Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Horizontal Internal Audit of Physical Security in Large and Small Departments

Published: 2020-09-28

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-57/2020E-PDF
ISBN: 978-0-660-36854-2

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Audit interne horizontal de la sécurité matérielle dans les grands et petits ministères

Horizontal Internal Audit of Physical Security in Large and Small Departments

From Treasury Board of Canada Secretariat

Notice to readers

This report contains confidential information, or information related to security, which has been redacted in accordance with the *Access to Information Act*.

July 2020

Office of the Comptroller General

On this page

Executive summary

▶ In this section

The objectives of this audit were to determine whether the following were in place: [1]

- government-wide and departmental governance frameworks supporting physical security
- departmental processes supporting the development, implementation, update and monitoring of physical security controls

The scope of the audit focused on frameworks and processes in place as at June 30, 2017. At the end of the examination phase, detailed findings were communicated to all participating departments. However, the issuance of this report was delayed due to unforeseen operational priorities that resulted in audit resources having to be temporarily reassigned to other projects. To help ensure the continued relevance of findings and recommendations in the current context, the audit also considered government-wide initiatives undertaken between June 30, 2017, and January 31, 2020 (such as the issuance of a renewed Treasury Board security policy framework effective July 2019).

Why this is important

Recent security events [2] around the world underscore the importance of having effective physical security in place to help adequately protect individuals, information and assets. [Redacted], protesters gaining access to National Energy Board [3] hearings and various Indigenous and Northern Affairs Canada [4] offices in 2016,

and the Parliament Hill shooting in 2014 [5] show that Canada is not immune to security threats. [6]

The Government of Canada employs approximately 220,000 individuals within the core public administration, [7] manages more than $86 billion in non-financial assets, [8] and owns or leases over 38,000 buildings. [9] While different government departments may face different threats depending on their operations, locations and assets, all federal departments could potentially face significant injuries in terms of the loss of confidentiality and integrity, and the unavailability of employees, information and assets if physical security were to be compromised. [10] The repercussions could be further compounded by the increasing interdependencies between departments, such as reliance on internal enterprise services or co-location.

In this context, comprehensive and strongly integrated governance frameworks, and departmental processes supporting physical security are key to helping adequately protect government employees, information and assets from compromise.

Key findings

Governance frameworks over physical security

The audit found that, overall, governance frameworks for physical security were in place at the government-wide and departmental levels. However, there are several opportunities for improvement at both levels.

Government-wide policy direction on physical security was established in the Treasury Board security policy framework. This framework was supported by technical guidance issued by the Royal Canadian Mounted Police (RCMP), as the lead security agency for physical security. While the Treasury Board security policy framework was renewed in 2019, and similar work is in progress to renew some of the RCMP's technical guidance, the audit noted that it took several years to complete these updates. In departments, roles and responsibilities were generally defined for employees with physical security-related responsibilities, often through departmental security policies. However, opportunities to improve the

communication, approval and maintenance of roles, responsibilities and reporting relationships were noted in most departments.

Several interdepartmental committees were in place and actively supported physical security. The majority of departments also established governance committees to provide oversight in this area. However, the tracking and follow-up of committee decisions were not done consistently by some committees at both the government-wide and departmental levels. Additionally, an opportunity was identified for greater collaboration among the different interdepartmental committees.

At the government-wide level, mechanisms have been put in place for the strategic planning of lead security agency initiatives supporting physical security; however, strategic plans were not finalized. While lead security agencies have undertaken initiatives to support departments in the area of physical security, services related to base building security [11] could be improved. Planning of physical security initiatives at the departmental level is done through departmental security plans (DSPs), which had been developed and approved in all departments. However, these plans were generally not fully aligned with the Treasury Board of Canada Secretariat's (the Secretariat) guidance and were not periodically maintained.

Finally, the audit noted that while the Secretariat did monitor and report on departments' compliance with some physical security-related policy requirements through its Management Accountability Framework (MAF) assessments, these assessments did not provide a broad government-wide view or assess the effectiveness of the policy instruments. However, work is underway to address these gaps. Additionally, monitoring and reporting frameworks over physical security in departments were either not in place or were limited.

Departmental physical security processes

Departments are required to define, document, implement, assess, monitor and maintain physical security practices and controls in alignment with the "Mandatory Procedures for Physical Security Control" appendix to the *Directive on Security Management*. This includes the completion of security assessments, such as threat and risk assessments (TRAs); [12] implementation of physical security controls to

restrict access to facilities and detect attempted or actual breaches; and processes to report, investigate and implement corrective actions resulting from security incidents.

Although all departments completed TRAs or equivalent assessments, [Redacted]. Most departments had a process in place to identify and implement physical security controls, [Redacted]. Furthermore, while processes to report security incidents were in place in most departments, processes to investigate security incidents and report the results were not in place in some departments.

Conclusion

Overall, the audit noted a need for improvements to the government-wide and departmental governance frameworks, and to physical security processes within departments.

Although lead security agencies have fulfilled their basic responsibilities in supporting physical security at the government-wide level, several opportunities for improvements were noted with respect to:

- updating policy instruments
- services relating to base building security
- coordination and operations of interdepartmental governance committees
- strategic planning of lead security agency priorities
- monitoring and reporting frameworks

Within departments, there were also several opportunities for improving physical security governance frameworks:

- the level of involvement of governance committees
- communication of roles and responsibilities (especially in regional offices)
- maintenance of DSPs and their alignment with the guidance issued by lead security agencies
- monitoring and reporting frameworks

Finally, [Redacted] gaps were identified in departmental physical security processes:

- [Redacted]
- [Redacted]
- [Redacted]
- reporting of incidents
- investigation of incidents
- follow-up on recommendations from past investigations

Conformance with professional standards

This internal audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

Mike Milito, MBA, CIA, CRMA
Assistant Comptroller General and Chief Audit Executive
Internal Audit Sector, Office of the Comptroller General

Background

▶ In this section

Physical security in the Government of Canada

Physical security, as one of eight security controls [13] within the broader area of government security, aims to provide reasonable assurance that individuals, information and assets are adequately protected, thereby supporting the delivery of government programs, services and activities. This is achieved by defining, documenting, implementing, assessing, monitoring and maintaining physical security requirements, practices and controls throughout all stages of the real property and materiel management life cycles.

More specifically, physical security refers to the use of security controls [14] (entrance gates at government offices, security guards, locked filing cabinets, cameras, alarms, and so on) to prevent or delay unauthorized access to employees,

information and assets, and to detect and report attempted or actual unauthorized access.

Physical security relies on and complements other aspects of a departmental security function. Ultimately, to be effective in protecting individuals, information and assets, physical security controls need to be tailored to departments and integrated with the other security controls outlined in the Treasury Board *Policy on Government Security*. For instance, the effectiveness of entrance gates controlling access to government facilities depends on the integrity of the process for issuing access cards only to individuals with appropriate security clearance (security screening). In turn, the effectiveness of other security controls, such as information technology security, relies on the adequacy of physical security safeguards (such as effectively restricting access to server rooms). Similarly, the success of a departmental and/or government-wide response to certain security incidents or events (security event management) relies on the effectiveness of physical security safeguards (cameras, alarms, security guards, and so on) to detect such incidents or events and report them in a timely manner to the appropriate authorities.

Although responsibility for departmental physical security rests ultimately with deputy heads, it should be noted that responsibility for the security of government as a whole is shared among several stakeholders (central agency, lead security agencies, internal enterprise service organizations [15] and departments).

Lead security agencies have a leadership and support role in relation to government security and contribute to the achievement of government security policy objectives. While their specific responsibilities vary, lead security agencies also share responsibilities for providing advice, guidance and services to support departmental security operations.

The main lead security agencies responsible for supporting physical security [16] are:

- the Treasury Board and its Secretariat for their policy roles as a central agency
- the Royal Canadian Mounted Police (RCMP) as the lead security agency for physical security

- Public Services and Procurement Canada (PSPC) for its role in providing base building security [17] as an internal enterprise service organization
- the Privy Council Office (PCO) for its national security role

Policy framework for physical security

The Treasury Board security policy framework, which sets out requirements for physical security, aims to ensure that deputy heads effectively manage security activities within departments, while also contributing to the effective management of government-wide security. During the audit, the Treasury Board of Canada Secretariat (the Secretariat) renewed this framework and streamlined the policy instruments to provide greater flexibility to departments. [18] Upon review, it was determined that the renewed policy framework does not negate the requirements of the previous policy framework, on which this audit was based. [19]

The renewed Treasury Board security policy framework took effect on July 1, 2019, and includes the following instruments relevant to physical security:

- the Treasury Board's *Policy on Government Security*
- the Secretariat's *Directive on Security Management* (includes "Mandatory Procedures for Physical Security Control")

Per the renewed *Policy on Government Security*, responsibility for providing leadership, advice and guidance on matters relating to physical security remains with the RCMP. In alignment with this responsibility, the RCMP issued physical security technical guidance between 1998 and 2014 to supplement the Treasury Board security policy framework and support departmental security operations. [20] The RCMP is in the process of updating some of its guidance to align with the recently renewed Treasury Board security policy framework.

