Gouvernement du Canada | Government of Canada

Crown-Indigenous Relations and Northern Affairs Canada

Indigenous Services Canada

Internal Audit Report

Audit of Physical Security

Prepared by:

Audit and Assurance Services Branch

December 2017

TABLE OF CONTENTS

ACRONYMS

CIRNAC	Crown-Indigenous Relations and Northern Affairs Canada
DDSM	Directive on Departmental Security Management
DSO	Departmental Security Officer
DSP	Departmental Security Plan
HTRA	Harmonized Threat and Risk Assessment
ISC	Indigenous Services Canada
IT	Information Technology
PGS	Policy on Government Security
RBAP	Risk-Based Audit Plan
RSO	Regional Security Officer
SAD	Security and Accommodations Division
SSC	Sector Security Coordinator
SSIS	Security Services Information System
TBS	Treasury Board of Canada Secretariat
TRA	Threat and Risk Assessment

EXECUTIVE SUMMARY

Background

The Audit and Assurance Services Branch of Crown-Indigenous Relations and Northern Affairs Canada (CIRNA) and Indigenous Services Canada (ISC) included the Audit of Physical Security in the Indigenous and Northern Affairs Canada's 2017-2018 to 2019-2020 Risk-Based Audit Plan (RBAP), approved by the Deputy Minister on March 13, 2017. The audit was identified as a high priority because physical security and the well-being of employees as well as the safeguarding of assets are important to the achievement of the departmental business objectives. The audit was initiated in June 2017, and audit fieldwork concluded in September 2017. This report details the results of the audit.

Audit Objective and Scope

The objective of the audit was to assess the adequacy and effectiveness of the management control framework in place to support the physical security function at CIRNA/ISC as well as its compliance with the Treasury Board's *Policy on Government Security* and other relevant policies, directives and standards.

The scope of the audit was to examine the management control framework, including the governance, risk management and internal controls in place to ensure the protection of personnel and the safeguarding of assets and information.

Due to other audit work completed or underway, there were some scope exclusions. Accordingly, the scope focused on physical security and excluded other components of government security, including IT security, occupational health and safety, and business continuity planning. Additionally, while audit work assessed the processes and controls in place to safeguard assets, asset management practices were excluded from scope. The scope of the audit also excluded environmental assets, real property, and vehicles, as well as buildings/facilities that are not being occupied by CIRNA/ISC employees.

Statement of Conformance

This audit conforms with the *International Standards for the Professional Practice of Internal Auditing*, as supported by the results of the quality assurance and improvement program.

Conclusion

A management control framework is in place to support the physical security function at CIRNA/ISC and its conformance to TBS *Policy on Government Security* and other relevant policies, directives and standards. However, opportunities for improvement were identified in the areas of roles and responsibilities, monitoring and oversight, training and awareness, and risk management, to better position CIRNA/ISC to counter physical threats to its employees and assets.

Recommendations

Based on observations made during the audit, the following three recommendations were developed:

1. The Director General of Human Resources and Workplace Services, in consultation with the Senior Assistant Deputy Minister of Regional Operations, the Assistant Deputy Minister of Northern Affairs Organization and Regional Directors General, should strengthen the governance framework for physical security by:

    - Ensuring that the approved roles and responsibilities and security requirements are implemented as expected throughout the Departments; and
    - Strengthening monitoring and oversight to promote the achievement of physical security objectives and requirements.

2. The Director General of Human Resources and Workplace Services should strengthen the risk management of physical security by:

    - Formalizing and communicating the departmental methodology to support the completion of TRAs including sharing the indicators used to assess threat and risks with stakeholders; and
    - Implementing a formal process to monitor TRA completion as well as the implementation of TRA recommendations.

3. The Director General of Human Resources and Workplace Services, in consultation with the Senior Assistant Deputy Minister of Regional Operations, the Assistant Deputy Minister of Northern Affairs Organization, and Regional Directors General, should strengthen the governance framework for physical security by:

    - Reinforcing and communicating policies and procedures to promote improved communication and collaboration between labor relations and accommodations functions when performing activities involving physical security;
    - Assessing regional disparities in physical security measures and confirming whether they are appropriate and risk-based; and
    - Performing a review to identify prioritized security training needs and updating the departmental security training & awareness program based on the results.

Management Response

Management is in agreement with the findings, has accepted the recommendations included in the report, and has developed a management action plan to address them. The management action plan has been integrated in this report.

