Audit of physical security

Internal Audit and Program Evaluation Directorate
March 2026

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

Table of contents

Introduction

The Government of Canada (GC) safeguards its people, information, and assets through a comprehensive security framework governed by the 2019 Treasury Board Secretariat's (TBS) *Policy on Government Security* and the accompanying *Directive on Security Management*. The policy defines eight key security controls, one of which is physical security. Physical security refers to the measures implemented to protect people, property, and physical assets from physical threats.

The Canada Border Services Agency (the CBSA or the agency) plays a vital role in ensuring the safety, security, and prosperity of Canada by managing the movement of people and goods across the border. For example, between 2023 and 2024, the agency processed over 89 million travellers and over 25 million commercial releases[1]. To effectively deliver its critical mandate, the CBSA must maintain a safe

[1] Canada Border Services Agency's 2023 to 2024 Departmental Results Report: At a glance

and secure operational environment where its personnel, facilities, information, and assets are protected from security threats and vulnerabilities.

As per the *Policy on Government Security*, the CBSA must establish security governance including responsibilities for security controls and authorities for security risk management decisions while identifying security management requirements for all departmental programs and services.

At the CBSA, these responsibilities and accountabilities are defined in the *Framework on Security Program Management* and the 2024 *Policy on Physical Security* and establish the following roles.

- The Chief Security Officer, designated by the President, is the functional lead responsible for managing the Security Program (including the physical security function), implementing and maintaining security governance; and providing oversight for security activities.
- Security practitioners are responsible for providing advice to management and delivering security services.
- The National Real Property and Accommodation Directorate (NRPAD or Real Property) and the Major Projects Office (MPO), within the Finance and Corporate Management Branch (FCMB) Branch, cost physical security requirements in order to allocate funding and integrate security considerations throughout the lifecycle of facilities and assets. Regions and program areas are responsible for integrating security considerations into their respective operations.
- All employees have a responsibility for adhering to government security policy and departmental security practices, including safeguarding information and assets under their control, whether working on or off-site.

In addition to the above, the CBSA must work with third parties who own and maintain some of the buildings that the CBSA operates within, particularly those covered under Section 6 of the *Customs Act*.

Security program

The Security Program sits within the Security and Professional Standards Directorate, which as of 2024, moved from FCMB to the new Recourse, Standards and Program Integrity Branch (RSPIB). The CBSA's Security Program includes the physical security control function, among others. Key areas involved in physical security include the Security and Emergency Management Programs Division that provides policy direction, design and reporting, the Security Operations Division (SOD) that operationalizes the Security Program, including the conduct of activities related to physical security such as managing security incidents and events. The Infrastructure Security Systems Division that manages technologies and assets such as Closed-Circuit Television (CCTV) and the Professional Integrity Division that investigates security incidents where employee misconduct might be involved.

About the audit

The objective of this audit was to assess whether the CBSA has implemented physical security governance, controls and risk management processes, in compliance with relevant GC policies, to support the protection its employees and safeguarding of assets and infrastructure.

Audit scope inclusions

The scope period spanned April 1, 2022, to September 30, 2025, and centered on physical security governance and oversight, internal controls and processes such as risk management, and monitoring and reporting of physical security activities.

Audit scope exclusions

- Processes and practices related to the seven other security controls[2] listed in the TBS *Policy on Government Security*, except where they directly intersect with physical security controls (such as physical security related awareness and training for security practitioners).
- Business continuity management, though it supports the physical security control, is excluded, as it is slated for a standalone upcoming internal audit.
- Secure storage, transport, transmittal and destruction of information in physical form; however, secure storage was referenced as part of site walkthroughs.
- Physical security controls related to duty firearms and seized goods or currency, as these areas were both recently audited.

Audit methodology

- 300+ documents reviewed
- 75+ stakeholders interviewed
- 18 sites visited with walkthroughs in the Southern Ontario Region (SOR), the Northern Ontario Region (NOR), the National Capital Region (NCR), the Pacific Region (PAC) and the Quebec Region (QUE)

Significance of the audit

The CBSA employs approximately 16,000[3] people in hundreds[4] of facilities across Canada and manages billions of dollars worth of information and assets[5]. Failure to adequately protect and ensure physical security can result in serious consequences, including injury or death, loss or compromise of assets, operational disruptions, risk to national security, legal liabilities, and the erosion of public trust.

Events such as unauthorized entry and access to assets and sensitive information are just some of the threats that the agency is exposed to and underscores the importance of maintaining an effective physical security posture and supporting program.

A physical security function relies on key elements including defined and effective governance; a robust risk management process; and controls such as the GC's mandatory physical security procedures, to

[2] Security Screening, Information Technology, Business Continuity, Information Management, Security in Contract and Other Arrangements, Security Event Management, Security Awareness and Training

[3] 2024 to 2025 Departmental results report

[4] Canada Border Services Agency reports three escapes at Laval Immigration Holding Centre - Canada.ca

[5] 2025, CBSA Departmental Security Plan

mitigate identified risks. Together, these components form the foundation of a physical security function that can effectively fulfill its purpose of protecting people, information, and assets from physical security threats.