Audit objectives and scope

The objectives of this audit were to determine whether the following were in place: [21]

- government-wide and departmental governance frameworks supporting physical security
- departmental processes supporting the development, implementation, update and monitoring of physical security controls

The scope of the audit focused on frameworks and processes in place as at June 30, 2017. At the end of the examination phase, detailed departmental findings were communicated to each participating department. However, the issuance of this report outlining horizontal findings and recommendations was delayed due to unforeseen operational priorities that resulted in audit resources having to be temporarily reassigned to other projects. To help ensure the continued relevance of this report in the current context, government-wide initiatives undertaken by lead security agencies between June 30, 2017, and January 31, 2020, were considered during the reporting phase (such as the issuance of a renewed Treasury Board security policy framework).

Given the previously mentioned delay, some of the participating departments may have since addressed the findings and recommendations presented in this report. Any progress made in this regard is to be reflected and tracked in departmental management action plans.

The lines of enquiry and criteria for this audit were initially developed with reference to the Treasury Board security policy framework in place as at June 30, 2017. In order to ensure their continued relevance for the purpose of this report, these lines of enquiry and criteria have also been mapped to the renewed Treasury Board security policy framework. [22] While the new policy framework has streamlined security requirements to provide departments with greater flexibility, it was determined that most of the underlying requirements related to physical security that formed the basis of the audit criteria were still relevant. However, new requirements introduced in the revised policy framework, such as the requirement for departments to implement facility security assessment and authorization processes, were not examined by the audit.

The elements of governance examined were:

- policy frameworks
- committees and organizational structures
- strategic planning at the government-wide level
- lead security agency services to support departments
- interdepartmental coordination and collaboration processes
- departmental roles and responsibilities
- departmental security planning
- monitoring and reporting

The departmental physical security processes examined were:

- conduct and maintenance of threat and risk assessments (TRAs)
- implementation of physical security controls and detection measures
- training and tools
- reporting and investigation of physical security incidents

The audit did not assess or test the actual physical security controls within departments themselves (alarm systems, key pads, turnstiles, and so on), but rather examined the processes in place to implement and maintain these controls, including processes to monitor their effectiveness.

Information management, information technology security and business continuity management were excluded from the audit scope, as other Office of the Comptroller General (OCG) horizontal audits have covered these areas. Security screening, security event management, security requirements associated with contracts and other arrangements, and occupational safety and health were also excluded from the audit scope given their unique nature, complexity and risks. [23] The need for audit coverage in these areas will continue to be considered as part of the OCG's annual risk-based internal audit planning process.

Appendix B lists the departments and lead security agencies included in the audit.

Appendix C outlines the lines of enquiry and related audit criteria used to conclude on the audit objectives.

Findings and recommendations

▶ In this section

Finding 1: Governance at the government-wide level

Effective security governance, both within departments and across government, is one of the expected results of the Treasury Board *Policy on Government Security*. Under this policy, the Secretariat is responsible for establishing government-wide security policy governance. This involves setting strategic direction and priorities, and coordinating security priorities, plans and activities government-wide. Lead security agencies share responsibility for participating in government-wide security policy governance (including providing policy implementation advice to departments). Lastly, internal enterprise service organizations are responsible for establishing governance to oversee security considerations for the internal enterprise services they provide.

Given the complexity of federal government operations, the various stakeholders involved, the shared accountabilities and the variety of threats and risks faced by departments, having clearly defined and integrated government-wide governance is key to effectively coordinating physical security activities.

The audit examined whether the Secretariat, and the selected lead security agencies and internal enterprise service organizations, carried out their physical security governance responsibilities under the *Financial Administration Act* and the *Policy on Government Security*. At the government-wide level, the audit focused on the following aspects of governance: policy instruments, initiatives supporting departments, committee structures, strategic planning, and monitoring and reporting frameworks.

Policy instruments were issued by both the Secretariat and the RCMP to provide government-wide direction on physical security. After several years, the Secretariat's instruments were recently renewed and work is now in progress to update the RCMP's technical guidance.

Pursuant to its mandated responsibilities, the Secretariat published policy instruments on its website to support a whole-of-government approach to physical security. During the audit, the main instruments developed by the Secretariat to provide government-wide direction on the roles, responsibilities and requirements for physical security included the *Policy on Government Security*, the *Directive on Security Management* (in effect as of July 2019), including the "Mandatory Procedures for Physical Security Control", the *Directive on Departmental Security Management* (now archived) and the *Operational Security Standard on Physical Security* (now archived).

At the time of the audit fieldwork, the Treasury Board security policy framework had not been updated in several years. The main reasons raised by the Secretariat's representatives to explain this included the need for a detailed analysis to increase the clarity of requirements, the need to re-align with emerging new priorities (including the new *Policy on Service and Digital*) and a change in senior management at the Secretariat. The Secretariat was, however, in the process of renewing this framework and completed this major undertaking during the reporting phase of the audit in 2019. As part of the process, the Secretariat sought input from various stakeholders across the government's security community, including from small departments, interdepartmental governance committees, other lead security agencies and internal enterprise service organizations. Consultation drafts of the policy instruments were also made widely accessible on the federal government's intranet (GCpedia) throughout the process in an effort to engage with departments and help them prepare for the transition.

During the transition to the new Treasury Board security policy framework, there is as an inherent risk that its new and streamlined requirements may not be appropriately implemented by departments. Representatives interviewed at the Secretariat are aware of this and mentioned that work is underway to issue change management guidance in support of the physical security requirements currently in effect.

In alignment with its responsibilities under the *Policy on Government Security*, the RCMP, as the lead security agency for physical security, also published several physical security-related technical guidelines on its website. However, similar to the Secretariat's policy instruments, these had not been updated in recent years, with one in particular having been issued two decades ago. Several departments included in the audit raised this as an issue, and RCMP representatives interviewed explained that the department's limited capacity to perform its lead security agency role was the main challenge in this regard. Work is currently underway to update the Security Equipment Guide, which the RCMP deems as the most needed physical security technical guidance by the security community. Additionally, representatives from the RCMP indicated that a strategic plan is being developed for a planned review and update of all of its physical security technical guidance.

Having up-to-date government-wide physical security policy instruments and technical guidance that are broadly communicated, harmonized and regularly maintained to address the needs of stakeholders would reduce the risk that roles, responsibilities, expectations and requirements are not clearly understood and implemented. This would in turn increase the federal government's readiness and resilience to disruptions.

Recommendations: Government-wide policy instruments

1. The Secretariat and the RCMP should establish formal mechanisms to help ensure that their respective government-wide policy instruments supporting physical security will be periodically reviewed and updated in a timely manner going forward.
    - For example, such mechanisms could include a formally approved plan or strategy outlining the process, roles, responsibilities and timelines to review and update policy instruments, and an assessment of capacity to support the completion of reviews and updates. Linking such plans to performance agreements and/or to the forward agenda of a governance committee could in turn help ensure that these plans will be implemented
2. The Secretariat and the RCMP should:

a. in consultation with the government security community, assess and prioritize government-wide needs for change management guidance (while respecting individual departmental operating contexts) to help ensure the effective implementation of the renewed physical security requirements under the Treasury Board security policy suite currently in effect
b. issue supplementary guidance required to meet these needs

To complement government-wide security policy instruments, lead security agencies also provided support to departments in the area of physical security. Support relating to base building security [24] could be improved in terms of maintenance of TRAs, [25] and consultation in identifying risks, needs and priorities.

In addition to providing formal technical advice and guidance, lead security agencies also share responsibility for providing services to support the day-to-day security operations of departments (see Appendix E).

To fulfill this responsibility, lead security agencies undertook various general security initiatives related to physical security. For example, the Secretariat, PSPC and the RCMP all provided day-to-day support to departmental security operations (including physical security) by answering enquiries through generic email accounts established for this purpose. On an ad hoc basis, the Secretariat also reviewed and provided feedback on departmental security plans (DSPs) (which include physical security measures) upon request by departments. Through its Security Centre of Excellence, [26] PCO conducted briefings with newly-appointed security professionals to inform them of its various initiatives that support security government-wide. Additionally, the Secretariat indicated that its Security Policy Division meets with newly appointed chief security officers to apprise them of their policy responsibilities. To support the security functional community, annual security summits (covering physical security-related topics in some years) were held and co-hosted by the Secretariat, PCO and Public Safety Canada. These events aimed at raising awareness of new security initiatives, sharing knowledge and providing security practitioners across government with an opportunity to network.