1. BACKGROUND

The Audit and Assurance Services Branch of Crown-Indigenous Relations and Northern Affairs Canada (CIRNA) and Indigenous Services Canada (ISC) identified the Audit of Physical Security in the Department's 2017-2018 to 2019-2020 Risk-Based Audit Plan (RBAP), approved by the Deputy Minister on March 13, 2017. The audit was identified as a high priority because physical security and the well-being of employees as well as the safeguarding of assets are important to the achievement of the departmental business objectives. The audit was initiated in June 2017, and audit fieldwork concluded in September 2017. This report details the results of the audit.

1.1 Context

Physical security is defined as the use of physical safeguards to prevent or delay unauthorized access to assets, to detect attempted and actual unauthorized access and to activate appropriate responses. It consists of the measures in place to reduce the risk of workplace violence and to ensure that information, assets, and facilities are protected from unauthorized access, disclosure, modification or destruction, in accordance with their level of sensitivity, criticality and value. Physical security also protects the people working with and within the organization. Departments must ensure that their physical security strategy incorporates identifiable elements of protection, detection, response and recovery.

A strong physical security function is essential to protect personnel and to safeguard assets and information. The management of security, including physical security, intersects with other management functions including access to information, privacy, risk management, incident and emergency management and business continuity planning, occupational health and safety, real property, materiel management, information technology (IT) and finance. Management of security also requires the continuous assessment of risks and the implementation, monitoring and maintenance of appropriate internal management controls involving detection, prevention, mitigation, and implementation of corrective measures.

The Treasury Board of Canada Secretariat (TBS) *Policy on Government Security (PGS)* ensures that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management.[1] Deputy Head responsibilities include establishing a security program for the coordination and management of departmental security activities, approving the departmental security plan, ensuring the integration of security requirements into departmental activities, and ensuring that investigations are conducted when security issues arise. Deputy Heads are also responsible for appointing a departmental security officer (DSO) to establish and direct a security program.

The PGS is supplemented by the TBS *Directive on Departmental Security Management (DDSM)*. The objective of the DDSM is to achieve efficient, effective and accountable management of security including roles and responsibilities at various levels within

1 Policy on Government Security. TBS. (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578)

departments.[2] In accordance with PGS and DDSM, the TBS *Operational Security Standard on Physical Security* describes baseline physical security requirements designed for common types of threats that departments would encounter.[3]

1.2 Physical Security at CIRNA/ISC

To comply with the PGS and DDSM, CIRNA/ISC developed its Departmental Security Plan (DSP), a three-year plan to respond to departmental security requirements, including physical security, based on a security risk assessment. The DSP provides the Deputy Minister and senior officials with prioritized risk-based strategies, objectives and timelines for improving the Department's security posture that are aligned with the strategic priorities, programs, plans and processes. The departmental Security Management Framework includes various departmental policies and procedures, which provide department-specific security guidance on how to meet the security requirements set out in the PGS.

At CIRNA/ISC, the responsibility for the physical security function falls under the Security and Accommodations Division (SAD) (also referred to in this report as "headquarters") within the Human Resources and Workplace Services Branch. The Departments also has security resources outside SAD, which are located in each sector and region. The Regional Directors General have overall accountability for physical security at their regional offices and regional security activities are carried out by Regional Security Officers (RSO). Furthermore, each sector has a designated Sector Security Coordinator (SSC). SSCs and RSOs report functionally to the DSO.

CIRNA/ISC operates a large decentralized network of offices, many of which are co-located with other government and non-government tenants. Maintaining appropriate control in these environments is inherently challenging and complex, particularly where CIRNA/ISC does not control central access to the facility.

2. AUDIT OBJECTIVE AND SCOPE

2.1 Audit Objective

The objective of the audit was to assess the adequacy and effectiveness of the management control framework in place to support the physical security function at CIRNA/ISC as well as its compliance with the TBS *Policy on Government Security* and other relevant policies, directives and standards.

2.2 Audit Scope

The scope of the audit was to examine the management control framework, including the governance, risk management and internal controls in place to ensure the protection of

2 Directive on Departmental Security Management. TBS. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579)

3 Operational Security Standard – Physical Security. TBS. (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329)

personnel and the safeguarding of assets and information. The audit work examined the following high priority areas as determined by the risk assessment performed during the planning phase:

- Governance, including the accountabilities, roles and responsibilities of departmental employees with security responsibilities as well as the governance structures in place for the oversight and management of the physical security function;
- Risk management, including the processes in place to systematically identify, document, assess, and mitigate physical security threats and risks; and,
- Internal controls, including the policies and procedures, training and awareness, and physical controls/processes in place to protect personnel, information and assets as well as monitoring, reporting and performance measurement against departmental physical security objectives

Due to other audit work completed or underway, there were some scope exclusions. The Department's Business Continuity Plan was excluded from the scope of this audit, as an audit was conducted in 2016-2017. Also, Occupational Health and Safety was excluded from the scope since this audit is planned in fiscal year 2018-2019. Furthermore, an Audit of IT Security was being conducted in parallel to this Audit of Physical Security and has been excluded from scope.

