[*] An asterisk appears where sensitive information has been removed in accordance with the *Access to Information Act* and *Privacy Act*.

PRIVY COUNCIL OFFICE

Audit of Physical and Personnel Security

Audit and Evaluation Division

Final Report

September 13, 2013

Table of Contents

Acronyms used in this Report

CRA	Canada Revenue Agency
CSB	Corporate Services Branch
CSIS	Canadian Security Intelligence Service
DSEMP	Departmental Security and Emergency Management Plan
DSO	Departmental Security Officer
IRBM	Integrated Results-based Management
ITSD	Informatics and Technical Services Division
OPI	Office of Primary Interest
OSB	Office of the Superintendent of Bankruptcy
PCO	Privy Council Office
PMO	Prime Minister's Office
PWGSC	Public Works and Government Services Canada
RCMP	Royal Canadian Mounted Police
SECOPS	Security Operations Division
SEM	Security and Emergency Management
TBS	Treasury Board Secretariat
TVRA	Threat, Vulnerability and Risk Assessment

Executive Summary

Authority

The Audit of Physical and Personnel Security was approved by the Clerk as part of the Privy Council Office (PCO) Risk-Based Internal Audit Plan 2012-2013 to 2014-2015.

Objectives

The objectives of the audit were:

1. To assess the design and operating effectiveness of governance structures and processes for physical and personnel security;
2. To assess the adequacy of risk assessment processes for physical and personnel security;
3. To determine if appropriate physical security controls have been established and implemented to safeguard facilities, information and assets, and to comply with government policy; and
4. To determine if appropriate personnel security controls have been established and implemented to protect sensitive information and assets, and to comply with government policy.

Scope

The audit scope included physical and personnel security components of the PCO Security and Emergency Management (SEM) program administered by Security Operations Division. The period of audit coverage was July 2009 to October 2012, though subsequent events were also considered.

For purposes of the audit, we defined physical security as the use of physical safeguards, equipment or procedures to prevent or delay unauthorized access to assets, to detect attempted and actual unauthorized access and to activate appropriate responses. The audit included all facilities used by PCO regardless of ownership; a risk-based approach was used to select facilities and controls for audit testing.

The assessment of personnel security focused on processes for granting Reliability Status and security clearances at the SECRET and TOP SECRET levels. The population for audit testing included all arrivals to PCO, the Prime Minister’s Office (PMO), offices of Ministers and Parliamentary Secretaries supported by PCO, and Commissions of Inquiry during the scope period. This line of inquiry also included support provided by PCO to the Prime Minister in establishing candidates' fitness for office for public office positions.

Conclusions

Under the *Policy of Government Security* the Clerk, as PCO deputy head, is accountable for security in the department. This comprises the security of departmental personnel, including those who work in the Prime Minister's Office or offices of Ministers supported by PCO, as well as departmental information, facilities and other assets. Physical and personnel security examined for the audit are key components within this construct that includes security and emergency management.

Definition and documentation of roles, responsibilities, accountabilities and relationships have advanced greatly with development of a new *Security and Emergency Policy* that applies to PCO, PMO and offices of Ministers supported by PCO and creation of PCO's first Departmental Security and Emergency Management Plan (DSEMP). [*]

Effective committee oversight and meticulous planning by security officials has led to steady advancements in the area of performance measurement. A framework for measuring SEM performance has been developed and implementation is now underway. Management plans to continue with a phased approach, making adjustments as necessary, to fully operationalize their framework.

Security Operations Division has adopted, and is now implementing, a comprehensive risk management model that is consistent with Treasury Board Secretariat (TBS) and PCO risk frameworks. The approach to security risk management is well described in the DSEMP and features two interrelated phases including Risk Assessment and Risk Treatment. [*]

Appropriateness of physical security controls must be assessed in relation to management's tolerance for risk. We examined physical security initiatives, [*]. Some planned initiatives have been successfully implemented and previously identified vulnerabilities have now been addressed, while others are behind schedule, but on their way to full implementation. [*]

PCO is meeting most of the minimum requirements stated in the TBS *Personnel Security Standard*; [*] .