This Audit was approved as part of the 2024 to 2025 Risk-Based Audit Plan.

Statement of conformance

This audit engagement conforms to the Treasury Board's Policy and Directive on Internal Audit and the Institute of Internal Auditors' (IIA) Global Internal Audit Standards, as supported by the results of the quality assurance and improvement program. Sufficient and appropriate evidence was gathered through various procedures to provide an audit level of assurance. The agency's internal audit function is independent, and internal auditors performed their work with objectivity as defined by the IIA's Global Internal Audit Standards.

Audit conclusion

The CBSA operates within a large and complex environment delivering services to Canadians in hundreds of ports of entry across the country. Evolving security threats, aging infrastructure and resource constraints are some of the challenges that the agency faces as it addresses its physical security needs.

Overall, the CBSA has implemented physical security governance, controls and risk management processes in compliance with relevant GC policies. However, shortcomings in physical security risk management and its associated governance have contributed to weaknesses in physical security controls. This includes security assessments that are missing or outdated for a number of facilities with limited tracking of the associated recommended security measures. The agency had developed extensive guidance material to support the assessment of its facilities; however, opportunities exist to further ensure these materials are leveraged in a consistent manner. Increased participation and collaboration from all key stakeholders would improve decision making and oversight of the implementation of security measures. The agency has introduced new processes to improve the mitigation of risks and vulnerabilities, however clarifying roles and responsibilities and adding precision to processes and procedures would support overall success and help in the delivery of a risk-based approach and plan.

Addressing these challenges is key to ensuring a robust physical security function.

Summary of recommendations

To address the identified gaps, the audit recommends that the agency:

1. Ensures that there is a governance process that includes all physical security stakeholders and addresses all physical security matters, including:
    a. overseeing the development, funding, implementation and tracking of recommendations from Threat and Risk Assessment (TRAs) and documentation of all associated decisions

   b. escalating issues based on defined thresholds for management decision making
2. Clarifies, updates and communicates physical security policies and procedures related to:
   a. roles and responsibilities for all stakeholders involved in the risk management of a TRA
   b. expectations for when physical security activities should be conducted along with oversight responsibilities
   c. roles and responsibilities for regional operations including Regional Directors General (RDGs)
   d. expectations for stakeholder collaboration throughout physical security related projects
   e. a framework to determine thresholds for reporting security incidents to senior management and when a TRA is needed following a security incident
3. Improves the integrity of its physical security data and reporting by:
   a. ensuring that all facility and TRA information is complete, accurate and up to date
   b. conducting regular checks to ensure that all security-controlled assets including port stamps are accounted for
   c. assessing required physical security activities against capacity (including required training), agency priorities and the Departmental Security Plan (DSP) in order to develop physical security performance targets and report against their progress

Management response

The RSPIB welcomes the results of the Audit of Physical Security and accepts all recommendations made.

The Canada Border Services Agency (CBSA) maintains physical security measures at its facilities across the country. As part of its recapitalization and infrastructure projects, the agency also continues to invest in physical security elements such as intrusion alarm systems, distress alarms, lighting, fences, barriers and bollards, signage, doors, windows and other components of the Standard on Security Design for CBSA Facilities. In addition, over the past six years, the agency has made significant investments in and implemented a national level lifecycle management approach towards the recapitalization and maintenance of its inventory of CCTV and access control systems. In relation to the deficiencies identified during the audit at the 18 facilities sampled, some have already been corrected while others are being added to the program of work to be addressed.

The audit's recommendations confirm the key findings and work plan actions of the 2024 CBSA DSP related to Physical Security. Strengthening the physical security governance process for TRA recommendations will also yield improvements that can be shared Government-wide to ensure other departments benefit from the CBSA's advanced state of implementation of the Royal Canadian Mounted Police (RCMP) *Guide to the Facility Security Assessment and Authorization* (FSA&A) Process. In particular, this will include documenting decisions on Threat and Risk Assessment recommendations and compliance monitoring of their implementation. The RSPIB further agrees that the work carried out to improve security incident management and analysis will ensure appropriate alignment of TRA activities. Reporting on physical security will also be improved by the provision of the overall status of valid TRAs for CBSA facilities.

Audit findings

The audit resulted in the findings below.

Managing physical security risks

Assessing physical security risks in CBSA facilities

According to the DSP, the CBSA operates in over 1,000 facilities across Canada, some of which are owned by third parties such as Public Services and Procurement Canada, industry partners or owner/operators of Legislated Buildings per Section 6 of the *Customs Act*. Facilities include airports, land border crossings, mail processing centres, marine terminals, warehouses, telephone reporting sites and office buildings. The audit examined facility security in particular. The Security Program deemed 410 of these sites as critical based on various criteria such as the types of assets or information housed within and presence of officers. Of these critical sites, 248 were considered low risk and 162 high and medium risk facilities. There was, however, no documentation to show whether all 410 sites were assessed using the above criteria, and whether the list of critical facilities was complete. Such an assessment would support a well-informed understanding of the agency's threat environment, overall risk exposure, and management decision-making.