While our audit scope focused on the governance, risk management, and internal controls in place to support the safeguarding of assets, the assessment of asset management practices was excluded from scope. Additionally, the following assets were not specifically included in the scope of the audit: environmental, real property, and vehicles. The scope of the audit also excludes buildings/facilities that are not being occupied by CIRNA/ISC employees.

3. APPROACH AND METHODOLOGY

The Audit of Physical Security was planned and conducted in accordance with the Institute of Internal Auditors *International Professional Practices Framework* and in alignment with the TBS *Policy on Internal Audit*.

The audit was performed from June 2017 to October 2017 and consisted of three phases: planning, conduct and reporting. Based on information gathered during the planning phase, a risk assessment was completed to determine the most significant risks to CIRNA/ISC physical security. Audit criteria were developed to cover areas of highest priority as determined by the risk assessment and served as the basis for developing the detailed audit program for the conduct phase of the audit. Refer to Appendix A for the audit criteria developed for this audit, which were informed by relevant policies, standards, and guidance listed in Appendix B.

The conduct phase included the completion of audit procedures at headquarters as well as in three regions (Ontario, Saskatchewan and Manitoba). Audit procedures were also conducted through teleconferencing with three additional regions (Northwest Territories, Nunavut, and

British Columbia). During the conduct phase performed between August 2017 and September 2017, the audit team examined sufficient, reliable and relevant evidence to provide a reasonable level of assurance in support of the audit conclusion. The principle audit techniques used were:

- Interviews with key stakeholders
- Walk-throughs
- Physical inspections
- Documentation review
- Risk analysis

4. CONCLUSION

A management control framework is in place to support the physical security function at CIRNA/ISC and its conformance to TBS *Policy on Government Security* and other relevant policies, directives and standards. However, opportunities for improvement were identified in the areas of roles and responsibilities, monitoring and oversight, training and awareness, and risk management, to better position CIRNA/ISC to counter physical threats to its employees and assets.

5. FINDINGS AND RECOMMENDATIONS

Based on a combination of evidence gathered through interviews, facility walkthroughs, observation, examination of documentation and risk analysis, each audit criterion was assessed and observations were made. Where a significant difference between the audit criterion and the observed practice was found, the risk of the gap was evaluated and used to develop relevant recommendations.

Observations and recommendations below focus on the management control framework established for physical security, including the governance, risk management and internal controls in place to ensure the protection of personnel and the safeguarding of assets and information.

5.1 Governance

Oversight structures and mechanisms are expected to be in place to ensure the effective and efficient management of physical security within a department.[4] An effective physical security governance structure requires defined, documented and communicated accountabilities, roles, responsibilities and reporting relationships. Furthermore, physical security governance mechanisms (e.g. oversight committees) are to be established to ensure the coordination and

4 Policy on Government Security. TBS. (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578)

integration of physical security activities with departmental operations, plans and priorities.[5]

In alignment to the PGS, the Deputy Head has formally appointed a Departmental Security Officer (DSO) to implement the government security requirements, including physical security. The physical security governance structure is documented in the Department's Security Management Framework and its embedded documents, including the *Departmental Security Policy*, collectively referred to as the "Framework". The Framework is aligned to the requirements of *PGS* and its related *Directive on Departmental Security Management.*

Accountabilities, roles, and responsibilities of security practitioners are further defined in documents including, but not limited to, the DSO Handbook, RSO Terms of Reference, and the SSC roles and responsibilities document.

Additionally, the Departments has established committees that provide an oversight role over departmental security, including physical security. Specifically, there is a Departmental Security Committee, which provides advice, guidance and recommendations concerning departmental security. There are other senior management committees (e.g. Operations Committee, Internal Affairs Committee) that are involved in oversight and decision-making related to security; however, these committees have broader mandates and are involved with matters pertaining to physical security on an ad-hoc basis. The Departments has also established a monthly teleconference call that is chaired by the DSO and attended by security practitioners from across the headquarters, sectors, and regions. The monthly call provides a forum to share important updates and discuss security related matters.

Roles and responsibilities

Although roles and responsibilities are defined in documentation, there is an opportunity to strengthen their implementation in practice. For example, the RSO Terms of Reference contains a comprehensive listing of the various responsibilities to be carried out. However, we observed several instances where these roles are not being carried out consistently, including but not limited to, performing routine inspections (e.g. security sweeps) to support conformance to and promote awareness of physical security requirements; and maintaining an ongoing security/awareness program.