Recommendations

We recommend that the National Security Advisor to the Prime Minister, as the senior management lead for departmental security:

1. [*]
2. Identify all risk owners responsible to address PCO SEM risks enunciated in the DSEMP and document their formal evaluation and treatment decisions, including the rationale for their decisions. The Departmental Security Officer (DSO) should review all resulting evaluations and decisions for consistency with acceptable PCO risk tolerances. When situations arise where the DSO believes the risk owners are accepting residual risks that exceed acceptable PCO risk tolerances, the matter should be brought to an appropriate level up to and including the PCO Executive Committee for resolution.
3. [*]
4. [*]
5. [*]

We recommend that the Executive Director of Security Operations, as administrator of the Guidelines for Pre-Appointment Background Checks on Candidates for Certain Public Office Positions on behalf of the Clerk:

6. Review the process described in the Guidelines to ensure their consistent application to all positions identified therein.

Management Response

Management has accepted all recommendations. Their response and action plan are included at Section 3.0 in the body of this report.

Statement of Conformance

The audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada. A practice inspection has not been conducted.[1]

Original signed by Chief Audit Executive

_____

SIGNATURE OF CHIEF AUDIT EXECUTIVE
JIM HAMER
DIRECTOR, AUDIT AND EVALUATION

[1] An external practice inspection is underway and scheduled for completion in the fall 2013.

1.0 Introduction

1.1 Authority

The Audit of Physical and Personnel Security was approved by the Clerk as part of the Privy Council Office (PCO) Risk-Based Internal Audit Plan 2012-2013 to 2014-2015.

1.2 Objectives and Scope

The objectives of the audit were:

1. To assess the design and operating effectiveness of governance structures and processes for physical and personnel security;
2. To assess the adequacy of risk assessment processes for physical and personnel security;
3. To determine if appropriate physical security controls have been established and implemented to safeguard facilities, information and assets, and to comply with government policy; and
4. To determine if appropriate personnel security controls have been established and implemented to protect sensitive information and assets, and to comply with government policy.

The audit scope included physical and personnel security components of the PCO Security and Emergency Management (SEM) program administered by Security Operations Division (SECOPS). The period of audit coverage was July 2009 to October 2012, though subsequent events were also considered.

For purposes of the audit, we defined physical security as the use of physical safeguards, equipment or procedures to prevent or delay unauthorized access to assets, to detect attempted and actual unauthorized access and to activate appropriate responses. The audit included all facilities used by PCO regardless of ownership; a risk-based approach was used to select facilities and controls for audit testing.

The assessment of personnel security focused on processes for granting Reliability Status and security clearances at the SECRET and TOP SECRET levels. The population for audit testing included all arrivals to PCO, the Prime Minister's Office (PMO), offices of Ministers and Parliamentary Secretaries supported by PCO, and Commissions of Inquiry during the scope period. This line of inquiry also included support provided by PCO to the Prime Minister in establishing candidates' fitness for office for public office positions.

1.3 Background and Context

Good physical and personnel security are of particular importance for PCO because of the department's proximity to the centre of government both geographically and intellectually. Physical security controls protect PCO facilities and the people working in them, as well as the department's assets and information. The risks associated with PCO physical security are heightened because the Parliamentary Precinct and its surroundings, in which the department's operations are based, are vulnerable to a variety of threats and hazards. Personnel security is

significant due to the degree of access individuals working at PCO have to sensitive information; great reliance is placed on the trustworthiness and suitability of all individuals working at PCO.

From a policy perspective, under the Treasury Board *Policy on Government Security,* the Clerk, as PCO Deputy Head, is accountable for the effective implementation and governance of security within the department; this includes security of departmental personnel, information, facilities and other assets. Deputy heads are also responsible to appoint a departmental security officer (DSO) functionally responsible to the deputy head or departmental executive committee to manage the departmental security program. The Clerk has appointed the Executive Director of Security Operations, Security and Intelligence Secretariat, as the PCO's DSO.

Roles and responsibilities of employees who support deputy heads in the management of departmental security are defined, in a government-wide context, in the Treasury Board Secretariat (TBS) *Directive on Departmental Security Management*. The Directive outlines DSO responsibilities for managing the departmental security program including planning, governance, risk management, monitoring and oversight, and performance measurement and evaluation.