Threat and risk assessments

The agency's security threat and risk environment is assessed through the DSP, which is approved by the President. According to the RCMP (lead agency for physical security within the GC), the threat to a department or agency's facilities must be formally assessed on a periodic basis. This is done in large part through TRAS, used to identify and objectively determine the vulnerabilities and residual risk of a particular asset or facility and provide recommendations to address them. Per agency standard, facilities with a criticality rating of medium or higher should have a TRA completed every five years. According to the available physical security data, 312 out of 410 (75%) critical facilities, had no TRA or had a TRA that was more than 5 years old. Moreover, only 69 of the 162 (40%) medium and high-risk facilities had a valid TRA. This indicates that the agency does not have a comprehensive or up to date baseline understanding of the risks and vulnerabilities present in most of its facilities.

In February 2025, the Security Program updated its multiyear plan which outlined the approach to addressing the missing and outdated TRAs; however, the available data show a backlog of TRAs. A large number of facilities across all risk levels had planned TRAs that were late or had no plan for when they would be conducted. This included two high risk facilities with missing TRAs. Security's Program Management has attributed the low percentage of valid TRAs to other, higher priorities and limited human and financial resources, which inhibits practitioners' ability to travel. However, the audit found no documented assessment of the Program's capacity required to address its backlog. Risks associated with facilities can evolve over time; keeping security assessments current is an important element of protecting CBSA personnel, information and assets from potential threats and ensuring that the agency is not exposed to unknown security risks and vulnerabilities.

Data integrity

The audit reviewed the Program's available data on the facilities in use across all regions. Amongst other things, the data included the type of facility (such as airport, office) the facilities' risk or criticality rating (high medium and low), the ownership arrangement (custodial, leased or third party) and the date and link to the TRA last conducted. This data is tracked centrally by the National Headquarters (NHQ) Security Operations Coordination unit, within the SOD and manually updated by each security office.

The audit identified deficiencies in the availability and completeness of data, which are essential for establishing a reliable baseline understanding of completed and planned TRAs. Specifically, records were incomplete, with 60% of all site entries (245 of 410) missing information on their TRA completion status, and 79 of 410 sites (19%) lacking data on their criticality, impacting the overall quality of the information.

In addition to the above, the audit noted overall poor records management, with inconsistent retention of TRAs signed and approved by both Security and parties responsible for the facility, leaving it unclear whether the TRA process had been finalized. These gaps in information hinder:

- an accurate understanding of where investments are required and where residual risks may exist
- effective risk-informed business planning
- reporting risks and results to senior management

Refer to Recommendation 3 for the related recommendation for this finding.

Mitigating and monitoring physical security risks

As part of the TRA control process, the Security Program issues recommendations to mitigate identified vulnerabilities and lower residual risks to an acceptable level. The risks and associated recommendations are shared with the regional or program areas responsible for the facility in question. Regions and program areas then share the TRA with NRPAD and MPO, who determine the cost and the feasibility of the recommendations. Security recommendations that require infrastructure investments depending on scale and complexity are governed either through annual planning or investment planning processes, or, through project-specific governance structures. Additionally, stakeholders noted that, at times and in the absence of funds, regions may also make the decision to redirect funding to ensure recommendations were implemented.

Overall, the audit found limited tracking of TRA recommendations to determine whether the identified risks and vulnerabilities were mitigated. The audit reviewed 180 physical security TRA recommendations issued between April 2022 and April 2025 and could only confirm that 44 (25%) of them had been implemented. The remaining 136 recommendations (75%) were either not implemented or their status could not be confirmed, which indicates that vulnerabilities observed in the TRA may persist. The most common reasons supplied for the low implementation rate of the recommended measures were a lack of funding, they were structurally unfeasible and lacked prioritization (no distinction between mandatory and suggested measures), making it impracticable to allocate limited funds effectively. Consultations with other government departments, highlighted that challenges with tracking TRA recommended measures are not unique to the CBSA.

At the time of the audit, there was no policy expectation for the Security Program to track the implementation of TRA recommendations. In addition, there was no dedicated governance to support the prioritization of recommendations, assessment of feasibility and associated funding needs and establishment of risk tolerance along with mitigation plans. There was also no clear escalation path to senior management in instances where recommendations had broader agency implications, could not be implemented and risks had to be accepted. This is important because in addition to security requirements, facilities must also consider other evolving GC building codes related to accessibility, fire and emergency etc. Security design requirements are not embedded in NRPAD or MPO's infrastructure guidelines, making collaboration vital to ensure the agency balances all GC requirements, determines the most cost-effective approach that does not compromise security needs, and only accepts risks when necessary. Failing to track TRA recommendations and the actions taken to address them, does not provide assurance that vulnerabilities have been resolved and limits the effectiveness of the TRA process.

Refer to Recommendation 1 for the related recommendation for this finding.