While each region has appointed an RSO that reports functionally to the DSO, the role is generally carried out on a part-time basis as the RSO typically carries out multiple other administrative roles outside of security. The roles and responsibilities are generally being carried out on a reactive basis and there were several instances where the RSOs did not find it attainable to proactively perform all defined roles and responsibilities. For instance, interviews demonstrated that carrying out RSO responsibilities such as conducting investigations, developing security design briefs and delivering security training are challenging due to high demands from a knowledge, experience and capacity perspective.

5 Directive on Departmental Security Management. TBS. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579)

Moreover, each sector has an SSC that supports SAD in carrying out security-related responsibilities. Unlike RSO who are directly responsible for the delivery of various physical security activities, SSCs roles and responsibilities are more focused on promoting physical security awareness and coordinating the completion of physical security activities, such as reporting identified issues/deficiencies to SAD and following up on physical security requests (access card applications, incident reports etc.). While these roles and responsibilities are documented, we observed an example where an SSC was not fully aware of the responsibilities associated with the role.

The roles and responsibilities of the RSOs and SSCs are essential to managing a system of processes and controls to protect, detect, and respond to physical security-related risks/issues facing the Department, as well as raise awareness of physical security requirements. CIRNA/ISC's ability to meet its physical security requirements at a department-level is dependent on regional and sectoral security personnel carrying out their defined roles and responsibilities.

Monitoring & oversight

The overall responsibility for managing the departmental physical security program falls under SAD; however, much of the conduct of physical security activities takes place at the regional level. While the Department has established mechanisms to provide oversight for the management of physical security and to communicate security related information to relevant stakeholders, departmental monitoring processes over the implementation of physical security requirements throughout the Departments is limited and informal. For instance, information sent from regions (e.g. incident statistics) is often not subject to headquarters monitoring and follow-up. In some cases, (discussed further in the *Risk Management* and *Internal Controls* sections), physical security requirements such as security sweeps and threat and risk assessments were not conducted at certain facilities, which may be attributable to limited oversight for these activities.

Given the decentralized organizational structure, strong monitoring and oversight practices are essential to ensure that physical security activities are carried out in a coordinated and integrated manner across the departments and physical security controls remain current and address significant threats and risks. Specifically, strong monitoring and oversight practices would allow the Departments to identify, escalate and address exceptions where physical security requirements and responsibilities are not being met. In turn, this will promote and better enforce the implementation of individual responsibilities to carry out physical security activities across sectors and regions.

Recommendation

1. The Director General of Human Resources and Workplace Services, in consultation with the Senior Assistant Deputy Minister of Regional Operations, the Assistant Deputy Minister of Northern Affairs Organization and Regional Directors General, should strengthen the governance for physical security by:
    - Ensuring that the approved roles and responsibilities and security requirements are

implemented as expected throughout the Departments; and
- Strengthening monitoring and oversight to promote the achievement of physical security objectives and requirements.

5.2 Risk Management

Management of physical security requires the continuous assessment of risks and the implementation, monitoring and maintenance of appropriate internal management controls.[6] Furthermore, departments are expected to develop, document, implement and maintain processes for the systematic management of physical security risks to ensure continuous adaptation to the changing needs of the Departments and threat environment.[7] A threat and risk assessment (TRA) is an essential activity carried out to support the management of physical security risks. To guide departments in the process of conducting TRAs, the Government of Canada has endorsed the *Harmonized Threat and Risk Assessment (HTRA) Methodology*.[8]

Through the TRA process, threats and risks are identified and assessed for a specific location. Based on the results of the assessment, recommendations may be made to provide additional safeguards or modify existing safeguards in order to achieve an acceptable level of residual risk.

Departmental methodology

The development of TRAs may be either contracted to external security firms or conducted in-house by security practitioners within SAD. As per CIRNA/ISC's Security Management Framework, the *HTRA Methodology* is to be adopted and consistently applied when developing TRAs for departmental facilities, including for the identification of assets and threats. While SAD has established a methodology for conducting TRAs, it is not aligned to the HTRA and has not been formally approved. Additionally, the methodology and criteria for assessment are not openly shared with relevant stakeholders, such as those responsible for making decisions on whether to accept or reject TRA recommendations (e.g. regional management).

Attaining senior management buy-in will strengthen the overall credibility of the TRA activity and reinforce the risk management of physical security. With improved transparency, relevant stakeholders will be made aware and fully confident in the process used to reach findings and recommendations.