Baseline physical security requirements designed for common types of threats that departments would encounter are described in the TBS *Operational Security Standard on Physical Security.* Certain departments, like PCO, may face different threats because of the nature of their operations, their location and/or the attractiveness of their assets. Controls should be based on departmental requirements identified through risk assessment conducted by management. Physical security controls should incorporate identifiable elements of protection, detection, response and recovery. Please note that the latter element, recovery, was assessed during the 2011 Audit of Business Continuity and Emergency Preparedness and was therefore not included in the current audit.

Deputy heads of all departments are responsible for ensuring that all individuals who will have access to government information and assets, including those who work in or for offices of Ministers and Ministers of State, are security screened at the appropriate level before the commencement of their duties.[2] PCO policy further specifies that all individuals must have at least a SECRET security clearance, as a condition of employment. Individuals who require access to TOP SECRET information must have a TOP SECRET clearance before they can access such information. Specific requirements and recommended safeguards have been established for personnel screening in the TBS *Personnel Security Standard*. Additionally, as a lead security agency, PCO is responsible for supporting the Prime Minister in establishing candidates' fitness for office for public office positions and conducting security clearances for deputy heads.

1.4 Approach and Methodology

The audit began with a planning phase, conducted from July to October 2012, that included a review of relevant policies, directives and guidelines, interviews with SECOPS personnel and a preliminary examination of program information including the PCO Departmental Security and Emergency Management Plan (DSEMP) and results from a 2012 Threat, Vulnerability and Risk Assessment. Prior to moving into audit examination, the Chief Audit Executive communicated planning phase results with management and received their agreement with the detailed audit criteria.

[2] Policy on Government Security, 2009

Audit Criteria were sourced from TBS authorities including the *Directive on Departmental Security Management*, *Operational Security Standard on Physical Security*, *Personnel Security Standard* and *Audit Criteria related to Management Accountability Framework – A Tool for Internal Auditors* as well as *Policies for Ministers' Offices* and the PCO *Security and Emergency Management Policy*.

The examination phase, conducted from October 2012 to March 2013, included interviews with security officials and program managers from Human Resources and Administration Divisions; detailed examination of documentation and comparison against government and departmental policy and planned results; site visits to PCO facilities to observe physical security controls; quantitative analysis of personnel screening data; and sample testing of personnel security processes and procedures.

Two samples were developed for the audit objective pertaining to personnel security controls. The first was a random sample of 31 individuals who began working for PCO, PMO, offices of Ministers and Parliamentary Secretaries supported by PCO, or Commissions of Inquiry during the scope period. We subsequently expanded the sample by adding 5 names to enhance coverage of the 2012 period. The second sample included 35 Governor-in-Council appointees and other positions for which PCO is responsible to conduct pre-appointment background checks. The sample sizes were determined judgmentally to include all positions identified in the Guidelines; therefore, no attempts were made to draw statistical inferences about the populations.

At the end of the examination phase, audit results were validated with management and a draft report was prepared and sent by the Chief Audit Executive to senior management for response and development of action plans to address audit recommendations. Draft audit reports and management action plans are provided to PCO's Audit Committee for review and recommendation to the Clerk of the Privy Council for approval.

2.0 Findings, Conclusions, and Recommendations

This section is organized around the four audit objectives: 1) Governance, 2) Risk Assessment, 3) Physical Security Controls, and 4) Personnel Security Controls. For each audit objective we present the criteria that were agreed to by management followed by an overall conclusion for the objective and detailed findings aligned with the criteria statements. Recommendations are found at the end of this section.

2.1 Governance

Audit Objective: To assess the design and operating effectiveness of governance structures and processes for physical and personnel security.

To respond to the first audit objective, we looked for evidence to confirm that:

- *Accountabilities, delegations, reporting relationships, and roles and responsibilities of departmental personnel with physical and personnel security responsibilities are defined and documented;*
- *Effective security governance bodies are established to ensure the coordination and integration of physical and personnel security activities with broader SEM and departmental operations, plans, priorities and functions to facilitate decision making; and*
- *Management has identified and implemented appropriate performance measures linked to planned results.*

Conclusion

Under the *Policy of Government Security,* the Clerk, as PCO deputy head, is accountable for security in the department. This comprises the security of departmental personnel, including those who work in the PMO or offices of Ministers supported by PCO, as well as departmental information, facilities and other assets. Physical and personnel security examined for the audit are key components within this construct that includes security and emergency management.

