Internal Audit Division

AUDIT OF SECURITY GOVERNANCE

FINAL REPORT

AUGUST 2017

Canada

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY 1

1.1 OBJECTIVES AND SCOPE 1
1.2 AUDIT CONCLUSION 1
1.3 SUMMARY OF RECOMMENDATIONS 1
1.4 STATEMENT OF ASSURANCE 2

2.0 INTRODUCTION 3

2.1 BACKGROUND 3
2.2 OBJECTIVES, SCOPE AND METHODOLOGY 3

3.0 OBSERVATIONS AND RECOMMENDATIONS 5

3.1 OVERSIGHT 5
3.2 SECURITY IS PART OF GOVERNANCE, PROGRAMS AND SERVICES 6
3.3 ACCOUNTABILITY 7
3.4 GOVERNANCE MECHANISMS 8
3.5 DEPARTMENTAL SECURITY OFFICER APPOINTMENT 9
3.6 ARRANGEMENT WITH THIRD PARTY 9
3.7 SECURITY PLAN 10
3.8 SECURITY CULTURE 10

4.0 CONCLUSION 11

5.0 ANAGEMENT ACTION PLANS 12

APPENDIX A – AUDIT CRITERIA 13

APPENDIX B – LIST OF ABBREVIATIONS 14

1.0 EXECUTIVE SUMMARY

1.1 OBJECTIVES AND SCOPE

The objective of this audit was to provide assurance on the adequacy and effectiveness of the governance of security.

The scope included information, personnel and physical security, and a review of the status of action plans following the Preliminary Survey conducted in 2013-2014. It focussed on the management of information security (hard copy and electronic) through its life cycle as well as physical security including access to the Public Prosecution Service of Canada's (PPSC) facilities/assets and employee protection. The audit also examined if proper governance structures for the screening of employees and contractors were in place. The audit scope did not include the Office of the Commissioner of Canada Elections as a bill has been tabled to move this office out of the PPSC.

The audit complied with generally accepted auditing practices and was conducted in accordance with the Treasury Board (TB) Policy on Internal Audit.

The audit methodology included the following:

- interviews with:
  - Deputy Director of Public Prosecutions (DDPP), Regulatory and Economic Prosecutions and Management Branch
  - Director, Administration Services and Chief Information Officer (CIO)
  - Departmental Security Officer (DSO)
  - Staff, Security Services
  - Regional Security Officers (RSO)
  - Business Coordinators / Administrative Support, Regions
  - Chief Federal Prosecutors (CFP)
- a review and analysis of documented policies, practices and procedures, and related corporate documents; and
- analysis of security data.

The planning and conduct phases of the audit were carried out between January and May 2017.

1.2 AUDIT CONCLUSION

The Internal Audit Division (IAD) assessed the adequacy and effectiveness of the governance of security against predetermined audit criteria based on the Policy on Government Security, the Directive on Departmental Security Management, the Guideline on Developing a Departmental Security Plan and auditor's judgement. Overall the governance of security at the PPSC is adequate and effective; however, there are areas for improvement in terms of formalizing existing relationships, delegation and enhancing communication.

1.3 SUMMARY OF RECOMMENDATIONS

The report includes the following recommendations addressed to the DSO:

- The DSO should complete a security manual with clear roles and responsibilities.

- The DSO should review how to best communicate security information to PPSC staff, including the usage of the PPSC intranet site.
- The DSO should review and update the Memorandum of Understanding (MoU) to ensure it reflects the PPSC's increasing role in security.
- The DSO should complete a Strategic Awareness program on security.

The following recommendation is directed at the Director of Public Prosecutions (DPP):

- The DPP should formally delegate the DSO with his responsibilities.

1.4 STATEMENT OF ASSURANCE

In my professional judgment as the PPSC's acting Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusion provided and contained in this report. The audit findings and conclusion are based on a comparison of the conditions, as they existed at the time of the audit, against pre-established and approved audit criteria that were agreed upon with the PPSC's management. The findings and conclusion are applicable only to the entity examined. The audit was conducted in accordance with the *Internal Auditing Standards for the Government of Canada*.

I appreciate the cooperation and assistance provided to the audit team by PPSC staff in Headquarters and regional offices.