Governing physical security

Facility security assessment and approval

In February 2025, the agency implemented the Facility Security Assessment and Approval (FSA&A) process. The process is a TBS requirement[6], meant to support transparency and increased accountability in the management of physical security risks. At the time of the audit, after a TRA is completed, the FSA&A process required one of three outcomes: responsible parties (Regions, Program Area, NRPAD or MPO) are to attest that the recommended measures:

1. are accepted and will be implemented
2. are acknowledged but an alternative, functionally equivalent mitigation will be implemented
3. will not be implemented, with no alternatives, and a responsible manager accepts the associated risks

The audit reviewed TRAs for two facilities conducted as part of the FSA&A and found that the process was not complete. The responsible parties did not fully agree with Security's recommended measures and had not yet signed the attestation. More broadly, concerns with the FSA&A process included insufficient budgets to implement security recommendations and unclear authorities to accept risks on behalf of the agency including for facilities owned and operated by third parties (such as tolled bridges, tunnels or airports). As per Section 6 of the *Customs Act*, third-party facility owners are responsible for funding and implementation some of the recommend measures identified in a TRA, while other costs such as CCTV are the responsibility of the agency. However, under the FSA&A process, an agency party must formally attest on their behalf for accepting the risk of not implementing recommended measures. Stakeholders were concerned that this may increase the agency's liability, particularly if security recommendations are not implemented.

[6] Directive on Security Management- Canada.ca, Section C.2.5

The audit reviewed the FSA&A guidance procedures and found that it includes a matrix which defines the levels of risk identified in the TRA (acceptable, possibly unacceptable or definitely unacceptable). It also includes the management level in the Security Program who can approve the identified risk level. This matrix, however, did not identify accountabilities for funding the work required to implement the associated recommended measures or to accept the risk when no alternatives measures could be found. Changes were being made to the matrix at the end of the audit to better reflect roles, responsibilities and accountabilities. Lack of clear roles and responsibilities can delay the implementation of security recommendations and work to reduce risks and vulnerabilities.

Refer to Recommendation 1 for the related recommendation for this finding.

The audit assessed whether there was governance to support oversight and decision-making as required by TBS. Effective security governance includes clearly defining those who are responsible and accountable, in order to ensure that security risks are managed, and that security investments align with risks and priorities. Physical security governance at the agency included the Executive Committee, the Agency Operations Committee, the Director General Steering Committee and the Security Program Functional Management Board (SPFMB or the Board). Based on a review of the mandate and membership of these committees, the SPFMB was the only body with a security-focused mandate responsible to set the strategic vision and direction of the Security Program. The Board was established in 2021 and according to its Terms of Reference was expected to meet four times every fiscal year and review and approve security risks, plans and strategies.

The audit found that the Board met at least three times a year. Though it did review and approve security risks and strategic plans, the gaps in the conduct of TRAs (refer to the section on performance measurement and reporting) and implementation of recommendations indicate that the Board did not have full awareness and oversight of the status of physical security risks in the agency. Neither NRPAD or MPO were members of the SPFMB, though they are primarily responsible for the funding and implementation of physical security requirements signalling that the governance did not fully reflect all those responsible and accountable for physical security risks. This is particularly important given that insufficient funding was the primary reason that security recommended measures from TRAs were not implemented. Additionally, there was no clear escalation path to SPFMB to ensure that investments in or decisions to not implement security recommended measures were appropriately governed.

During the course of the audit, the SPFMB was dissolved. Oversight responsibilities for physical security have since been revised, and related matters are now slated for initial discussion at the Director General Steering Committee, which includes both NRPAD and MPO. The Committee has a much broader, agency-wide mandate with a very high volume of issues to address, which may make sustained, detailed oversight for physical security challenging. Therefore, in order to provide comprehensive oversight, it is imperative that the Security Program provides accurate and meaningful reporting on the status of physical security activities (such as conduct of TRAs), residual risks and any challenges and needed resources to treat these risks to the appropriate authorities or committee. It is also important to establish a clear escalation path that outlines the issues and associated thresholds that must be brought forward to senior management for decision making. Clear governance that includes all key stakeholders facilitates appropriate oversight and management of physical security risks and decisions.

Recommendation 1

The Vice-president (VP) of RSPIB in collaboration with the VP of FCMB should ensure that there is a governance process that reflects all physical security stakeholders and addresses all physical security matters, including:

a. overseeing the development, funding, implementation and tracking of recommendations from TRAs and documenting associated decisions
b. escalating issues based on defined thresholds for management decision making

Management response: The VP of RSPIB in collaboration with the VP of FCMB agrees with the recommendation and will establish a process with all physical security stakeholders to govern decision-making required to finalize and document individual FSA&As including their development, funding, implementation tracking and, as necessary, escalation to the appropriate decision-making authority.