Definition and documentation of roles, responsibilities, accountabilities and relationships have advanced greatly with development of a new *Security and Emergency Policy* that applies to PCO, PMO and offices of Ministers supported by PCO and creation of PCO's first Departmental Security and Emergency Management Plan. [*]

Effective committee oversight and meticulous planning by security officials has led to steady advancements in the area of performance measurement. A framework for measuring SEM performance has been developed and implementation is now underway. Management plans to continue with a phased approach, making adjustments as necessary, to fully operationalize their framework.

Findings

- **Accountabilities, Roles and Responsibilities**

In December 2012, the PCO *Security and Emergency Management Policy* came into effect, replacing the (2005) *Security Policy*. Among the updates are expanded descriptions of roles and responsibilities that are clearer and more extensive than in the former *Security Policy*. The breadth and depth of these newly documented responsibilities provide a much better picture of

who is responsible for what within PCO in the area of security and emergency management, including physical and personnel security.

The SEM governance structure is further described in the new PCO DSEMP. A graphical representation presents the governance structure in three levels: (1) the operational level – including SECOPS, divisions of the Corporate Services Branch (CSB), Corporate Management Advisory Committee and the Executive Director of SECOPS; (2) the senior management level – including the Assistant Deputy Minister, CSB, Offices of Primary Interest (OPIs) for PCO critical functions, and the Assistant Secretary to Cabinet, Security and Intelligence; and (3) the executive management level – including the National Security Advisor, PCO Executive Committee, the Clerk, and the Prime Minister's Office. Descriptions of program governance address all of these positions or entities with exception to the PMO, which is described solely in the context of a client for SEM services.

The Clerk has delegated the authority for granting security clearances to the Executive Director of Security Operations, in his role as DSO. [*]

Effective Committees

The roles of governance committees are well described in the DSEMP. Within the SEM framework, PCO Executive Committee oversees and approves security and emergency management programs. It is supported by the Corporate Management Advisory Committee, which addresses PCO corporate management priorities and initiatives by providing input and advice to directors on items presented, as well as recommendations to PCO Executive Committee to facilitate its decision making. The DSO and SECOPS team provide the Corporate Management Advisory Committee with debriefs and updates on ongoing issues as well as products, such as the DSEMP and new *Security and Emergency Management Policy*, before they go to Executive Committee or the Clerk for decision.

Additionally, the DSO provides regular updates to the PCO Departmental Audit Committee; over the past year, these have included reports on development of the DSEMP and ongoing security initiatives.

The Corporate Risk Profile provides Executive Committee with regular information on risks that could hinder the achievement of PCO's activities and strategic outcomes. It is also intended to communicate risk mitigation strategies and the degree of management attention required for areas of identified risk. [*] The high-level view of security risk presented in the Corporate Risk Profile combined with the detailed perspective found in the DSEMP provides Executive Committee with good information on these risk areas.

Performance Measurement

In the 2011 Audit of Business Continuity and Emergency Preparedness, we reported that performance measurement (in the emergency management domain) was quite basic. Some performance data was being collected and reported periodically, but performance measurement was in its early stages. We applauded what had been done and encouraged continued progress; management responded positively to the audit recommendation. The DSEMP discusses SECOPS' current approach to Integrated Results-based Management (IRBM), inclusive of performance measurement, in a way that demonstrates a level of maturity that has come about from close management attention:

> "An IRBM approach focuses on achieving functional outcomes (immediate, intermediate and ultimate), through: (1) the development of a logic model; (2) the measurement of selected and well-designed qualitative and quantitative indicators, both lagging and leading; (3) the implementation of feedback loops for the purpose of learning and improving the overall program through preventive and corrective measures; and (4) the formalization of monitoring and reporting mechanisms to demonstrate the results achieved."
>
> -- PCO Departmental Security and Emergency Management Plan, 2012

In 2011, SECOPS developed a performance measurement framework for the division. While not specific to physical and personnel security, the framework does capture these functions within its scope. It includes information on SECOPS' strategic objectives, a logic model, and a performance measurement strategy. Quantitative performance indicators have been developed for a series of elements that are in turn linked to the three angles[3] from which performance will be measured. The design of the framework is quite complex and becomes separated from the logic model making it difficult to draw linkages between performance indicators and intended outcomes; however, the true test will come through implementation.