Abdellah Ismaili
Acting Chief Audit Executive

2.0 INTRODUCTION

2.1 BACKGROUND

The Security Services unit reports to the Director, Administration Services Division. It includes:

- Manager, Security Services / DSO
- Physical Security Officer
- Personnel Security Officer
- Security Officer
- Employee Protection Plan and Business Continuity Planning (BCP) Security Officer

2016-2017 SECURITY SERVICES UNIT OVERVIEW

Salary ($)	O&M ($)	Total ($)	Full Time Equivalents
358,155	326,409	684,564	5

The PPSC receives Safety and Security Management Services from a Corporate Service Provider (CSP) as well, costed at $61,284 for the 2016/2017 fiscal year.

The PPSC's Security Services unit is responsible for the protection of employees, physical and information assets, as well as our facilities. It covers diverse areas such as security management, physical and personnel screening, emergency management and BCP.

The PPSC's IAD completed a Preliminary Survey on Security in November 2013. The PS identified the central deficiencies and allowed management to address high-risk areas prior to this audit.

The IAD conducted this Audit of Security Governance in accordance with the PPSC's 2016-2019 Risk-Based Audit Plan which was approved by the DPP on March 29, 2016.

2.2 OBJECTIVES, SCOPE AND METHODOLOGY

The objective of this audit was to provide assurance on the adequacy and effectiveness of the governance of security.

The scope included information, personnel and physical security, and a review of the status of action plans following the Preliminary Survey conducted in 2013-2014. It focussed on the management of information security (hard copy and electronic) through its life cycle as well as physical security including access to the PPSC's facilities/assets and employee protection. The audit also examined if proper governance structures for the screening of employees and contractors were in place. The audit scope did not include the Office of the Commissioner of Canada Elections as a bill has been tabled to move this office out of the PPSC.

The audit complied with generally accepted auditing practices and was conducted in accordance with the TB Policy on Internal Audit.

The audit methodology included the following:

- interviews with:

  - The DDPP, Regulatory and Economic Prosecutions and Management Branch
  - The Director, Administration Services and CIO
  - The DSO
  - Staff, Security Services
  - RSOs
  - Business Coordinators /Administrative Support, Regions
  - CFPs
- a review and analysis of documented policies, practices and procedures, and related corporate documents; and
- analysis of security data.

The planning and conduct phases of the audit were carried out between January and May 2017. As this was an audit on governance, all lines of enquiry were within this area.

3.0 OBSERVATIONS AND RECOMMENDATIONS

3.1 OVERSIGHT

Oversight committees are appropriately established with clearly defined roles and responsibilities.

Governance is the combination of processes and structures implemented by the PPSC to inform, direct, manage and monitor the activities of the organization toward the achievement of its objectives. The audit expected the PPSC to have appropriate structures in place to provide effective oversight of security and that roles and responsibilities related to oversight of security were clearly defined, coordinated and communicated. An effective security program is a combination of the services provided by the Security Services team along with the use of security as part of strategic decision-making by the PPSC's management.

The PPSC Security governance-related oversight bodies include the Executive Council (EC) and the Security and Information Management Committee (SIMC). Their mandates clearly indicate what security-related areas they are responsible for.

The EC is chaired by the DPP, meets once a month and discusses and approves security-related items when such items are brought forth. EC mandated security responsibilities include approving directions and strategic plans and its mandate also expressly mentions delegating its decision-making to other committees.

Meetings with EC members found that the committees were appropriate with clearly defined roles and responsibilities.

The SIMC is the result of the merger of two committees, the Security Management Committee and the Information Management Committee. It is chaired by the Director of Administration who is also the CIO. The SIMC security responsibilities include the following:

- Taking into account regional, national and horizontal perspectives, policy directions and public sector management imperatives:
    - Reviews emerging issues and risks, strategic directions and PPSC priorities on security, information technology and information management, makes recommendations to Executive Council; and monitors progress.
    - Approves operational directives and plans as well as local initiatives on security, information technology and information management; and monitors progress.

Interviewees indicated that the merger of these two committees would reduce overlap and decrease gaps that had occurred with the previously existing Security Committee and Information Management Committee.

Members of the SIMC and the EC found the security responsibilities between these two committees to be well-coordinated with clearly defined roles and responsibilities.

3.2 SECURITY IS PART OF GOVERNANCE, PROGRAMS AND SERVICES

Security management is an identifiable and integral element of departmental governance, programs and services; however, there are areas of improvement in terms of documenting roles and responsibilities, security awareness and communication.