Completion date: March 2027

Physical security controls

Policies and procedures

TBS requires that departments define and document their physical security requirements and practices. Well defined policies support security practitioners and employees in carrying out their responsibilities. The audit mapped the CBSA's policies against the elements of the *Directive on Security Management*, Appendix C: Mandatory Procedures for Physical Security Control, to determine whether all requirements had up to date and accessible guidance with clear expectations for security practitioners and agency employees. All key requirements in the *Directive on Security Management* had a corresponding CBSA policy and/or supporting procedure. The policies and procedures were available to employees and security practitioners through the agency's intranet and those produced by Security were current and had been updated within the last five years.

The audit also assessed whether policies and procedures had defined roles and responsibilities, set clear expectations for when and how key physical security activities should be conducted, as well as the associated accountabilities. The Physical Security policy had defined roles and responsibilities for key stakeholders, but did not include RDGs. Some procedures did not consistently define expectations for when and how physical security activities should be conducted as well as oversight. For example, standards for security inspection (SI) did not include the required frequency for when they should occur. Additionally, guidance regarding review of access records by regions did not include NHQ's monitoring and oversight expectations. In addition, stakeholders expressed concerns that security responsibilities have increasingly been transferred to and absorbed by regional operations without clear communication and delineation of roles and responsibilities. Procedures that do not provide clear expectations can limit the Security Program and regions' ability to work in a harmonized, nationally consistent manner.

In addition, expectations for the timing of Security's consultation and involvement on infrastructure projects were not clearly defined. This led to varying perceptions of whether the Security Program was consistently involved in infrastructure projects, particularly at the planning phase. Physical security

activities whether carried out by the Security Program, or employees in regions and other branches, help keep the organization safe. A lack of clear policies, guidance, and expectations on when security activities should occur, who should be conducting them and most importantly the expected oversight, can result in security activities being missed, and additional costs when remedial measures need to be added after the fact.

Recommendation 2

The VP of the RSPIB should clarify, update and communicate physical security policies and procedures related to:

a. roles and responsibilities for all stakeholders involved in the risk management of a TRA
b. clear expectations for when physical security activities should be conducted along with oversight responsibilities
c. roles and responsibilities for regional operations including RDGs, expectations for stakeholder collaboration throughout physical security related projects
d. a framework to determine thresholds for reporting security incidents to senior management and when a TRA is needed following a security incident

Management response: The VP of RSPIB agrees with the recommendation and will clarify, update, and communicate the organization's physical security policy instruments related to the Facility Security Assessment and Authorization process, which includes the TRA. This will also include clarifying stakeholders' roles and responsibilities, establishing clear expectations and oversight responsibilities, defining regional operations and RDGs' roles and responsibilities, including stakeholder expectations by strengthening collaboration requirements.

Completion date: June 2026

Training, tools and resources

A combination of comprehensive policies, training, tools, and resources can enable security practitioners to develop the necessary knowledge, skills and competencies to carry out their duties. This includes technical knowledge of construction, infrastructure, building design and RCMP security guidelines, which are leveraged when conducting TRAs, site assessments and providing advice and guidance to various stakeholders. There currently is no required CBSA training to address these technical knowledge areas. As is also the case in other government departments, practitioners may be recruited to their position with limited or no security and/or infrastructure background and are required to apply RCMP guidelines without the necessary technical know-how. Newer practitioners primarily draw from on-the-job learning and mentoring from their more experienced colleagues. There is no budget allocated to training, meaning security practitioners cannot leverage relevant third-party offerings.

To bridge this training gap, the Security Program has developed a Security Profession and Career Development Training Plan, which recommends free training offerings based on the practitioner's level. However, the plan was not mandatory and additionally not known or leveraged consistently across regional security teams. As an additional measure, the Security Program offers optional, internally

designed workshops and information sessions, but does not delve into technical concepts required to effectively discharge a practitioner's role.

Currently there are 20 security practitioners with a primary responsibility to conduct TRAs, one of the more complex physical security activities. In addition to a small number of subject matter experts at NHQ, practitioners are located within the agency's seven regions, reporting to the Security Program NHQ. Informally, practitioners are expected to conduct two TRAs a year. Positively, the Security Program has developed a number of guides to aid practitioners in the performance of these assessments. The information is extensive and spread across multiple documents. Practitioners have developed their own checklists to help perform their TRAs, leading to inconsistencies in the elements assessed. For instance, one checklist included building construction details like window glazing and wall type, while another did not. A lack of standardization in TRA tools can lead to inconsistency in the assessments of risks in facilities (including those owned and operated by third parties) as well as in the recommendations to remediate vulnerabilities.

Refer to Recommendation 3 for the related recommendation for this finding.

Security inspections

TBS requires departments to conduct SIs in facilities where sensitive or valuable information or assets are handled or stored, or in facilities that support critical services or activities. They help assess whether assets are properly safeguarded when individuals are absent from their workspaces. SIs are shorter, less complex assessments than a TRA and can provide a status of the security of the facility in between the five-year TRA cycle. SIs, in combination with TRAs, support a robust physical security program, maintain high security standards and support security culture and awareness.

