and those responsible for BCPs receive all core training to fulfill their roles and responsibilities in a timely manner.	Agree DSO will ensure that security personnel and those responsible for BCPs (approximately 20 FTEs) receive all critical training to fulfill their roles and responsibilities by determining alternative options, pending the development of a new course at the Canada School of Public Service (CSPS), thereby ensuring that training can be provided as and when required. This may include the use of training that currently is offered from recognized third party organizations.	Manager EM	March 2014
2.3 The Departmental Security Officer should strengthen physical controls over the protection of classified and sensitive information.	Agree DSO will continue to provide mandatory security awareness session to all PCH staff which will focus, in part, on the proper handling of sensitive information. DSO will work with the CIO to develop a	D/DSO	March 2014

	departmental directive on the proper/secure use of portable storage devices. Planning efforts are currently underway with CIOB, and various options were shared, in September 2013, with a Level 2 Governance Committee (Human Resources and Business Services Committee).		
Risk Management			
Recommendation	**Actions**	**Who**	**Target Date**
3. *The Departmental Security Officer should ensure that annual updates, reviews and assessments of security risks are reflected in the DSSP in a timely manner.*	Agree As part of the regular DSSP review process, risks will be assessed and updated on a three year cycle.	D/DSO	December 2013