The audit expected to find that security management was an identifiable and integral element of departmental governance, programs and services.

Management interviewed noted that security is part of the culture of the PPSC and security is mentioned in all relevant documents such as the Departmental Plan, which includes Information Security and Safety of Staff as key risks. The Corporate Risk Profile includes both these risks, along with risk drivers, mitigation methods, consequences, responsibilities and due dates. A four year security plan goes into much finer detail as well. Security is considered integral to operations and the new SIMC has been formed to better provide input to EC on emerging risks and to approve operational directives and plans.

There is also a Security Plan for 2016 to 2020, approved by the EC, which expands on the above responsibilities, including objectives and target dates.

Reviewing EC's minutes, this audit also found that security was an important issue of discussion.

A comprehensive security manual with clear roles and responsibilities, supporting guidelines and procedures for all security activities, is currently in development by the DSO.

Interviews indicated that this manual intended to address a lack of clarity from some employees on their specific security requirements and on how to best integrate security into their work. Employees often obtain information informally – either by asking security officials or by asking other employees. Security training is not standardized; although, the DSO is developing training he hopes to be mandatory across the PPSC. The intranet is difficult to navigate and not all of the security documents are readily available. Some documents, such as the MoU with the CSP are not available at all.

Recommendations

1. *The DSO should complete a security manual with clear roles and responsibilities, supporting guidelines and procedures for all security activities.*

2. *The DSO should complete a Strategic Awareness program on security so employees are more familiar with their security obligations.*

3. *The DSO should review how to best communicate security information to PPSC staff, including the usage of the PPSC intranet site.*

3.3 ACCOUNTABILITY

Accountabilities, delegations, reporting relationships and roles and responsibilities of departmental employees with security responsibilities are defined, documented and communicated to relevant persons. Areas, such as formal written delegation of departmental security, could be clarified further.

Accountabilities are clearly defined and documented in most areas.

The Director of Administration and the DSO felt that accountabilities were clearly defined although the DSO was not familiar with his work description. There is also some overlap between Occupational Health and Safety and Security – both sections report to the Director of Administration – particularly in the areas of workplace violence and evacuation planning.

The DSO indicated that roles and responsibilities will be documented in a security manual; which is presently in the developmental stage.

An MoU between CSP and the PPSC exists and clearly lays out security responsibilities. However, it is not always being followed and much is done based on past practice. A CSP RSO stated he found the MoU quite clear, but admitted that he had been providing a service (accommodation support) that was not in the MoU and had been asked to stop. Simultaneously, the Quebec Regional Office expressed concern that not all of the responsibilities that the CSP accepted in the MoU are being met (changing the combinations of secure filing, involvement in the Employee Protection Program, involvement in the BCP, training sessions on safety for employees in the region).

The DSO stated the CSP continues to provide services based on past practice that are rightly his responsibility. The lack of a mutual understanding of this MoU has led to uneven service delivery. As the MoU is updated each year, there is an opportunity to make changes incorporating feedback from the DSO.

The MoU is not communicated to all PPSC staff. There is no Service Level Agreement that states specific service conditions, which organization provides which service, where it is provided or how it is delivered.

As part of the BCP, a plan for continuity of security services has been developed. It is a PPSC responsibility, but the CSP is involved.

Both the Director of Administration and the DSO stated the Director is performing some of the duties of the DSO with respect to strategic planning – the DSO is new to the organization and new to the DSO position. This is expected to change with time as the DSO takes on increasing responsibility.

The Privacy Breach Protocol has been updated since 2013 to reflect the role of the DSO. This is in line with the TB Guidelines for Privacy Breaches which requires that the Office of Primary Interest notify the DSO in the case of a breach.

It also states that participation of the Manager, Security Services, may be necessary and that the Manager, Security Services, should be part of the post-privacy breach analysis, which is in line with the TB Guidelines for Privacy Breaches.

The TB Directive on Departmental Security Management notes one responsibility is "ensuring that accountabilities, delegations, reporting relationships and roles and responsibilities of departmental employees with security responsibilities are defined, documented and communicated to relevant persons".

The DSO does not have a formal delegation agreement. In order to better define and document this responsibility, formalization of this role should be considered.