The audit team performed a walkthrough at one high risk site in order to observe security controls that are typically assessed during a SI, such as verifying the use of locked cabinets for sensitive information and locked computer screens when employees leave their workstation. The audit team then performed a number of walkthroughs in various locations to test access controls and employee behaviour regarding access to restricted areas. During these walkthroughs:

- The audit team members were able to access all secure and non-secure floors, unannounced, at various times of day, without access cards or visible CBSA identification. They were let in by occupants of the floors or entered through piggybacking (i.e. by following an authorized individual onto the floor). The audit team's presence was questioned on only one of the six secure floors and two of the nine non-secure floors.
- The audit identified two instances where employees left their workstations with computer screens unlocked and unattended; however, given the size and occupancy of the building, this was not a material rate of occurrence. The audit also noted sensitive documents left at printers, including financial documents and documentation containing personal traveller data including names, passage dates, passport numbers, and dates of birth. In some instances, the audit team was also able to consult paper documents with Protected B and C information, in cabinets that were left open, without being questioned.

These results highlight the importance of consistently conducting SIs, as a means to flag to management when training and awareness reminders for employees are warranted and to further support a security

minded culture. TBS does not prescribe SI frequency, but states that they should occur in accordance with the organizations' defined processes and timelines. The agency does not currently dictate how frequently SIs are expected to be conducted, however; security practitioners aim to perform them annually in any given location. Resource and travel limitations often make this unfeasible, particularly in geographically dispersed regions. The inability to conduct these assessments on a regular basis, combined with low TRA completion rates, contributes to a poor understanding of the agency's threat and risk environment, and impacts the agency's ability to mitigate security vulnerabilities before security incidents and events occur.

Safeguarding employees, information and assets

Physical security controls, in combination with the effective design and management of facilities, should create conditions that reduce the risk of violence to employees, protect against unauthorized access and activate an effective response and recovery plan in the event of a security incident. Effective physical security strategies leverage a combination of crime prevention through environmental design principles, electronic access controls, CCTV and alarm systems.

The audit assessed whether key physical security controls were in place and operating effectively for a selection of 18 facilities across Canada. The facilities were judgementally selected based on criteria such as high traveller and commercial volumes, representation across the four travel modes (air, land, marine and rail), building type (ports of entry and office buildings), ownership type (custodial, leased or Section 6), and no TRA completed in 2025. While the results cannot be statistically extrapolated, they are aligned with the most common recurring risks and recommendations made in the available TRAs reviewed by the audit.

The audit assessed a selection of basic physical security controls including CCTV, signage, condition of doors and windows, access controls, intrusion alarms, and perimeter controls such as physical barriers, illumination, fencing, landscaping and line of sight. Overall, physical security controls were generally in place and operational at all selected sites (refer to Appendix C for a summary of results). However, some important deficiencies and weaknesses were noted, particularly around CCTV and access controls.

Physical security control measures must incorporate elements of protection, detection, response and recovery concepts to mitigate risks and prevent the impact of any potential security incident in an organization. An effective control environment would ideally use a combination/mix of these controls especially for higher risk areas.

For example, security cameras, used alone, do not prevent a security event. However, when combined with locks and security guards (preventive controls), and perhaps an audible alarm (a detective control), they form a layered defense that significantly reduces the overall risk of an undesired event.

Note that single controls such as detective controls may be sufficient for lower risk areas but are not enough for higher risk areas.

CCTV and access controls

Though all sites had some form of electronic surveillance or CCTV infrastructure, issues were noted at nine of them (50%), including no coverage in key operational areas and low-quality resolution. For

example, one site had no CCTV installed at the primary inspection lane that process millions of commercial conveyances annually. Three other locations had no CCTV coverage in areas such as the bond rooms, where seized goods are held. The remaining five locations had CCTV cameras with poor resolution and in some cases images that were not visible. Plans for repair had been identified for two of the nine locations.

Access to and within facilities should be restricted to only those who have the authority and need. This can be achieved through various measures such as creating zones within the facility where access is progressively restricted and controlled. Tools such as electronic access management systems allow facilities to grant, track and restrict access privileges to the specific areas employees are authorized to be in. All selected facilities had discernible zones with access controls in place; however, deficiencies were noted. The most significant deficiencies were noted in one facility that had no electronic access management system; the entire Port of Entry (POE) leveraged locks with a pin code and/or keys with the same code for the entire facility. In addition, this facility had no intrusion alarm, although the audit notes that it is manned 24/7 with officers. Another three POEs had access management systems which were deemed to be at a very high risk of failure. These POEs were unable to make any changes to the system to issue access cards to new employee or make changes to the access for current employees including removing access altogether. According to the Security Program, repairs to the access management systems at these sites were slated for repair at the end of fiscal year 2025-26. The inability to manage access controls in real time and limit access to sensitive activities and information can expose the agency to vulnerability.

Intrusion, detection, access control and surveillance

One contributing factor to the poor status of CCTV and access control systems is the inconsistent management of the lifecycle of the various systems. Following a 2019 program evaluation, the agency developed plans and strategies to address gaps in both areas. With regard to CCTV, plans were developed, and progress has been made in replacing systems, however these initiatives are costly with complex infrastructure constraints in some facilities (such as old infrastructure with asbestos concerns). Progress includes 148 out of 164 identified CCTV projects across the agency that have been completed to date.