Regarding base building security, PSPC has provided several internal enterprise services to support departments in this area; however, opportunities for improvements were identified. In alignment with its mandated responsibilities, PSPC managed the procurement of security guard services, established a generic email address to interact with members of the security community who have questions or need to alert PSPC of incidents in buildings, and completed base building TRAs. However, the audit noted that although PSPC has implemented mechanisms to track the completion of base building TRAs, there were instances where the TRAs were not updated at the department's expected frequency (every five years). [Redacted] Representatives from PSPC indicated that some base building TRAs require updates more frequently than others and that a new risk-based model is currently being implemented to improve the planning of updates. Furthermore, representatives interviewed in some of the departments included in the audit mentioned having experienced challenges in obtaining copies of base building TRAs for their facilities. Departments need the information from PSPC's base building TRAs to inform the development of their own TRAs. PSPC representatives indicated that a presentation has since been provided to inform the security community that copies of TRAs could be obtained by contacting PSPC's Base Building Security Operations group through its generic email for community outreach and TRA enquiries. At the time of the audit, PSPC did not demonstrate having put in place an ongoing process to ensure that departments are consistently made aware of its various services and of the mechanisms available to collaborate on base building security matters (such as how to obtain a copy of a base building TRA). PSPC also did not demonstrate having consulted with other government departments and lead security agencies in identifying risks and priorities related to base building security.

In a context where requirements have now been significantly streamlined, departments will likely increasingly rely on the services, advice and guidance provided by lead security agencies to help them navigate the new flexibilities provided within the higher-level requirements of the renewed Treasury Board security policy framework.

Recommendations: Enabling services supporting departments in the area of physical security

3. PSPC should continue to consult regularly with client departments and other lead security agencies to identify base building security risks, needs and priorities.
4. PSPC should finalize the implementation of its risk-based approach for conducting and regularly maintaining base building TRAs.

Interdepartmental security governance committees were in place and actively supported physical security. Committee operations could be further enhanced.

In a complex organization such as the federal government, where multiple stakeholders share various responsibilities to ensure adequate physical security, interdepartmental governance is key to effectively coordinating efforts. The Secretariat and the RCMP share the main responsibilities for establishing government-wide governance in this area (see Appendix E).

Both the Secretariat and the RCMP have established interdepartmental governance committees supporting a whole-of-government approach to physical security. The Secretariat, on the one hand, established policy governance committees with broad mandates to provide direction supporting the *Policy on Government Security*. Its committee at the assistant deputy minister level is co-chaired by PCO. [27] The RCMP, on the other hand, established an Advisory Committee on Physical Security (ACOPS), a working-level committee dedicated exclusively to providing government-wide support for physical security. All of these committees demonstrated their support to a whole-of-government approach for physical security through periodic discussions. For example, ACOPS presented several updates on its activities to the Secretariat's and PCO's policy governance committees.

Opportunities for improvements were identified in the way the previously mentioned committees operate. Some of these committees did not demonstrate that they consistently tracked and followed up on their decisions. Regarding ACOPS, no documentation was found supporting the approval of its terms of reference, nor

demonstrating that roles and responsibilities were defined for and communicated to its various working groups. Additionally, there was limited representation of small departments in the membership of all of these committees for a number of reasons. The Secretariat was aware of this and indicated that work was underway to address this issue in collaboration with representatives of small departments. Finally, some representatives of lead security agencies interviewed indicated that increased coordination among the interdepartmental security governance committees (for example, through regular status updates on physical security activities) would be beneficial.

Having formally approved and documented terms of reference in place for all governance committees that clearly define their respective mandates, roles, responsibilities and accountabilities could help the various stakeholders involved collaborate more effectively and efficiently. Also, consistently tracking and following up on committee decisions help ensure that they will be implemented as intended. Finally, stronger coordination between the governance committees could result in synergies, which may in turn further enhance physical security across government.

Recommendations: Interdepartmental governance committees

5. The Secretariat and the RCMP should ensure that their security governance committees regularly coordinate their government-wide physical security activities (such as through periodic status updates).
6. The Secretariat and the RCMP should ensure that the governance committees they are responsible for with respect to government-wide physical security consistently track and follow up on their decisions and initiatives.
7. The Secretariat and the RCMP, with the collaboration of relevant interdepartmental small department governance committees (such as the Heads of Federal Agencies committee), should jointly assess the membership of the various governance committees supporting government-wide physical security to ensure adequate representation of small departments.
8. The RCMP should ensure that its governance committees (including working groups) supporting government-wide physical security have formally approved

and documented terms of reference that clearly define their respective mandates, roles, responsibilities and accountabilities. These terms of reference should also be communicated to all relevant governance committee members.

Foundational mechanisms were established to strategically plan government-wide initiatives supporting physical security; however, strategic plans were not finalized.

The Secretariat is responsible for establishing government-wide security policy governance to set strategic direction and priorities. This includes ensuring the coordination of government security priorities, plans and activities. All the lead security agencies are expected to participate in this process. In particular, the RCMP was designated as the lead security agency specifically responsible for providing leadership on matters related to physical security.

In alignment with its responsibilities, the Secretariat established the Government of Canada Enterprise Security Control Committee (GC ESCC) at the director general level to act as an advisory body on key strategies for strengthening the effectiveness of government security policy, services and related operations (including physical security). All the lead security agencies and internal enterprise service organizations identified by the *Policy on Government Security* are members of this committee. The terms of reference specify that members are responsible for developing and monitoring priorities on an annual basis to fulfill the various lead security agency and internal enterprise service organization responsibilities under the *Policy on Government Security*. The chair's responsibilities include reporting on progress in implementing priorities to an interdepartmental Assistant Deputy Minister Security Committee (ADM SC) established by the Secretariat and to other senior management committees, as appropriate. ADM SC, which includes all lead security agencies and internal enterprise service organizations in its membership, is the decision-making body on government-wide security policy initiatives. Its mandate is to provide strategic direction and leadership to the development, implementation and ongoing evaluation of the *Policy on Government Security*. This entails supporting an integrated risk-based approach between lead security agencies, internal

enterprise service providers, central agencies and departments in support of the Government of Canada security policy objectives and related ongoing operations (including physical security).

During the audit fieldwork and reporting phase, GC ESCC demonstrated that work was underway to develop a formal Lead Security Agency and Internal Enterprise Security Services annual joint work plan to identify and track progress on strategic priorities. A partially completed plan was provided that listed some physical security priorities including status, milestone target dates and deliverables. Priorities were identified for all lead security agencies and internal enterprise security organizations included in the audit.

The audit also noted that the GC ESCC has briefed the ADM SC once (in June 2019) to provide an overview of the objectives of the GC ESCC and of some gaps, potential risks, opportunities and issues that may impact Government of Canada security. At this meeting, the chair of GC ESCC presented mock-ups of executive dashboards to be used going forward in identifying and monitoring progress on strategic priorities (including physical security). GC ESCC also committed at this meeting to engaging ADM SC and other deputy head-level committees regularly.

Formal and coordinated strategic planning at the government-wide level would help strengthen the integration of physical security management between all stakeholders involved.

Recommendations: Government-wide physical security strategic planning

9. Under the Secretariat's leadership, GC ESCC should finalize the Lead Security Agency and Internal Enterprise Security Services work plan and ensure that all physical security strategic priorities are identified. The committee should also put mechanisms in place to regularly maintain this plan and leverage ACOPS as part of the process.
10. Under the Secretariat's leadership, GC ESCC should follow through with its commitment to regularly engage ADM SC and other relevant deputy head-level committees on lead security agency strategic priorities (including physical security priorities).

While the Secretariat has monitored and reported on compliance, its current monitoring approach does not provide a broad government-wide view of compliance with physical security policy instruments and does not assess their effectiveness. Work is underway to address these gaps.

The Secretariat is responsible for ensuring government security policy oversight and for overseeing a whole-of-government approach to security management. This includes conducting periodic reviews of the effectiveness of security support services to provide assurance that they continue to meet the needs of the government as a whole.

With respect to monitoring and reporting on compliance with government-wide physical security requirements, the Secretariat has conducted annual Management Accountability Framework (MAF) assessments of departments. However, the Secretariat has recognized that MAF assessments were limited to the assessment of some large departments and agencies and, as a result, the findings generated by the assessment did not provide a broad government-wide view of compliance.

Moreover, the Secretariat did not demonstrate that it has monitored and reported on the effectiveness of its security policy framework covering physical security. Furthermore, the Secretariat did not demonstrate having monitored whether lead security agencies effectively fulfilled their physical security-related responsibilities under the *Policy on Government Security*.