Recommendation

4. *The DPP should formally delegate security responsibilities to the DSO.*

3.4 GOVERNANCE MECHANISMS

Security governance mechanisms are established (e.g. committees, working groups) to ensure the coordination and integration of security activities with departmental operations, plans, priorities and functions to facilitate decision making.

Governance mechanisms have been established to ensure the coordination and integration of security activities with departmental operations, plans, priorities and functions to facilitate decision-making. Their membership and mandate are current.

The Chair of the SIMC (Director of Administration) is also a member of the Senior Advisory Board, which helps ensure continuity and coordination. The SIMC reports to the EC.

Safety of staff and information security are both listed as critical risks in the 2017–18 Departmental Plan.

The SIMC is to support the Deputy Head in the effective management of security, information technology and information management, to aid PPSC program and service delivery; foster informed decision-making; facilitate accountability and transparency; and contribute to effective government-wide collaboration.

Responsibilities include the following:

- Taking into account regional, national and horizontal perspectives, policy directions and public sector management imperatives:
    - reviews emerging issues and risks, strategic directions and PPSC priorities on security, information technology and information management; makes recommendations to Executive Council; and monitors progress; and,
    - approves operational directives and plans as well as local initiatives on security, information technology and information management; and monitors progress.

The PPSC has no sub-committee or working groups with a security role and the DSO has stated he is reviewing whether there is a need for additional working groups to deal with Security Governance issues.

3.5 DEPARTMENTAL SECURITY OFFICER APPOINTMENT

A DSO is appointed to manage the departmental security program. He is functionally responsible to the Deputy Head; however, he is not formally delegated.

A DSO has been appointed (sometimes called the Chief Security Officer). His work description charges him with managing the departmental security program in accordance with the TB Policy on Government Security. He understands his responsibilities. He reports to the Director of Administration.

The DSO and the Director of Administration confirmed that no formal delegation agreement exists. The DSO's responsibilities are well-understood but are only formally outlined in his work description.

The DSO and the Director of Administration agreed that the DSO functionally reports to the Deputy Head; however, this is not formally documented.

3.6 ARRANGEMENT WITH THIRD PARTY

The organization has a formal arrangement in place when the role of a DSO is being fulfilled by a third party, as required by the TB Policy on Government Security. However, there remains a lack of role clarity with respect to responsibilities for security governance and what the appropriate responsibilities should be.

The PPSC has a formal arrangement with the CSP in the form of an MoU that is being renewed each year. The service catalogue appendix of this MoU specifically lists Safety and Security Management services. There is also a Detailed Costing for the Provision of Internal Services between the CSP and the PPSC which includes Safety and Security Management Services as part of Administrative Services and has a sum of total cost included as well ($90,313 for 2016/2017).

Much of the work that the CSP RSO's perform for the PPSC are based on past practice and is not done by consulting the MoU. As the PPSC is a small organization, Security employees are often contacted directly by CSP employees which allows them to coordinate their work. The names of CSP RSO are not posted for PPSC employees online. Also, there is no delegation agreement with RSO from the CSP.

Services are often provided based on past practice without reference to the MoU. This sometimes results in the CSP delivering more services than desired and sometimes less than expected. There is frequent contact between the two in order to collaborate though.

The MoU is not posted on the intranet for PPSC employees to consult about specific security questions.

The DSO intends to take more security responsibilities from the CSP in the future.

Recommendation

5. *The DSO should review and update the MoU to ensure it reflects the PPSC's increasing role in security.*

3.7 SECURITY PLAN

A departmental security plan that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security and supporting its implementation is approved.

The PPSC has a Security Plan (SP) for 2016-2020 which was approved by the EC on February 9, 2017.

The PPSC 2016-2020 SP contains decisions for managing risks as well as strategies, goals, objectives, priorities and timelines for improving security and supporting its implementation.

The PPSC 2016-2020 SP also includes two key corporate risks identified as Safety of Staff and Security of Information. These key risks have mitigation frameworks, involved parties and target dates. There is also a risk assessment matrix listing seven risks with ratings between low and high.

The strategies the PPSC intends to take are listed as Security Management Actions for the most part and these involve concrete actions in the areas of governance, risk management, planning, implementation, threat, vulnerability and incident management and government-wide support.

The SP includes goals that PPSC Security is trying to accomplish.