According to the Security Program, at least 80% of the agency's access control systems were operated independently by the regions or individual facility with no central awareness and management of their lifecycle. The Security Program conducted an assessment of the agency's 337 systems and identified 18 access control systems that had failed or were at a very high risk of technical failure.

At the time of the audit, the Security Program presented a five-year program of work to senior management and was seeking endorsement and funding approval to restore operational capability to 7 of the 18 critical access controls systems and for ongoing CCTV lifecycle management. In addition, the Security Program was also seeking approval to formalize an organizational unit at NHQ with the responsibility for centralizing and managing intrusion, detection, access control and surveillance, to help ensure that these technologies are consistently managed on a lifecycle basis. Given that work is underway in this area, no recommendations will be issued at this time.

Perimeter controls

Crime prevention through environmental design principles support the protection of buildings, a decrease in crime opportunities, the detection of intruders and the responses to security incidents. This involves the implementation of security features such as barriers, fencing, strategic lighting, and limited obstructions to reduce intruder hiding spots. Overall, all 18 facilities assessed by the audit had perimeter controls in place, however some deficiencies were noted including those with regard to barriers (refer to Appendix C for a summary of all results).

Barriers

Barriers such as bollards and cement blocks are important at operational areas in primary and secondary inspection lanes for safety, preventing accidents and to protect officers from vehicular impact. The primary and secondary examination areas in most locations had some barriers although there were variations in placement, type and the protection they offered. For example, the primary inspection lane booths at one high volume traveller port of entry had limited barriers and therefore sustained visible damage from larger vehicles including dents to the body and glass of all the booths. There was no available TRA for this facility and it is unclear whether this vulnerability had been previously identified by Security. This facility processes millions of travellers a year, as a result, adequate protection is paramount to ensure officer safety.

These deficiencies highlight the importance of maintaining a comprehensive understanding of the risks and vulnerabilities in the agency's facilities through up-to-date TRAs and other security assessments and the importance of ensuring that required mitigations are tracked and implemented.

Managing assets (port stamps)

The agency has five securities-controlled assets: port stamps, officer badges, and authority, designation, and identity cards. Of the five assets, the authority, identity, designation cards and officer badges are managed by Security while POEs manage the day-to-day movement of port stamps. The Security Program has the ultimate responsibility, of ensuring that inventories of all assets are kept up to date in the agency's Corporate Administrative System (CAS).

The audit leveraged its planned site visits and conducted a reconciliation of port stamps stored at POEs. Stamps were selected as they are the only asset not directly managed by Security. In addition, they are currently not being reviewed as part of the SOD national verification processes and had not been assessed for many years.

Port stamps are important because they are used to identify the date, location, purpose and duration of a traveller's authorized stay, or the personal and commercial goods entering and exiting Canada. They authenticate documents and identify the issuing officer as each stamp has a unique number associated to an officer in CAS. Compromise, such as a lost or stolen stamp, can directly impact the integrity of Canada's border and, per agency policy, must be reported to the Security Program and to the police.

Using CAS data, the audit assessed stamps at 14 locations and found that all the stamps in storage at the selected facilities were secured appropriately, located in locked cabinets. However, there were

significant discrepancies between the data in CAS and the spare stamps kept in POE storage. The most common explanations across all regions for the stamps that did not reconcile included: stamps were damaged, sent to Security and no longer on site, reassigned to an officer or another location, and/or location unknown. The audit also found stamps in storage that were not included in the CAS data, indicating that the CAS data was consistently out of date. Security practitioners noted that limited capacity and extensive movement of stamps made it difficult to keep the inventory up to date. The recent verifications by security have also identified gaps in the CAS data and status of cards and badges, although not to the same degree of those identified by the audit for port stamps. While CBSA policy requires a police report to be filed when a stamp is declared lost, the audit found limited awareness of this expectation. Poor tracking of stamps and out of date CAS data impedes the agency's ability to confirm that these security-controlled assets are accounted for.

Refer to Recommendation 3 for the related recommendation for this finding.

Maintaining an effective security posture

A security incident is any event (or collection of events), act, omission or situation that has resulted in a compromise. It can signal new and increased risk or vulnerabilities that need to be mitigated. Departments are required to have processes for the escalation and documentation of security breaches and incidents where a formal TRA is not warranted. This information, in combination with the results of security assessments such as TRAs and SIs, help to identify and monitor risk and take the necessary actions to ensure that physical security practices continually meet the needs of the agency. These actions ultimately help maintain an effective security posture.

The Security Program has service standards for responding to security incidents, but no defined and standardized escalation framework for reporting incidents to management or determining when a TRA should be conducted. For example, an unauthorized entry to a medium-risk facility which stores ammunition was reported in 2021 through the Security Incident reporting process. Three months later, a second incident occurred immediately outside the premises, although the facility was not breached. There was no follow-up assessment of whether these incidents warranted a TRA. The Security Program noted that the Security Operations Coordination Unit within the SOD was created in 2022 to address this issue.