Monitoring and follow-up

Departmental guidance on when to perform or update a TRA is not well established or communicated. Stakeholders, including regional management and headquarters security practitioners, were not aware of a defined policy statement or guidance on the conditions that should trigger the performance of a new TRA or an update to an existing TRA. In the absence of

6 Policy on Government Security. TBS. (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578)

7 Directive on Departmental Security Management. TBS. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579)

8 Harmonized Threat and Risk Assessment Methodology. Communications Security Establishment & Royal Canadian Mounted Police.

a well-communicated policy statement, it was unclear to stakeholders whether TRAs should be performed or updated on a regular and defined basis (e.g. every five years), as a result of emerging threats and risks identified at a regional or national level, or as a result of material changes to the physical work environment.

Additionally, monitoring is not being performed by headquarters on the completion of TRAs. Some CIRNA/ISC facilities have undergone multiple TRAs, while certain other facilities have not been subject to a TRA at all.

Moreover, there is no formalized process for headquarters to follow up on the implementation of recommendations from TRAs performed internally or externally. We observed instances where TRA recommendations were not tracked to resolution.

As per CIRNA/ISC's Security Management Framework, action plans are to be created and approved when a TRA report recommends implementing safeguards to mitigate residual risk to an acceptable level. However, at the regional level, there were instances where recommendations were not implemented and there was no supporting action plan or risk acceptance document in place.

While we did observe strong regionally-driven follow-up practices in two regions, whereby action plans for TRA recommendations were established with targeted timelines, assigned accountabilities and active monitoring (including examples of active engagement with SAD), a formal monitoring and oversight process for TRAs has not been established for the entire Departments.

By not proactively monitoring and following up on TRAs, the Departments are not able to ensure that physical security risks are being managed continuously and effectively throughout the Departments. For instance, proactive monitoring can ensure that TRAs are conducted as needed and TRA recommendations are actioned in a timely and effective manner. Furthermore, through effective management and oversight of the TRA activity, CIRNA/ISC will be better positioned to identify and mitigate pervasive gaps and vulnerabilities that could exist across the Departments.

Recommendation

2. The Director General of Human Resources and Workplace Services should strengthen the risk management of physical security by:
    - Formalizing and communicating the departmental methodology to support the completion of TRAs including sharing the indicators used to assess threats and risks with stakeholders; and
    - Implementing a formal process to monitor TRA completion in a timely manner as well as the implementation of TRA recommendations.

5.3 Internal Controls

The minimum physical security control objectives that a department must achieve to ensure its mandate and security requirements are met are established within the DDSM and are elaborated upon further in the TBS *Operational Security Standard on Physical Security*.[9] Physical security controls include those that are based on preventative measures, detection and response, and must be adapted to mitigate a department's specific threats, risks and vulnerabilities (as discussed in the *Risk Management* section).[10]

All CIRNA/ISC employees have roles in effectively implementing physical security controls. As mentioned previously, it is the responsibility of headquarters to monitor physical security controls across the Departments to ensure they remain effective in addressing the current physical security requirements as well as department-specific risks identified in risk assessments.[11] The government's approach to physical security is based on the premise that the design of facilities and physical security safeguards should create conditions that would reduce the risk of violence to employees, protect against unauthorized access, detect attempted or actual unauthorized access and activate an effective response.[12]

However, at various CIRNA/ISC facilities, installation of physical security measures must be approved by the landlord or the property manager (e.g. Public Services and Procurement Canada, Brookfield Global Integrated Solutions), and can involve Shared Services Canada in some instances. As such, CIRNA/ISC does not always have full control over the installation of physical security measures and it was noted that third party dependencies have caused delays or prevented installation in some instances.

Training & awareness

Appropriate and up-to-date training activities reduce the risk that physical security is inadvertently compromised by enabling employees to have the necessary knowledge and competencies to effectively perform their physical security responsibilities. Additionally, a departmental security awareness program helps ensure that employees at all levels are informed and regularly reminded of security issues and their security related responsibilities.[13]

CIRNA/ISC has established a departmental security awareness program that covers physical security. For example, there is an annual security awareness week, whereby security tips and materials are emailed to all CIRNA/ISC employees. Furthermore, security training material as well as indications that training is delivered to new RSOs exists. Security awareness training is also provided to new employees.