SECOPS is taking a prudent, phased approach to implement its IRBM framework for the overall departmental SEM program. To date, performance indicator analysis has been more qualitative than quantitative as they develop the capacity for data collection. Looking forward, SECOPS plans to build on progress already achieved; during 2013-2014 they plan to use the performance indicators to prepare an annual report – expected in April 2014. In the final phases of their multi-year implementation plan, management intends to review the indicators developed to ensure they are still relevant to desired results and use the information to assess the organization's overall improvement – focusing on closing gaps between capabilities and vulnerabilities.

[3] The three angles include (1) clients, (2) SECOPS teams, and (3) four performance measurement perspectives (operational readiness, knowledge leveraging, human capital and relationship management).

2.2 Risk Assessment

Audit Objective: To assess the adequacy of risk assessment processes for physical and personnel security.

To respond to the second audit objective, we looked for evidence to confirm that management:

- *Identifies & documents a comprehensive inventory of physical and personnel security risks;*
- *Assesses the risks it has identified (likelihood and impact);*
- *Formally responds to its risks (risk treatment decisions); and*
- *Identifies control objectives for each risk determined to be "unacceptable" and for which the selected treatment is to reduce the risk.*

Conclusion

SECOPS has adopted, and is now implementing, a comprehensive risk management model that is consistent with TBS and PCO risk frameworks. The approach to security risk management is well described in the DSEMP and features two interrelated phases including Risk Assessment and Risk Treatment. [*]

Findings

- **Risk Identification**

Between 2009 and 2011 SECOPS undertook a number of studies that provided a great deal of data [*] Also in 2011, Security Operations conducted a Risk Assessment for the SECOPS Division. Though the focus of this risk assessment was on the division rather than the department, it demonstrated a positive shift in the way risk was being considered by featuring a risk register that identified physical and management risks facing SECOPS including discussion of the assets at risk, threats or hazards, probability of occurrence, and the risk owner.

Early in 2012, with support from external experts, SECOPS undertook a landmark Threat, Vulnerability and Risk Assessment (TVRA) with the stated purpose to identify and validate a consolidated list of critical assets and activities and the full array of threats and hazards and risks facing PCO and its operations. The TVRA work included broad consultation within PCO and produced an updated risk register [*]

Recognizing the challenge, SECOPS began work internally in mid-2012 to revise and simplify the risk register in order to consolidate and build on information obtained during the TVRA as well as other threat and risk assessments and security reviews conducted in recent years. [*]

- **Assessment of Likelihood and Impact**

[*]

The risk assessment builds on analysis performed by the consultant team that conducted the TVRA; the latest version was prepared by SECOPS division managers and analysts including representation at the Director and Executive Director level. The analysis was informed by the

expertise of multiple division managers in weekly team meetings, an approach which had not previously been undertaken.

Risk Treatment Decisions

The risk management model described in PCO's DSEMP includes risk evaluation; i.e.: determination if risks are acceptable or not acceptable, as a key step in the risk assessment process. Using this lens, SECOPS has evaluated each of the identified risks. All risks include a brief explanation as to why each was deemed "Treat" or "Accept". Additionally, the risk register identifies those risks that are 2013-2014 treatment priorities and indicates if additional resources will be required to mitigate each risk.

[*] Under the TBS *Directive on Departmental Security Management*, the DSO is responsible for ensuring that managers at all levels formally accept or recommend for acceptance residual risks as defined in the DSEMP.

[*]

Control Objectives

The TBS *Directive on Departmental Security Management* includes 56 minimum security control objectives departments are required to achieve – 6 are under the heading Physical Security and 5 are under Individual Security Screening [Personnel Security]. These control objectives are useful for the whole of government approach to managing security in that they provide consistent minimum expectations for all departments covered by the Directive, but they are generic in nature and do not necessarily address the risks identified by PCO. Additional department specific security control objectives are to be selected and implemented based on the results of risk assessments.

The purpose of having PCO specific control objectives is well stated in the DSEMP – "security control objectives define the desired result or purpose to be achieved by treating security risks. They guide the selection of controls (including measures and safeguards) to treat the risk, and help define performance indicators to measure achievement of the objective." The SEM risk management model being implemented by SECOPS does include definition of control objectives as one of the next steps in the process, but this step is yet to be completed. However, given the strong progress demonstrated to date with the risk assessment process, security officials are now well positioned to identify appropriate, departmental specific control objectives and fully implement their risk management model.