During the reporting phase of the audit, however, the Secretariat did demonstrate that work was underway to develop a Government of Canada Security Performance Measurement Framework (GCSPMF) to address the previously mentioned oversight gaps. [Redacted] Finally, the audit noted that the Secretariat plans on developing the GCSPMF in a phased approach, which will include consultations with the government security community and a pilot in selected departments prior to its full implementation.

Comprehensive government-wide monitoring and reporting frameworks to periodically oversee the effectiveness of and compliance with the policy instruments supporting physical security would help increase the likelihood that the objectives,

expected results and outcomes of the renewed *Policy on Government Security* will be achieved.

Recommendation: Government-wide monitoring and reporting

11. The Secretariat should finalize and implement its GCSPMF in consultation with other lead security agencies, internal enterprise service organizations, departments and the government security community. The GCSPMF should cover monitoring and reporting on compliance with and effectiveness of the Treasury Board security policy framework.

Finding 2: Governance at the departmental level

The Treasury Board *Policy on Government Security* states that deputy heads are responsible for establishing security governance within their departments. The audit examined whether departments carried out their governance-related responsibilities according to the government security policy framework in effect as of June 30, 2017 (see Appendix A). Upon review, it was determined that the renewed Treasury Board security policy framework issued in July 2019 does not negate the requirements of the previous policy framework on which the findings in this section are based. [28]

The audit focused on the following aspects of departmental governance for physical security:

- governance committees
- communication of roles and responsibilities
- departmental security planning
- monitoring and reporting

Given the previously mentioned delay in reporting for this audit, some of the participating departments may have since addressed the findings and recommendations presented in this section. Any progress made in this regard is to be reflected and tracked in departmental management action plans. Recommendations in this section were framed in the context of the renewed Treasury Board security policy framework to ensure their continued relevance.

Although the vast majority of departments established governance committees to oversee physical security activities, half did not demonstrate that these committees were actively involved in this area.

Under the *Directive on Departmental Security Management*, departments were required to establish security governance mechanisms (such as committees and working groups) to ensure the coordination and integration of security activities and to facilitate decision-making.

The audit found that nearly all departments had put in place formal governance committees with broad mandates, which included oversight and support for physical security activities. As a good practice, it was noted that half of the large departments and the majority of small departments had established committees or working groups with mandates specifically dedicated to departmental security.

However, half of the departments did not demonstrate that these governance committees actively supported physical security activities by both regularly discussing topics related to physical security at their meetings, and tracking and following up on initiatives in this area. This was particularly the case in departments without committees dedicated to security.

Active involvement from governance committees would help raise the profile of physical security within departments and further enhance the integration of related activities with the other security controls.

Recommendation: Departmental governance committees

12. Departments should ensure that governance committees are actively supporting physical security activities by regularly meeting to discuss related topics and systematically following up on initiatives in this regard.

While physical security roles and responsibilities were defined in all departments, their documentation, approval and communication could be improved.

The *Policy on Government Security* required deputy heads to appoint a departmental security officer (DSO) [29] to manage the departmental security program. The DSO

was required to report functionally either to the deputy head or to the departmental executive committee. Additionally, departments were expected to appoint security practitioners to support the departmental security program. These practitioners were required to maintain a functional or direct reporting relationship with the DSO. Finally, according to the *Directive on Departmental Security Management*, the accountabilities, delegations, reporting relationships, roles and responsibilities of departmental employees with security responsibilities were to be defined, documented and communicated to the relevant people.

The audit found that all departments appointed a DSO and security practitioners responsible for physical security. Roles and responsibilities for most key security stakeholders were defined in all departments, often through an approved departmental security policy. In the vast majority of cases, DSOs and security practitioners were also held accountable for their physical security responsibilities through their performance management agreements. As a good practice, the audit noted that the Canadian Food Inspection Agency required its managers and employees to formally acknowledge their understanding and commitment to comply with the *Policy on Government Security* and *Directive on Departmental Security Management*. However, while security practitioners in almost all departments had a direct or functional reporting relationship to their DSO, it was noted that in half of the large and small departments, the reporting relationship between the DSO and the deputy head or executive committee was not aligned with expectations.

Opportunities for improvements were also identified in most departments regarding the documentation, approval and communication of roles and responsibilities. For example, specific and up-to-date roles and responsibilities for physical security were not defined for governance committees in most large departments and half of the small departments. Additionally, defined roles and responsibilities were not consistently approved in half of the large departments and small departments. In all of the departments that assigned physical security roles and responsibilities to employees working in regional offices, the audit found that communication surrounding these roles and responsibilities could be improved. For example, several regional security practitioners expressed a desire for increased support from their

headquarters (such as through additional training opportunities). Finally, most of the large and small departments had not reviewed all physical security-related roles and responsibilities. Two small departments indicated that they were waiting for the Secretariat to finalize its policy suite renewal before updating their own departmental security policies.

Ensuring that up-to-date physical security roles and responsibilities are formally communicated to all relevant stakeholders would help foster a better understanding of expectations and coordination of efforts, and help ensure that assigned responsibilities are carried out. Furthermore, aligning the reporting relationship of senior departmental security officials with the *Policy on Government Security* would help raise the profile of security within departments and help ensure proper coordination during security incidents.

Recommendation: Departmental roles and responsibilities

13. Departments should ensure that up-to-date roles, responsibilities and reporting relationships are formally communicated to all stakeholders involved in physical security activities in alignment with the Treasury Board security policy framework.

Most departments had an overarching DSP covering physical security; however, the content of DSPs was generally not consistently aligned with the DSP process suggested by the Secretariat's guidelines and, in most cases, DSPs were not regularly reviewed and updated.

According to the *Directive on Departmental Security Management*, departments were required to develop and maintain a DSP providing an integrated view of departmental security requirements (including physical security). The purpose of DSPs was to detail the decisions for managing security risks and to outline strategies, goals, objectives, priorities and timelines for improving departmental security. To assist departments in meeting expectations, the Secretariat issued guidelines on how to develop DSPs.

The audit found that all departments had an approved DSP in place. The majority of the large departments' and half of the small departments' DSPs covered goals, objectives, priorities and timelines. Most departments also demonstrated that a process was established and followed to identify and analyze risks, including those relating to physical security. Additionally, most departments consulted relevant departmental stakeholders during the development of their DSPs.

In general, the content of DSPs examined was not consistently aligned with the Secretariat's *Guideline on Developing a Departmental Security Plan*. Opportunities for improvements in this regard mostly revolved around the need to include further details in terms of performance indicators, implementation strategies, and risk evaluations to determine whether the risks identified were acceptable or not. Furthermore, half of the large departments and the majority of small departments did not demonstrate having maintained their DSPs by conducting periodic reviews and updates. In half of the small departments, the main challenge raised pertained to a lack of resources for completing such reviews and updates.

Regularly maintaining and fully aligning DSPs with the Secretariat's policy instruments would help departments better address emerging security risks and clarify priorities. It would also provide a stronger baseline within departments to monitor the effectiveness of their plans over time, and to identify when and where corrective actions may be needed. Strong and up-to-date DSPs could also help departments cope more effectively with capacity issues by prioritizing their limited resources to mitigate the highest security risks.

Recommendation: Departmental security plans (DSPs)

14. Departments should regularly (at least annually) review their DSP to ensure that it is up to date and aligned with the expectations of the Treasury Board security policy framework.

Physical security monitoring and reporting frameworks were either non-existent or limited.

DSOs were required to actively monitor the implementation of all security activities within their department and recommend appropriate remedial action to the deputy head or senior management committee (as appropriate) to address any deficiencies. This expectation included evaluating the achievement of objectives outlined in the DSP and the effectiveness of security controls, and reporting the results to the appropriate governance committees.

While most departments had completed some monitoring activities, these tended to be ad hoc, incomplete and informal. [Redacted]

Establishing formal processes to regularly monitor and report on compliance and the effectiveness of departmental physical security activities would help to proactively identify gaps and make any necessary adjustments. [Redacted]

Recommendation: Departmental monitoring and reporting

15. Departments should establish formal monitoring and reporting frameworks to periodically assess their compliance with the government's security policy framework and the overall effectiveness of their physical security function (including physical security controls).

Finding 3: Departmental physical security processes

Under the *Directive on Departmental Security Management*, security practitioners within departments were expected to select, implement and maintain physical security controls. The Secretariat's *Operational Security Standard on Physical Security* provided baseline physical security requirements to counter threats to government employees, assets and service delivery. Baseline requirements were designed to provide a consistent minimum level of physical security controls across government in order to help mitigate common types of threats that departments would encounter. Certain departments could face different threats because of the nature of their operations, their location and/or the attractiveness of their assets. The standard therefore prescribed a physical security approach to help departments supplement baseline physical security controls where appropriate, based on the particular threats and risks they face. The RCMP also issued various technical

guidance to support departments in tailoring physical security controls to meet their needs.