While the Security Operations Coordination unit has developed a suite of procedures and tools for managing security incidents, there remains no defined framework. The Security Program confirmed that current incident report escalation is guided by security practitioners' professional judgement and experience, and that incidents considered to have a high or very high degree of injury are reported weekly to the Chief Security Officer. In some cases, incidents are reported to other government department stakeholders such as the RCMP or Public Safety.

In April 2025, the agency also launched the Security Event Management Reporting Tool, a digital tool to support better intake, tracking and reporting of security incidents. A defined escalation framework in addition to the new tool would enhance consistent and documented responses to security incidents, such as determining when a TRA should be conducted.

Refer to Recommendation 2 for the related recommendation for this finding.

Performance measurement and reporting

The Security Program reports its security activities in the Security and Emergency Management Program Annual Report (SEMPAR) to executive management and the Audit Committee; however, the report does not include data on the effectiveness of physical security across the agency.

The audit reviewed the 2024 to 2025 SEMPAR and found that the Program's annual reporting focused primarily on reporting a count of the activities that were conducted in a given fiscal year, such as number of TRAs or SIs completed; however, it did not indicate whether a performance target had been met or progress against physical security objectives. No other qualitative information such as general themes of identified or emerging risks were reported. In addition, the number of TRAs conducted in that fiscal year were both over- and under-reported. The biggest discrepancy was noted in one portfolio where 16 TRAs were reported as completed but only 5 were conducted. Reporting also did not indicate if a full TRA was completed as opposed to an assessment of parts of a facility, or whether the TRA was complete or still in progress.

The Security Program may be asked to conduct security assessments in relation to a new or ongoing infrastructure project. The SEMPAR does not distinguish TRAs that are conducted as a result of these requests and those that are planned. This limits visibility on the progress in addressing the 312 facilities with no or outdated TRAs including those that are high and medium risk. Overall, these concerns are important because TRAs and other physical security activities directly support management's understanding of the residual risks that are present in the agency's programs, facilities and general environment. Inaccurate reporting limits a clear understanding of the status of physical security activities and the ability to respond to and prioritize investments in needed safeguards.

Recommendation 3

The VP of the RSPIB should improve the integrity of its physical security data and reporting by:

a. ensuring that all facility and TRA information is complete, accurate and up to date
b. conducting regular checks to ensure that all security-controlled assets including port stamps are accounted for
c. assessing required physical security activities against capacity (including required training), agency priorities and the DSP in order to develop physical security performance targets and report against their progress

Management response: The VP RSPIB agrees with the recommendation to improve the integrity of its physical security data and reporting and will ensure the accuracy and completeness of facility and TRA information, maintain national oversight of security-controlled asset (stamps) and align physical security activities with available capacity to set and track performance target.

Completion date: March 2027

Appendix A: Audit criteria

Lines of enquiry	Audit criteria
1. Governance, oversight and risk management	1.1 The CBSA has an effective governance structure in place for the management and oversight of physical security. 1.2 Roles, responsibilities and authorities for physical security stakeholders are clearly defined, documented, understood and exercised in accordance with TBS requirements. 1.3 Physical security policies, procedures and guidance are in place and aligned with TBS requirements. 1.4 Risk management processes are in place to support business planning, the timely identification, documentation and reporting of risks and the implementation of mitigating controls.
2. Internal controls	2.1 Physical security controls are in place and operating effectively in accordance with internal and external policies.

Appendix B: Selected facilities

Region	Facility	Mode	Impact Rating*	Owner/ Operator	TRA Last Completed
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

*Facility Rating Score is assigned by the SOD to denote the impact if compromised and required security controls.

Appendix C: Summary of site visits

The following table includes a summary of the select safeguards assessed at each of the 18 facilities. [redacted].

Safeguard Assessed	Summary of Site Safeguards
[redacted]	[redacted]

Appendix D: Acronyms

CAS	Corporate Administrative System
CBSA	Canada Border Services Agency
CCTV	Closed-Circuit Television
DSP	Departmental Security Plan
FCMB	Finance and Corporate Management Branch
FSA&A	Facility Security Assessment and Authorization
GC	Government of Canada
MPO	Major Projects Office
NCR	National Capital Region
NHQ	National Headquarters
NOR	Northern Ontario Region
NRPAD	National Real Property and Accommodation Directorate
PAC	Pacific Region
POE	Port of Entry
QUE	Quebec Region
RCMP	Royal Canadian Mounted Police
RDGs	Regional Directors General
RSPIB	Recourse, Standards and Program Integrity Branch
SEMPAR	Security and Emergency Management Programs Annual Report
SI	Security Inspections
SOD	Security and Operations Division
SOR	Southern Ontario Region
SPSD	Security and Professional Standards Directorate
SPFMB	Security Program Functional Management Board
TBS	Treasury Board of Canada Secretariat
TRA	Threat and Risk Assessment
VP	Vice-president