While there are training activities being delivered, there are opportunities to improve. For

9 Directive on Departmental Security Management. TBS. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579)

10 Operational Security Standard – Physical Security. TBS. (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329)

11 Directive on Departmental Security Management. TBS. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579)

12 Operational Security Standard – Physical Security. TBS. (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329)

13 Directive on Departmental Security Management. TBS. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579)

example, several RSOs expressed the desire for more training opportunities that would allow them to be better equipped to fulfill the broad array of responsibilities (e.g. conducting investigations, delivering regional security training activities) encompassed within managing the regional security activities. Training is essential for ensuring that security practitioners have the necessary knowledge and competencies to not only carry out their specific security related roles and responsibilities but to also transfer knowledge and promote awareness to all employees.

Additionally, staff members in regions often do not receive adequate training on physical security beyond the security briefing received when they first joined CIRNA/ISC. Examples of job-specific training that could be provided include security training on how to deal with conflict situations involving public interactions as well as how to identify and avoid potentially dangerous situations while travelling. Training should be made available to employees who are exposed to duties and situations by which workplace violence could arise.[14]

Protection

Physical security is required to be fully integrated into the processes of planning and designing facilities.[15] To meet this requirement, CIRNA/ISC's Security Management Framework specifies that security personnel are to be involved in the development of security design briefs, which is a document that aims to ensure that security considerations and requirements are factored into the planning and design phases for new facilities or renovations to existing facilities. However, instances where the security team was not involved in the planning and design of new facilities or facilities being retrofitted were identified.

While baseline physical security controls were generally observed to be in place at the regions visited, there were several instances of regional disparity in security measures and for which rationale was not known or documented. The following are examples:

- **Configuration and safeguards for Registration Offices**. Security measures provided for Registration Offices varied from facility-to-facility, including one facility that had no evacuation route to secure space, as well as no plexiglass or panic button in place to mitigate the threat of a hostile client. Additionally, Registration Offices in some regions are outside of the operational zones.

- **Safeguards for delivery of treaty payments**. Security measures in place for delivering treaty payments varied across regions. Specifically, we noted some regions with limited security measures (e.g. no security escort), which could increase the risk exposure for regional employees.

- **Dedication to security roles.** Some regions have created or are in the process of creating full-time positions for security roles, while other regions have these roles (e.g. RSO, Deputy RSO) performed part-time.

14 Directive on Departmental Security Management. TBS. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579)

15 Operational Security Standard – Physical Security. TBS. (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329)

- **Visitor access controls.** Some facilities did not have processes in place for visitor sign-in, including having visitors verify their identity and sign a visitor log book. Additionally, visitors are not always provided with a visitor ID badge to identify themselves as an approved visitor to the facility.

- **Presence of commissionaires at facilities.** Commissionaires are posted at some, but not all CIRNA/ISC premises, to monitor the control of access within the facility.

While there is no expectation to have a "one size fits all" approach to security across the Departments, there is an expectation that security measures will be commensurate to the level of threats and risks identified. Rationale for disparities in security measures were not always provided or known by interviewees. Furthermore, there was a general expectation of staff interviewed that their office should have similar levels of security as other regional offices. It is essential to leverage the departmental risk management process (i.e. TRAs) to analyze identified threats and risks and ensure that physical security controls and measures are implemented according to the level of risk identified. Taking a risk-based approach will help to ensure that management is addressing their physical security needs on a prioritized basis.

Detection and response

Detection and response are important components in ensuring an active defence strategy against physical security threats, vulnerabilities and incidents. One process employed by the Departments to detect non-compliance with physical security requirements (as well as promote physical security awareness) is security sweeps of facilities, which are governed by the Departmental Physical Security Inspection Procedures and required to be conducted on a routine basis by the Directive on Departmental Security Management.[16] While the documented departmental procedures were considered to be sound, issues related to the frequency, assigned responsibilities and documentation of security sweeps were observed.

There were several instances where security sweeps were not being regularly performed at facilities. Furthermore, sweeps were generally carried out by employees with security roles (e.g. RSOs, headquarters security practitioners); however, there was one observed instance where the task was informally assigned to administrative staff and there were no documented results. Additionally, some sites visited had documented sweep statistics such as the amount and percentage of unsatisfactory results by function, while other sites visited did not have any documented sweep statistics. The Departmental Physical Security Inspection Procedures requires that sweep statistics (e.g. number of annual notices, most common deficiencies) be collected and reported to security personnel, and used to track long-term patterns.

When security sweeps are not carried out, instances and trends of physical security breaches may go unnoticed for a prolonged period, at both a regional and national level.

Another detection and reporting control employed by CIRNA/ISC is the Security Services

16 Directive on Departmental Security Management. TBS. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579)

Information System (SSIS).[17] SSIS is the primary mechanism used to monitor and report on physical security activities across the departments (e.g. number of incidents in regions/sectors), however, it was noted by headquarters security practitioners that monitoring is generally not performed on the information uploaded to the system. Furthermore, there was a lack of clarity among regional stakeholders on how the information reported in SSIS was used by headquarters for monitoring and decision-making.