The audit focused on expectations outlined in the Secretariat's policy instruments and the RCMP's technical guidance in effect as of June 30, 2017 (see Appendix A), and assessed whether departments had processes in place to assess threats and risks, identify and implement physical security controls, report and investigate security incidents, and implement corrective actions following incidents and/or investigations.

Upon review, it was determined that the renewed Treasury Board security policy framework issued in July 2019 does not negate the requirements of the previous policy framework on which the findings in this section are based. [30] Recommendations in this section were framed in the context of the renewed policy framework to ensure their continued relevance.

Given the previously mentioned delay in reporting for this audit, some of the participating departments may have since addressed the findings and recommendations presented in this section. Any progress made in this regard is to be reflected and tracked in departmental management action plans.

While all departments completed some form of TRAs, their coverage and the level of rigor to develop and maintain these could be improved.

The *Directive on Departmental Security Management* required departments to document, implement and maintain processes for the systematic management of security risks to ensure continual adaptation to their changing needs and threat environment. Under the Secretariat's *Security Organization and Administration Standard*, departments were expected to complete TRAs for sensitive information and assets as part of the risk management approach to security. The TRA process was concerned with defining what required protection, analyzing and assessing threats and risks, and making recommendations for the management of risks. Specific technical guidance on how to complete TRAs was provided in the Secretariat's *Security Organization and Administration Standard* and in the *Harmonized TRA Methodology* (issued by the RCMP and the Communications Security

Establishment Canada). According to the Secretariat's *Operational Security Standard on Physical Security*, departments were expected to base their selection and implementation of physical security controls on the results of TRAs.

The audit assessed whether departments had conducted and maintained up-to-date TRAs for their facilities in alignment with the *Security Organization and Administration Standard* and the *Harmonized TRA Methodology*.

All departments completed some form of TRAs or equivalent security assessments and, in most cases, had provided employees with relevant training and guidance on TRAs prior to completing the assessments. In addition, all large departments and half of the small departments had consulted relevant internal stakeholders while developing these assessments.

[Redacted] [31] Most departments also indicated that they had not consulted external stakeholders such as lead security agencies as part of their TRA process to seek additional advice and guidance. [Redacted]

[Redacted] Strong TRA processes, coupled with the implementation of TRA recommendations, help reduce the risk that some areas within departments may be under-protected by physical security controls.

Recommendation: Threat and risk assessments (TRAs)

16. [Redacted]

Most departments had processes in place to implement physical security controls based on TRAs. [Redacted]

Following TRAs, the next steps in managing security risks relate to the approval and implementation of safeguards. The Secretariat's *Operational Security Standard on Physical Security* required departments to ensure that access to and safeguards for protected and classified assets were based on a clearly discernable hierarchy of zones. [32] The standard also required departments to control access to restricted-access areas using safeguards that would grant access only to authorized employees.

The audit assessed whether departments had processes in place to approve and implement facility access controls and hierarchy of zones to protect information, assets and employees in alignment with TRAs and the previously mentioned standard. The audit also examined departmental processes in place to implement and approve devices, systems and procedures to detect attempted or actual physical security incidents. As part of these processes, the audit expected that all relevant stakeholders within departments and lead security agencies would have been consulted.

Although not always formalized, the majority of departments had processes in place to implement the physical security controls assessed. [Redacted] Additionally, opportunities for improvements were identified in most of the small departments with respect to ensuring that all relevant internal and external stakeholders are consulted as part of the process to implement physical security controls.

Adopting formal processes [Redacted] would help departments strengthen their ability to adequately protect their employees, information and assets from compromise.

Recommendation: Processes to approve and implement physical security controls

17. Departments should establish formal processes to ensure that the physical security controls recommended in TRAs are approved by senior management and consistently implemented in the context of the departmental risk environment and tolerances, and in consultation with all relevant stakeholders.

In general, processes for reporting security incidents were defined and communicated; however, in most small departments, they were not followed consistently. In the majority of departments, the audit also found no evidence demonstrating that incidents had been both investigated and the results of such investigations reported to senior management.

Within the context of physical security, the response process involved reporting security incidents to the appropriate security officials and taking immediate and long-term corrective action. Under the *Policy on Government Security*, deputy heads

were responsible for the completion of investigations and assessments of the effectiveness of the departmental security program.

The audit found that the majority of departments had fully defined and communicated security incident reporting processes. However, in most of the small departments and in one large department, these processes were not followed consistently for the incidents sampled as part of the audit.

Half of the departments also had not fully defined a process to investigate security incidents and report the results of such investigations to the relevant stakeholders. Furthermore, the majority of departments did not demonstrate that the incidents sampled as part of the audit were both investigated and the results of such investigations reported consistently to senior management. Some departments indicated that they did not think it was necessary to report the results of investigations into security incidents to senior management. While departments that identified required corrective actions during investigations did implement these in most cases, the majority of departments have not established a formal process to track and follow up on investigation recommendations.

Consistently implementing security incident reporting and investigation processes would strengthen the physical security response and help identify areas where improvements are needed to physical security controls. Regularly tracking and following up on investigation recommendations would further encourage the timely adoption of corrective actions within departments.

Recommendations: Incident reporting and investigation

18. Departments should establish a formal process to investigate incidents and report the results of such investigations to senior management. As part of this process, departments should regularly monitor and report on the implementation of investigation recommendations.
19. Departments should ensure that their incident reporting and investigation processes are consistently carried out in practice. For example, departments could consider formally tasking their chief security officer to regularly monitor

past incidents, on a sample basis, to assess alignment with the departmental processes and report back to senior management on these assessments.

Conclusion

Overall, the audit noted a need for improvements to the government-wide and departmental governance frameworks, and to physical security processes within departments.

Although lead security agencies have fulfilled their basic responsibilities in supporting physical security at the government-wide level, several opportunities for improvements were noted with respect to:

- updating policy instruments
- services relating to base building security
- coordination and operations of interdepartmental governance committees
- strategic planning of lead security agency priorities
- monitoring and reporting frameworks

Within departments, there were also several opportunities for improving physical security governance frameworks:

- the level of involvement of governance committees
- communication of roles and responsibilities (especially in regional offices)
- maintenance of DSPs and their alignment with the guidance issued by lead security agencies
- monitoring and reporting frameworks

Finally, [Redacted] gaps were identified in departmental physical security processes:

- [Redacted]
- [Redacted]
- [Redacted]
- reporting of incidents
- investigation of incidents
- follow-up on recommendations from past investigations

Management response

The findings and recommendations of this audit were presented to the Secretariat, the RCMP, PSPC and PCO, along with the four large departments and four small departments that participated in this audit.

Management has agreed with the findings included in this report and will take action to address all applicable recommendations.

Appendix A: Applicable policy, directive, standards and guidance

Policy, directive, standards and guidance	Description
Policy on Government Security Effective date: July 1, 2019	The objectives of this policy are to effectively manage government security controls in support of the trusted delivery of Government of Canada programs and services and in support of the protection of information, individuals and assets, as well as to provide assurance regarding security management in the Government of Canada. This policy replaced the *Policy on Government Security* that was in effect from July 1, 2009, to June 30, 2019.
Directive on Security Management Effective date: July 1, 2019	This directive, issued pursuant to the authorities indicated in section 2 of the *Policy on Government Security*, outlines requirements for the management of security at the departmental level. The directive includes, as appendices, mandatory procedures for the eight security controls defined in the *Policy*

	on Government Security, including the "Mandatory Procedures for Physical Security Control" appendix, which provides details on the requirements to support the deputy head accountability for physical security. The *Directive on Security Management* and its Mandatory Procedures replaced the *Directive on Departmental Security Management*, the *Operational Security Standard: Business Continuity Planning (BCP) Program*, the *Operational Security Standard on Physical Security*, the *Operational Security Standard: Readiness Levels for Federal Government Facilities*, and the *Operational Security Standard: Management of Information Technology Security (MITS)*.
Harmonized Threat and Risk Assessment (TRA) Methodology Effective date: August 28, 2007	The *Harmonized TRA Methodology* was issued under the authority of the Chief, Communications Security Establishment Canada and the Commissioner, Royal Canadian Mounted Police (RCMP) to provide guidance on the conduct of TRAs. This document was developed as a practical tool elaborating on the previous *Policy on Government Security* and supporting standards to help government managers meet both the objectives and the requirements of the policy.
RCMP guidelines	The Treasury Board security policy framework is complemented by

	several physical security guidelines issued by the RCMP, including the G1-001: Security Equipment Guide (last updated February 25, 2014) and the G1-025: Protection, Detection and Response (issued December 2004).
Guideline on Developing a Departmental Security Plan Last modified: December 4, 2013	The purpose of this guideline is to assist departments in meeting the requirements of the *Policy on Government Security* to develop a departmental security plan that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security.