2.3 Physical Security Controls

Audit Objective: ***To determine if appropriate physical security controls have been established and implemented to safeguard facilities, information and assets, and to comply with government policy.***

To respond to the third audit objective, we looked for evidence to confirm that:

- *PCO employs appropriate protection, detection and response controls to protect information, assets and facilities;*
- *Access to assets and facilities is limited to authorized individuals;*
- *Custodian-tenant relationships are defined in formal agreements to achieve optimum security outcomes; and*
- *Security considerations are fully integrated into facility planning processes.*

Conclusion

Appropriateness of physical security controls must be assessed in relation to management's tolerance for risk. We examined physical security initiatives, [*] Some planned initiatives have been successfully implemented and previously identified vulnerabilities have now been addressed, while others are behind schedule, but on their way to full implementation. [*]

Findings

[*]

For the first line of inquiry under this audit objective, we examined [*]

[*]

PCO has well documented access card procedures that address the responsibilities of managers and employees alike. [*] Documented procedures have also been developed for employees expecting visitors and for contractors [*]

Documented standard operating procedures have been developed by SECOPS for issuing access cards including procedures for granting individuals' access rights [*]. Communiqués are routinely sent to employees to inform them of how and when to renew their access card, how it should be displayed, etc. [*]

- **Formal Custodian-Tenant Security Agreements**

As identified in the TBS *Directive on Departmental Security Management*, custodian-tenant relationships are to be defined in formal agreements that ensure shared and individual responsibilities are addressed to achieve optimum security outcomes. Through these agreements, PWGSC, as the custodian, and PCO, as the tenant, would collaborate in identifying physical/base-building security requirements and formalize how these would be addressed in a

way that would clarify respective roles, funding arrangements, controls and plans for implementing controls and managing risk.

Formal Occupancy Instruments are established between PCO and PWGSC that outline services that would normally be provided for PCO occupied space. The descriptions of services offered in these agreements, however, are generic in nature and do not discuss security provisions beyond the custodian providing “building security in accordance with applicable standards and practices”.

[*]

2.4 Personnel Security Controls

Audit Objective: ***To determine if appropriate personnel security controls have been established and implemented to protect sensitive information and assets, and to comply with government policy.***

To respond to the fourth audit objective, we looked for evidence to confirm that:

- *All individuals have a SECRET security clearance, as a minimum, prior to assuming their duties;*
- *An efficient process exists to process security updates;*
- *Individuals are formally briefed on access privileges;*
- *Individuals are treated in a fair manner should their security screening status come under review, be revoked, denied, temporarily suspended or downgraded for cause;*
- *Security screenings are conducted in a manner that meets Government of Canada standards; and*
- *PCO has established an effective process to support the Prime Minister in establishing candidates' fitness for office for public office positions*

Conclusion

PCO is meeting most of the minimum requirements stated in the TBS *Personnel Security Standard*; [*]

Findings

[*]

Efficiency of the Security Update Process

For the audit, we focused on cycle time as the measure of efficiency of the security update process. The TBS *Personnel Security Standard* does not specify how long security clearance updates should take to complete, so we took a “reasonableness approach”, i.e.: determine how long it takes to conduct security updates and assess whether that delay is reasonable given the work involved. Basically, the process should be efficient enough to enable security clearance updates to be completed before the end of the update cycle.

[*]

Formal Briefing on Access Privileges

The principal document used to provide evidence that an individual has been briefed on his or her security screening is the standard Security Screening Certificate and Briefing Form. This form, used throughout the Government of Canada, includes a briefing summary that is to be read and acknowledged by signature of the individual indicating they understand and agree to comply

with the statutory and administrative requirements described therein. The form is then to be signed and dated by the security official who conducted the briefing.

[*]

Fair Treatment

[*]

[*] specifically addressed in the PCO *Security and Emergency Management Policy*, which states:

> "If adverse information of a serious enough nature is identified as a result of the checks, the individual must be given an opportunity to explain the information before a decision is reached. The Clerk of the Privy Council is the only person with authority to deny, temporarily suspend, downgrade for cause or revoke a security clearance for someone employed or being considered for employment with PCO. Individuals whose security clearance is denied or revoked must be advised of their rights of review or redress."