We also observed inconsistent practices in the data entry for SSIS. For instance, one region entered security incidents in infrequent batches as time permitted, and it was also noted by headquarters staff that regions did not always upload their incidents within the required timeframe (i.e. every 3 months). Additionally, we observed that the locking devices module (which tracks the departmental inventory of keys, alarms, secure telephones etc.) was limited in implementation (i.e. information not uploaded from regions), and not actively monitored and kept up-to-date.

If there are not consistent practices for uploading and monitoring information in SSIS, the reliability of the system as a central repository for monitoring and reporting on physical security activities may be impacted due to incomplete or inaccurate information.

In alignment with the DDSM, CIRNA/ISC has established procedures for conducting administrative investigations into security incidents; however, we were informed of issues related to the implementation of these procedures.[18] While there are standard operating procedures specifying how security personnel should be informed of and involved in investigations, it was found that security is not always informed of and fully involved in administrative investigations (both at a regional and national level), including those carried out by Labour Relations.

It is important that there be communication and collaboration with security personnel in investigations so that security input can be leveraged for various activities (e.g. gathering evidence, conducting interviews, closing files) and security-specific responsibilities such as deactivating access cards and retrieving departmental assets for suspended or terminated employees can be fulfilled.

Recommendation

3. The Director General of Human Resources and Workplace Services, in consultation with the Senior Assistant Deputy Minister of Regional Operations, the Assistant Deputy Minister of Northern Affairs Organization and Regional Directors General, should strengthen physical security internal controls by:
    - Reviewing, updating and communicating policies and procedures to promote improved communication and collaboration between Labor Relations and Accommodations

17 SSIS is a departmental system that was developed to manage, record, retrieve and report on security related information, including security clearances, incidents and locking devices.

18 Directive on Departmental Security Management. TBS. (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579)

functions when performing activities involving Physical Security;

- Assessing regional disparities in physical security measures and confirming whether they are appropriate and risk-based; and
- Performing a review to identify prioritized security training needs and updating the departmental security training & awareness program based on the results.

6. MANAGEMENT ACTION PLAN

Recommendations	Management Response / Actions (in consultation with the regions)	Responsible Manager (Title)	Planned Implementation Date
1. The Director General of Human Resources and Workplace Services, in consultation with the Senior Assistant Deputy Minister of Regional Operations, the Assistant Deputy Minister of Northern Affairs Organization and Regional Directors General, should strengthen the governance framework for physical security by:		Director General, Human Resources and Workplace Services in consultation with Senior Assistant Deputy Minister, Regional Operations and	
• Ensuring that the approved roles and responsibilities and security requirements are implemented as expected throughout the Departments; and,	1(1) The roles and responsibilities for the Regional Security Officers (RSO) were reviewed and agreed at the Operations Committee in July 2017. Regional consultations are underway to determine the best way to implement the RSO functions in the respective regions: <u>designated functions</u> vs <u>generic work descriptions</u>. Two regions, British Columbia and Québec, already opted to utilize a dedicated position to deliver services. A generic work description describing the RSO functions are available at the AS-05 and AS-03 level for the regions to use.	Assistant Deputy Minister, Northern Affairs Organization and Regional Directors General	Q2 2018-2019
• Strengthening monitoring and oversight to promote the achievement of physical security objectives and requirements.	1(2) NHQ Security will established an action plan to develop this capacity within its organization. Further consultation with regions is required to identify key performance indicators to monitor security activities.		Fy 2018-2019

2. The Director General of Human Resources and Workplace Services should strengthen the risk management of physical security by: • Formalizing and communicating the departmental methodology to support the completion of TRAs including sharing the indicators used to assess threat and risks with stakeholders; and • Implementing a formal process to monitor TRA completion as well as the implementation of TRA recommendations.	2(1) The methodology being used for conducting Threat and Risks Assessment (TRA) will be shared with each of the RDG responsible for the building where they are located. Two TRA reports have been completed, one for Manitoba and the other in British Columbia. The methodology will be share with them. 2(2) Action plans are developed by the regions in response to their TRA. These action plans are monitored by HQ Security and regular meeting take place to ensure common understanding and approach. A formal process to monitor TRA completion & implementation of TRA recommendation will be added as a specific objective of the new iteration of the Departmental Security Plan (DSP). As per the Policy on Government Security, the DSO is to report progress on the DSP to the Deputy Minister at least once a year.	Director General, Human Resources and Workplace Services	Q1 2018-2019 Fy: 2018-2019
3. The Director General of Human Resources and Workplace Services, in consultation with the Senior Assistant Deputy Minister of Regional Operations, the Assistant Deputy Minister of Northern Affairs Organization and Regional Directors General, should strengthen the governance framework for physical		Director General, Human Resources and Workplace Services in consultation with Senior Assistant Deputy Minister,	