The lines of enquiry and criteria for the audit were developed with reference to the security policy framework that was in place as at June 30, 2017, including the previous *Policy on Government Security*, *Directive on Departmental Security Management*, *Operational Security Standard on Physical Security*, and *Security Organization and Administration Standard*. A comparison of the previous and newly issued Treasury Board security policy framework follows.

Type of instrument	**Previous Treasury Board security policy framework**	**Revised Treasury Board security policy framework**
Legislation	*Financial Administration Act* (FAA)	*Financial Administration Act* (FAA)
Policy	Policy on Government Security (PGS) (2009 – amended 2012)*	Policy on Government Security*
Directives	• Directive on Identity Management (2009)	• Directive on Identity Management

	• Directive on Departmental Security Management (DDSM) (2009)*	• Directive on Security Management*
		  ◦ Mandatory Procedures on Security Controls*
		  ▪ Security Screening
		  ▪ Security Awareness & Training
		  ▪ Business Continuity Management
		  ▪ Information Management Security
		  ▪ Information Technology Security
		  ▪ Security in Contracts and Other Arrangements
		  ▪ Security Event Management
		  ▪ **Physical Security***

Standards	• Security Organization & Administration (1994)* • Security Screening (2014) • Readiness Levels for Federal Government Facilities (2002) • Identity and Credential Assurance (2013) • Management of Information Technology Security (2004) • Business Continuity Planning (2004)	• Standard on Security Categorization • Standard on Identity and Credential Assurance • Standard on Security Screening • Standard on Security Event Reporting (New)

	• Physical Security (2004)* • Security in Contracting (1994)	

* Define requirements for physical security

Appendix B: Departments included in the audit

Lead security agencies (including the policy centre) and large and small departments were selected for this audit through both a risk assessment and a self-identification exercise conducted as part of the Office of the Comptroller General's risk-based audit planning.

The following lead security agencies (including the policy centre) were selected for inclusion in the audit:

1. Treasury Board of Canada Secretariat (the Secretariat) – central agency/policy centre
2. Public Services and Procurement Canada (PSPC)
3. Royal Canadian Mounted Police (RCMP)
4. Privy Council Office (PCO)

The following large departments were selected for inclusion in the audit:

1. Canadian Food Inspection Agency (CFIA)
2. Crown-Indigenous Relations and Northern Affairs Canada (CIRNAC) and Indigenous Services Canada (ISC) [33]
3. Innovation, Science and Economic Development Canada (ISED)
4. Veterans Affairs Canada (VAC)

The following small departments were selected for inclusion in the audit:

1. Canadian Nuclear Safety Commission (CNSC)
2. Canadian Radio-television and Telecommunications Commission (CRTC)
3. Immigration and Refugee Board of Canada (IRB)
4. Library and Archives Canada (LAC)

Appendix C: Lines of enquiry and audit criteria

The audit criteria are presented in the table below by line of enquiry.

Line of enquiry	Criteria	Related source(s) ***Previous framework***	Related source(s) ***Current framework***
1. Government-wide governance framework A government-wide governance framework is in place for the management of physical security across the Government of Canada.	1.1 Governance structures* that support government-wide management of physical security are in place and their roles and responsibilities have been documented, approved, and communicated to all stakeholders. *For the purpose of this audit, the term "governance structures" refers to governance bodies (e.g. Senior management committees, forums, working group, etc.), their interrelationships, and members.	*Policy on Government Security* (PGS) 3.6, 5.2, 6.2.2, 6.3, Appendix B *Directive on Departmental Security Management* (DDSM) 6.1.15	*Policy on Government Security* (PGS) 3.2.1, 4.2.1, 4.2.4, 4.3.2, 4.3.3.1, 4.4.1, 4.4.2, 5.7.2.1, 5.12.1
	1.2 A government-wide policy framework* defining roles and responsibilities and requirements for	PGS 3.4, 3.9, 6.2, 6.3, Appendix B	PGS 2.2, 4.2.4, 4.3.3.2, 5.7.1, 5.10.1, 5.12.1, 5.12.2

	physical security is in place and up-to-date to reflect the current operating environment. *For the purpose of this audit, the term “policy framework” is used broadly to encompass policies, procedures, guidance, advice and tools (i.e. mandatory and non-mandatory guidance) provided to departments by the lead security agencies (LSAs) selected.		
	1.3 A government-wide security approach* has been developed, implemented, and communicated to support the identification and management of physical security threats, risks, and incidents across the Government of Canada. *For the purpose of this audit criterion, the term “approach” refers to a strategy or plan used by LSAs to	PGS 3.4, 6.2.1, 6.2.3, 6.3, Appendix B	PGS 4.2.4, 4.3.2, 4.3.3.1, 4.3.3.4, 4.4.1, 5.12.1

	coordinate and ensure the completion of their physical security responsibilities.		
	1.4 Interdepartmental coordination and collaboration processes are in place to integrate physical security activities across government.	PGS 3.4, 5.2, 6.2.1, 6.2.3, 6.3, Appendix B DDSM 6.1.13, 6.1.14	PGS 3.2.2, 3.2.5, 4.2, 4.3, 4.4, 5.7, 5.9, 5.10.1, 5.12 *Directive on Security Management* (DSM) 4.6.3, C.2.7.1
2. Departmental governance framework Departmental governance frameworks are in place for the management of physical security.	2.1 Departmental governance structures that support physical security are in place and their roles and responsibilities have been documented, approved, and communicated to all stakeholders.	PGS 3.6, 5.2, 6.1.1, 6.1.2, 6.3 DDSM 6.1.5, 6.1.6, 6.1.16	PGS 3.2.1, 3.2.4, 4.1.1, 4.1.2, 4.1.4 DSM 4.1.2.1, 4.2.1, 4.2.2, 4.2.3, 4.2.6, 4.2.10, 4.3.1, 4.3.2, 4.3.3, 4.4.2
	2.2 A departmental policy framework defining roles, responsibilities, and requirements for physical security is documented, communicated and approved.	PGS 6.1.1(a), (b) DDSM 6.1.5 *Security Organization and Administration Standard* (SOA) 1.3, 3	Supports compliance with: PGS 4.1.4 DSM 4.1.2.1, 4.2.2, 4.2.6, 4.3.1, 4.4.2
	2.3 A departmental process is in place to develop and monitor a	PGS 3.5, 6.1.1(b), 6.1.4, 6.1.5, 6.3	PGS 4.1.1, 4.1.5

	systematic* plan for physical security that is integrated and coordinated with other aspects of departmental security. * For the purpose of this audit criterion, the term "systematic" refers to the following attributes: • methodical (i.e. aligned with the steps required under the Secretariat's *Guideline on Developing a Departmental Security Plan*) • documented; and, • consultative.	DDSM 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.6, 6.1.7, 6.1.8, 6.1.9, 6.1.10, 6.1.11, 6.1.12, 6.1.16, 6.1.22, 6.1.23, Appendix C SOA 3 *Guideline on Developing a Departmental Security Plan*, s. 5, 7	DSM 4.1.2.1, 4.1.3, 4.1.4, 4.1.5, 4.2.6, 4.2.10, 4.3.1, 4.3.3, 4.4.1, C.2.4 *Guideline on Developing a Departmental Security Plan*, s. 5, 7
3. Departmental physical security A departmental physical security approach is in place for the development, implementation, testing, update and monitoring of physical security safeguards and incident	3.1 Departments have conducted and maintained an up-to-date threat and risk assessment for departmental facilities and activities.	PGS 3.1, 3.3 DDSM 6.1.1.2, 6.1.4, 6.1.7, 6.1.10, 6.1.21, 6.1.23 *Operational Security Standard on Physical Security* (OSSPS) 6.3, 7.1 SOA 9 *Harmonized Threat and Risk*	Supports compliance with: PGS 3.2.4, 4.1.6, 4.3.3.4 DSM 4.1.4, 4.1.6, 4.2.7, 4.2.8, C.2.2, C.2.5, C.2.8 *Harmonized Threat and Risk Assessment Methodology*

management process.		*Assessment Methodology*	
	3.2 Departments have a process to implement and monitor the effectiveness of physical security safeguards that mitigate the threats and risks identified in their threat and risk assessments, which take into account interdependencies with key stakeholders*. * "Stakeholders" refer to departments, Lead Security Agencies and external organizations that play a role in the department's physical security.	PGS 5.2, 6.3 DDSM 3.1, 6.1.1.2, 6.1.2, 6.1.7, 6.1.9, 6.1.10, 6.1.11, 6.1.12, 6.1.17, 6.1.18, 6.1.19, 6.1.24, 6.1.25, 6.1.27, 6.1.28, Appendix C OSSPS 6-8 SOA 16.10	PGS 3.1.1, 3.2.1, 3.2.4, A.3 DSM 4.1.2.1, 4.2.6, 4.2.10, 4.3.1, 4.3.3, C.2.2.3, C.2.3
	3.3 Departments have an incident management process in place to detect, report, and respond* to physical security incidents. *See note 1 at the bottom of the table.	PGS 3.3, 5.2, 6.1.8 DDSM 6.1.7, 6.1.13, 6.1.14, 6.1.29, 6.2.2, Appendix B, Appendix C OSSPS 6.1 SOA 16.1 RCMP G1-025 Protection,	PGS 4.1.7, A.7 DSM 4.1.6, 4.1.7, 4.2.8, 4.2.9, 4.4.4, 4.4.5, 4.5.3, 4.6.5, C.2.3.1, C.2.3.2.4, G.2.2, G.2.3, G.2.5, G.2.6, I.2.2.2 RCMP G1-025 Protection, Detection and Response, s. 5, 6