The above is entirely consistent with requirements in the Treasury Board *Policy on Government Security*. Additionally, the security official interviewed had a good understanding of the requirements and how they should be applied should this situation be encountered.

Compliance with Government of Canada Standards

[*]

The TBS *Personnel Security Standard* indicates that field investigations are mandatory for initial personnel screening processes for TOP SECRET clearances and optional for updates based on subject interviews or checks. [*]

Support for establishing candidates' fitness for office for public office positions

PCO has documented guidelines titled "Guidelines for Pre-Appointment Background Checks on Candidates for Certain Public Office Positions" with the stated purpose to assist the Prime Minister in ensuring that there are no criminal, security or other concerns which could affect the suitability of candidates for certain public office positions. The current Guidelines are effective July 1, 2010; replacing the previous 2006 version. The Guidelines identify positions requiring pre-appointment background checks as well as the procedures for the conduct of these checks and the reporting on their results. Separate guidelines have been issued for Justice Canada checks of candidates for judicial positions subject to the *Judges Act*.

The Executive Director of Security Operations is responsible for the administration of the PCO guidelines on behalf of the Clerk. The PMO, or for certain appointments, PCO Senior Personnel are responsible for requesting and ensuring completion of background checks before any appointment to a position within the scope of the guidelines is made.

Depending on the position, pre-appointment checks could include two, three, or all four of the following: Royal Canadian Mounted Police (RCMP) police records check, CSIS security assessment, Office of the Superintendent of Bankruptcy (OSB) bankruptcy and insolvency check, and Canada Revenue Agency (CRA) compliance check.

[*]

A four-way check has also been required for the spouses or partners of candidates being considered for appointment as Minister, Minister of State or Parliamentary Secretary since the Guidelines were updated in 2010. [*]

2.5 Recommendations

We recommend that the National Security Advisor to the Prime Minister, as the senior management lead for departmental security:

1. [*]
2. Identify all risk owners responsible to address PCO SEM risks enunciated in the DSEMP and document their formal evaluation and treatment decisions, including the rationale for their decisions. The DSO should review all resulting evaluations and decisions for consistency with acceptable PCO risk tolerances. When situations arise where the DSO believes the risk owners are accepting residual risks that exceed acceptable PCO risk tolerances, the matter should be brought to an appropriate level up to and including the PCO Executive Committee for resolution.
3. [*]
4. [*]
5. [*]

We recommend that the Executive Director of Security Operations, as administrator of the Guidelines for Pre-Appointment Background Checks on Candidates for Certain Public Office Positions on behalf of the Clerk:

6. Review the process described in the Guidelines to ensure their consistent application to all positions identified therein.

3.0 Management Response and Action Plan

Audit of Physical and Personnel Security
The National Security Advisor to the Prime Minister has overall accountability for the Action Plan.

Recommendation	Response and Planned Actions	Responsibility	Due Date
We recommend that the National Security Advisor to the Prime Minister, as the senior management lead for departmental security:			
1. [*]	[*]	[*]	[*]
2. Identify all risk owners responsible to address PCO SEM risks enunciated in the DSEMP and document their formal evaluation and treatment decisions, including the rationale for their decisions. The DSO should review all resulting evaluations and decisions for consistency with acceptable PCO risk tolerances. When situations arise where the DSO believes the risk owners are accepting residual risks that exceed acceptable PCO risk tolerances, the matter should be brought to an appropriate level up to and including the PCO Executive Committee for resolution.	[*]	Executive Director, Security Operations Division	[*]

Recommendation	Response and Planned Actions	Responsibility	Due Date
3. [*]	[*]	[*]	[*]
4. [*]	[*]	[*]	[*]
5. [*]	[*]	[*]	[*]
We recommend that the Executive Director of Security Operations, as administrator of the Guidelines for Pre-Appointment Background Checks on Candidates for Certain Public Office Positions on behalf of the Clerk:			

Recommendation	Response and Planned Actions	Responsibility	Due Date
6. Review the process described in the Guidelines to ensure their consistent application to all positions identified therein.	[*]	Executive Director, Security Operations Division	[*]