security by: • Reinforcing and communicating policies and procedures to promote improved communication and collaboration between labor relations and accommodations functions when performing activities involving physical security; • Assessing regional disparities in physical security measures and confirming whether they are appropriate and risk-based; and	3(1) Establish mechanisms such as training (security briefs, Lockdown & Shelter in place, etc.), awareness sessions (messages in the Express, Security Awareness Week in February, Emergency Preparedness Week in May) and partnership with key stakeholder to improve communication, collaboration and the sharing of information. 3(2) Security Services will launch a review of regional security practices and measures in place to assess regional disparities (e.g.: commissionaires in some locations, none in others) and to determine whether they are appropriate for their environment and risk assessment. This item will be capture in the renewal of the DSP. In addition, physical baseline security measures, including Readiness levels for Federal Government Facilities measures were reviewed at the 2017 Security Workshop held in Winnipeg from October 24 to 26 contributing to consistent understanding of minimal physical security measures to be implemented. Security Services has developed the Security on-boarding package that will be provided to every new employee. The departmental security training & awareness program will be updated accordingly.	Regional Operations and Assistant Deputy Minister, Northern Affairs Organization and Regional Directors General	On-going activities Follow up to DAC Q1 2018-2019 Fy:2018-2019 Partially completed: baseline training identified in the RSO Terms of Reference.

• Performing a review to identify prioritized security training needs and updating the departmental security training & awareness program based on the results.	NHQ Security will engage with regions to determine gaps in training. Gaps identified will be address via a case-by-case approach to provide adaptive and tailored training for RSO. 3(3)The departmental security training & awareness program will be updated accordingly. In addition, shadowing experiences both with other regions and NHQ could be made available pending appropriate funding.		Q4 2018-2019 Fy:2018-2019

Appendix A: Audit Criteria

To acquire an appropriate level of assurance to meet the audit objective, the following audit criteria were developed.

Audit Criteria and Control Objectives	
1. Governance	
1.1	Accountabilities, roles and responsibilities of departmental employees with physical security responsibilities are defined, documented and formally communicated to relevant persons.
1.2	An organization structure for physical security has been established and operates in alignment with departmental operations, plans and priorities.
1.3	An oversight function has been established to ensure the coordination and integration of security activities with departmental operations, plans and priorities and to measure outcomes.
2. Risk Management	
2.1	The Departments has documented and implemented approaches to risk management of physical security, which include processes for risk identification, assessment, response, communication and monitoring
3. Internal Controls	
3.1	Policies and procedures have been established to support the delivery of the Department's physical security requirements
3.2	A departmental security training & awareness program covering physical security is established, to ensure that individuals are informed and regularly reminded of security issues and concerns, as well as trained to discharge their security responsibilities
3.3	Information, assets and facilities are protected from unauthorized access, disclosure, modification or destruction, in accordance with their level of sensitivity, criticality and value
3.4	Management employs a systematic and consistent approach to planning, monitoring and reporting physical security activities and results.
3.5	An incident management process is in place to detect, respond and report on physical security incidents.

Appendix B: Relevant Policies, Directives, and Guidance

The following authoritative sources were examined and used as a basis for this audit:

1. ASIS International publications (including Effective Physical Security, 4th Edition)
2. ISACA COBIT Delivery and Support (DS) 12: Manage the Physical Environment
3. Treasury Board *Directive on Departmental Security Management (DDSM)*
4. Treasury Board *Operational Security Standards on Physical Security*
5. Treasury Board *Policy on Internal Audit*
6. Treasury Board Management Accountability Framework (MAF)
7. Treasury Board *Policy on Government Security (PGS)*
8. Treasury Board *Standard on Security Screening*
9. RCMP Guidelines and Tools [including, but not limited to, Harmonized Threat and Risk Assessment (TRA) Methodology; Preparation of Security Briefs; Control of Access; and Protection, Detection, Response]

Key CIRNA/ISC policies, plans and directives examined during the audit included:

1. Security Management Framework
2. Departmental Security Policy
3. Departmental Physical Security Inspections Procedure
4. Departmental Security Plan
5. Directive on the Application of Administrative Measures Following Security Violations
6. Standard Operating Procedures - Administrative Investigations