		Detection and Response, s. 5, 6	
	3.4 Departments ensure that their incident management process is periodically tested and updated to reflect the changing operating environment. *See note 1 at the bottom of the table.	PGS 6.1.8, 6.3 DDSM 6.1.7, Appendix C OSSPS 6.1 SOA 16.1, 16.10 RCMP G1-025 Protection, Detection and Response, s. 6.1, 6.4	PGS 4.1.7 DSM 4.1.7, 4.4.5, G.2.2.6, G.2.6 RCMP G1-025 Protection, Detection and Response, s. 6.1, 6.4
	3.5 Departments ensure that sufficient and relevant training as well as tools are provided to enable the development, implementation and management of physical security safeguards.	PGS 3.3, 3.5 DDSM 6.1.20, 6.1.30, Appendix C SOA 15 RCMP G1-025 Protection, Detection and Response, s. 6.1.6	PGS A.8 DSM 4.4.2, 4.5.2, H.2.2 RCMP G1-025 Protection, Detection and Response, s. 6.1.6
4. Monitoring Government-wide and departmental processes are in place to monitor departmental compliance with Treasury Board policy framework requirements.	4.1 Departments monitor compliance with physical security-related requirements in the Treasury Board *Policy on Government Security* and inform the Secretariat of any gaps identified.	PGS 6.1.8, 6.2.2, 6.2.3, 6.3 DDSM 6.2.2	PGS 4.1.10 DSM 4.1.7, 4.4.4, C.2.6
	4.2 The Secretariat	PGS 6.3	Supports

	monitors and reports on the effectiveness of and compliance with physical security-related requirements in the Treasury Board policy framework.	DDSM 6.2.4	compliance with: PGS 5.12.1, 5.12.2

Note 1: During the examination phase, the audit assessed departmental incident management processes in place as at June 30, 2017, based on the relevant LSA policy instruments in effect at that time.

During the reporting phase of the audit, the renewed Treasury Board *Policy on Government Security* specifically identified security event management [34] as one of eight government security controls. New mandatory procedures for security event management were also issued in the Secretariat's renewed *Directive on Security Management*.

To recognize this change, some of the findings observed under criteria 3.3 and 3.4 have not been included in this report, given that these now relate to the broader area of security event management as defined in the renewed Treasury Board security policy framework. However, it should be noted that all detailed findings under criteria 3.3 and 3.4 were communicated to the participating departments during the audit examination.

Appendix D: Recommendations by department and risk ranking

The following table presents the departments to which the audit recommendations apply and assigns a risk ranking of high, medium or low to each recommendation. The determination of risk rankings was based on the relative priorities of the recommendations and the extent to which the recommendations indicate non-compliance with Treasury Board policies. The full names of the lead security agencies and the large and small departments are provided in Appendix B.

Recommendation	Departments to which this recommendation applies [35]	Priority level [36]
1. The Secretariat and the RCMP should establish formal mechanisms to help ensure that their respective government-wide policy instruments supporting physical security will be periodically reviewed and updated in a timely manner going forward. • For example, such mechanisms could include a formally approved plan or strategy outlining the process, roles, responsibilities and timelines to review and update policy instruments, and an assessment of capacity to support the completion of reviews and updates. Linking such plans to performance agreements and/or to the forward agenda of a governance committee could in turn help ensure that these plans will be implemented *Applies to opportunities for improvement identified under audit sub-criterion 1.2.2*	Secretariat, RCMP	Low
2. The Secretariat and the RCMP should: a. in consultation with the government security	Secretariat, RCMP	High

community, assess and prioritize government-wide needs for change management guidance (while respecting individual departmental operating contexts) to help ensure the effective implementation of the renewed physical security requirements under the Treasury Board security policy suite currently in effect b. issue supplementary guidance required to meet these needs *Applies to opportunities for improvement identified under audit criterion 1.2*		
3. PSPC should continue to consult regularly with client departments and other lead security agencies to identify base building security risks, needs and priorities. *Applies to opportunities for improvement identified under audit sub-criterion 1.3.1*	PSPC	Medium
4. PSPC should finalize the implementation of its risk-based approach for conducting and regularly maintaining base building TRAs. *Applies to opportunities for improvement identified under audit sub-criteria 1.4.1 and 1.4.3*	PSPC	Medium
5. The Secretariat and the RCMP should ensure that their security	Secretariat, RCMP	Low

governance committees regularly coordinate their government-wide physical security activities (such as through periodic status updates). *Applies to opportunities for improvement identified under audit criterion 1.1*		
6. The Secretariat and the RCMP should ensure that the governance committees they are responsible for with respect to government-wide physical security consistently track and follow up on their decisions and initiatives. *Applies to opportunities for improvement identified under audit sub-criterion 1.1.3*	Secretariat, RCMP	Medium
7. The Secretariat and the RCMP, with the collaboration of relevant interdepartmental small department governance committees (such as the Heads of Federal Agencies committee), should jointly assess the membership of the various governance committees supporting government-wide physical security to ensure adequate representation of small departments. *Applies to opportunities for improvement identified under audit criterion 1.1*	Secretariat, RCMP	Medium
8. The RCMP should ensure that its governance committees	RCMP	Low

(including working groups) supporting government-wide physical security have formally approved and documented terms of reference that clearly define their respective mandates, roles, responsibilities and accountabilities. These terms of reference should also be communicated to all relevant governance committee members. *Applies to opportunities for improvement identified under audit sub-criterion 1.1.2*		
9. Under the Secretariat's leadership, GC ESCC should finalize the Lead Security Agency and Internal Enterprise Security Services work plan and ensure that all physical security strategic priorities are identified. The committee should also put mechanisms in place to regularly maintain this plan and leverage ACOPS as part of the process. *Applies to opportunities for improvement identified under audit criterion 1.3*	Secretariat, RCMP	High
10. Under the Secretariat's leadership, GC ESCC should follow through with its commitment to regularly engage ADM SC and other relevant deputy head-level committees on lead security agency strategic priorities (including physical security priorities).	Secretariat	High

Applies to opportunities for improvement identified under audit criterion 1.3		
11. The Secretariat should finalize and implement its GCSPMF in consultation with other lead security agencies, internal enterprise service organizations, departments and the government security community. The GCSPMF should cover monitoring and reporting on compliance with and effectiveness of the Treasury Board security policy framework. *Applies to opportunities for improvement identified under audit criterion 4.2*	Secretariat	Medium
12. Departments should ensure that governance committees are actively supporting physical security activities by regularly meeting to discuss related topics and systematically following up on initiatives in this regard. *Applies to opportunities for improvement identified under audit sub-criteria 2.1.1 and 2.1.3*	CFIA, VAC, CRTC, IRB	High
13. Departments should ensure that up-to-date roles, responsibilities and reporting relationships are formally communicated to all stakeholders involved in physical security activities in alignment with the Treasury Board security policy framework.	All large and small departments [37]	High

Applies to opportunities for improvement identified under audit sub-criteria 2.1.1 and 2.1.2, and audit criteria 2.2 and 3.5		
14. Departments should regularly (at least annually) review their DSP to ensure that it is up to date and aligned with the expectations of the Treasury Board security policy framework. *Applies to opportunities for improvement identified under audit criterion 2.3*	All large and small departments	High
15. Departments should establish formal monitoring and reporting frameworks to periodically assess their compliance with the government's security policy framework and the overall effectiveness of their physical security function (including physical security controls). *Applies to opportunities for improvement identified under audit sub-criteria 2.3.3 and 3.2.2, and audit criterion 4.1*	All large and small departments	High
16. [Redacted]	[Redacted]	[Redacted]
17. Departments should establish formal processes to ensure that the physical security controls recommended in TRAs are approved by senior management and consistently implemented in the context of the departmental risk environment and tolerances, and in consultation with all relevant stakeholders.	CFIA, CIRNAC and ISC, CRTC, IRB, LAC	High

Applies to opportunities for improvement identified under audit sub-criteria 3.2.1 and 3.3.1		
18. Departments should establish a formal process to investigate incidents and report the results of such investigations to senior management. As part of this process, departments should regularly monitor and report on the implementation of investigation recommendations. *Applies to opportunities for improvement identified under audit sub-criteria 3.3.3 and 3.4.2*	CFIA, CIRNAC and ISC, ISED, CRTC, IRB, LAC	Medium
19. Departments should ensure that their incident reporting and investigation processes are consistently carried out in practice. For example, departments could consider formally tasking their chief security officer to regularly monitor past incidents, on a sample basis, to assess alignment with the departmental processes and report back to senior management on these assessments. *Applies to opportunities for improvement identified under audit sub-criteria 3.3.2, 3.3.3, and 3.4.2*	CFIA, CIRNAC and ISC, ISED, CRTC, IRB, LAC	Low

Appendix E: Roles and responsibilities of the main lead security agencies and central agency

Main departments	Summary of roles and responsibilities for supporting government-wide physical security
Treasury Board and the Secretariat (central agency / policy centre)	The roles and responsibilities of the Treasury Board and its Secretariat are detailed in the *Financial Administration Act* and in the Treasury Board *Policy on Government Security*. The main responsibilities of the Treasury Board and the Secretariat for supporting government-wide physical security are summarized below: • Under section 7 of the *Financial Administration Act*, the Treasury Board has the authority to issue a security policy and directives for the Government of Canada. In turn, the Treasury Board delegated to the President of the Treasury Board the authority to amend such directives as needed, including the authority to issue and amend related standards and guidance in the area of physical security. As the administrative arm of the Treasury Board reporting to its President, the Secretariat is the central agency responsible for developing and maintaining government-wide policy instruments in this area • Under the *Policy on Government Security*, the Secretariat is responsible for: ◦ establishing government-wide security policy governance to set strategic direction and priorities and coordinating security priorities, plans and activities government-wide ◦ establishing and overseeing a whole-of-government approach to security management as a key component of all management activities by ensuring the conduct of periodic reviews of the effectiveness of security support services, to provide assurance that they continue to meet the needs of the government as a whole

	◦ providing policy leadership, advice and guidance for all matters related to government security ◦ providing strategic policy oversight and coordination for the management of security events that may affect the government as a whole
Royal Canadian Mounted Police (lead security agency)	The RCMP, as the lead security agency for physical security, is responsible under the *Policy on Government Security* for providing leadership, advice and guidance for matters related to physical security.
Public Services and Procurement Canada (lead security agency)	PSPC is identified as a lead security agency in section 5.9 of the *Policy on Government Security*. PSPC is responsible for providing internal enterprise services for base building security for general-purpose office facilities under its custodial responsibility.
Privy Council Office (lead security agency)	PCO is identified as a lead security agency in section 5.7 of the *Policy on Government Security*. PCO is responsible for: • establishing policy direction for the security of Cabinet confidences • ensuring that national security objectives are reflected in government-wide security policy governance • providing advice and guidance on implementing security readiness levels in emergency and increased threat situations • providing strategic leadership to coordinate responses to operational security matters facing the government that are of national, intergovernmental or international importance

Footnotes

1 See Appendix C for the specific aspects of governance and physical security processes examined as part of this audit.

2 A security event is defined as “Any event, act, omission or situation that may be detrimental to government security, including threats, vulnerabilities and security incidents.” (*Policy on Government Security*, Appendix B: Definitions)

3 The National Energy Board has since been replaced by the Canada Energy Regulator.

4 Indigenous and Northern Affairs Canada has since been dissolved and replaced by two separate departments: Crown-Indigenous Relations and Northern Affairs Canada, and Indigenous Services Canada.

5 October 22, 2014: House of Commons Incident Response Summary, June 3, 2015

6 A threat is defined as “Any potential event or act, deliberate or unintentional, or natural hazard that could result in a compromise.” (*Policy on Government Security*, Appendix B: Definitions)

7 Population of the federal public service, 2019

8 *Annual Financial Report of the Government of Canada 2018-2019*, Finance Canada, p. 28

9 Directory of Federal Real Property

10 Compromise refers to “A breach of government security.” (*Policy on Government Security*, Appendix B: Definitions)

11 Base building security refers to “Security safeguards provided by a building custodian to protect the building’s structure and supporting infrastructure.” (*Policy on Government Security*, Appendix B: Definitions)

12 A TRA is an “evaluation of the nature, likelihood and consequence of acts or events that could place sensitive information and other assets at risk.” (Termium)

13 The *Policy on Government Security* defines eight security controls that departments are required to address in their departmental security planning: security screening, information technology security, physical security, business continuity management, information management security, security requirements associated with contracts and other arrangements, security event management, and security awareness and training.

14 A security control is defined as "A legal, administrative, operational or technical measure for satisfying security requirements. This term is synonymous with 'safeguard.'" (*Policy on Government Security*, Appendix B: Definitions)

15 An internal enterprise service organization is "A department or organization that provides internal enterprise services to other Government of Canada departments. This includes lead security agencies that deliver government-wide security services." An internal enterprise service is "A service provided by a Government of Canada department to other Government of Canada departments intended on a government-wide basis." (*Policy on Government Security*, Appendix B: Definitions)

16 See Appendix E for further details on the roles of the lead security agencies responsible for supporting physical security.

17 Base building security refers to "Security safeguards provided by a building custodian to protect the building's structure and supporting infrastructure." (*Policy on Government Security*, Appendix B: Definitions)

18 See Appendix A for a comparison of the current and the previous Treasury Board security policy frameworks, as well as an overview of the policy instruments relevant to physical security.

19 See Appendix C for a cross-walk of the audit criteria examined to the policy requirements currently in effect.

20 See Appendix A for the relevant RCMP technical guidance examined as part of this audit.

21 See Appendix C for the specific aspects of governance and physical security processes examined as part of this audit.

22 See Appendix C.

23 These security controls are described in Appendix A of the *Policy on Government Security* and in the *Policy on Occupational Safety and Health*.

24 Base building security refers to "Security safeguards provided by a building custodian to protect the building's structure and supporting infrastructure." (*Policy on Government Security*, Appendix B: Definitions)

25 A TRA is an "evaluation of the nature, likelihood and consequence of acts or events that could place sensitive information and other assets at risk." (Termium)

26 Previously the Departmental Security Officer Centre for Development.

27 The Secretariat's interdepartmental governance committee at the chief security officer level was also previously co-chaired by PCO, but is now co-chaired by National Defence.

28 Policy requirements noted throughout this section refer to the previous Treasury Board security policy framework. See Appendix C for a cross-walk of the audit criteria examined to the policy requirements currently in effect.

29 The current *Policy on Government Security* requires all departments to designate a chief security officer responsible for departmental security management activities. Under the previous version of the policy, this role was referred to as the departmental security officer (DSO). As the audit was conducted under the previous policy framework, the term DSO is used to describe findings.

30 Policy requirements noted throughout this section refer to the previous Treasury Board security policy framework. See Appendix C for a cross-

walk of the audit criteria examined to the policy requirements currently in effect.

31 [Redacted]

32 Instituting a hierarchy of zones allows departments to implement varied levels of access controls to protect various levels of assets. Departments can implement up to five zone types: public zone, reception zone, operations zone, security zone and high security zone. The latter three zones are "restricted-access areas." (*Operational Security Standard on Physical Security*, s. 6.2 Hierarchy of Zones)

33 Indigenous and Northern Affairs Canada was selected for inclusion in the audit as a large department. During the conduct of the audit, Indigenous and Northern Affairs Canada was dissolved and replaced by two separate departments: CIRNAC and ISC. Therefore, recommendations resulting from Indigenous and Northern Affairs Canada's audit findings have been issued to these two organizations.

34 Security event management practices are to be defined, documented, implemented and maintained to monitor, respond to and report on threats, vulnerabilities, security incidents and other security events, and ensure that such activities are effectively coordinated within the department, with partners and government-wide, to manage potential impacts, support decision-making and enable the application of corrective actions (*Policy on Government Security*, Appendix A: Security Controls).

35 Recommendations were made to address horizontal findings (at the government-wide level). As such, when directed at more than one department, recommendations may apply entirely or only partially to the individual departments listed in this appendix, depending on the specific findings observed in each department.

36 Priority levels were assigned based on risks from a government-wide perspective. Given that the findings in each department varied, the level of risk from a departmental perspective may vary.

37 Recommendations 13-16 apply to all large and small departments listed in Appendix B. These recommendations do not apply to the lead security agencies included in the audit.

Date modified: 2020-09-28