There are eight security control objectives listed, which are concrete statements describing a particular desired outcome. These are listed with areas of management, involved parties and target dates.

There are two areas listed with timelines in this plan; one is for the implementation of security control objectives and the other for implementing mitigation methods for key corporate risks.

3.8 SECURITY CULTURE

The PPSC has a culture of not always appropriately setting security requirements based on what is actually required for each position, resulting in employees sometimes having the incorrect classification for the level of information they are able to access.

The PPSC had set the standard of having all positions require secret status due to the particularly sensitive nature of PPSC information, with exceptions possible. This has resulted in some security clearances of positions not being based on actual duties.

The Standard on Security Screening (which the PPSC has until October 2017 to implement) allows for enhanced screening to take place at the reliability level, when one's duties involve or directly support security and intelligence functions, or involve access to security and intelligence sources and methodologies. This allows for a Law Enforcement Records Check which the DSO has identified as an important change.

The DSO is presently investigating this change in order to create new PPSC direction in respect to this new standard. The inclusion of Law Enforcement Records Checks in a reliability clearance is expected to result in more positions being staffed at an enhanced clearance level which will reduce the workload of security officials and staffing times.

The Human Resources Management System Employees by Security Level report lists 854 employees with security clearances. Of these, there are 709 positions where the security clearance of the incumbent matches that of the position, 105 positions have a security clearance level lower than the person's security clearance and 40 positions have a security clearance level lower than the requirement. This is a high level of positions where the security clearance of the incumbent does not match that of the position.

PPSC direction on the clearance level needed for new and existing positions is based on the TB Standard for Security Screening. The DSO is in the process of creating written direction specific to the PPSC.

4.0 CONCLUSION

The IAD assessed the adequacy and effectiveness of the governance of security against predetermined audit criteria based on the Policy on Government Security, the Directive on Departmental Security Management, the Guideline on Developing a Departmental Security Plan and auditor's judgement. Overall the governance of security at the PPSC is adequate and effective; however, there are areas for improvement in terms of formalizing existing relationships, delegation and enhancing communication.

5.0 ANAGEMENT ACTION PLANS

RECOMMENDATIONS	MANAGEMENT RESPONSE AND ACTION PLAN	OFFICE OF PRIMARY INTEREST	TARGET DATE
1. The DSO should complete a Strategic Awareness program on security so employees are more familiar with their security obligations. ***Risk rating: Medium***	Management agrees and the item has been identified in the Security Plan 2016-2020. Security Services is working towards implementing a comprehensive mandatory awareness program for all employees and agents.	Security Services, Administration Division, PPSC	September 2018
2. The DSO should review how to best communicate security information to PPSC staff, including the usage of the PPSC intranet site. ***Risk rating: Medium***	Management agrees, all new/revised directives and procedures will be posted on the PPSC Security Services intranet site. The Security Services site is currently being updated in order to ensure all information is accurate and easily accessible.	Security Services, Administration Division, PPSC	On-going/ December 2017
3. The DSO should complete a security manual with clear roles and responsibilities, supporting guidelines and procedures for all security activities. ***Risk rating: Medium***	Management agrees and the item has been identified in the Security Plan 2016-2020. Security Services is developing a comprehensive security manual with clear roles and responsibilities, supporting guidelines and procedures for all security activities.	Security Services, Administration Division, PPSC	March 2018
4. The DPP should formally delegate the DSO with his responsibilities. ***Risk rating: Medium***	Letter was presented to the DPP and signed June 22, 2017.	Security Services, Administration Division, PPSC	N/A
5. The DSO should review and update the MoU to ensure it reflects the PPSC's increasing role in security. ***Risk rating: Medium***	Management agrees and changes to the MOU were discussed with the CSP, the Director of Administration Services and the DSO. Discussions are still on-going and a final implementation date was not determined.	Security Services, Administration Division, PPSC	September 2018

APPENDIX A – AUDIT CRITERIA

Lines of Enquiry	Audit Criteria
1.Governance	1.1 Oversight committees are appropriately established with clearly defined roles and responsibilities.
	1.2 Security Management is an identifiable element of departmental governance, programs and services.
	1.3 Accountabilities, delegations, reporting relationships and roles and responsibilities of departmental employees with security responsibilities are defined, documented and communicated to relevant persons.
	1.4 Security governance mechanisms are established (e.g. committees and working groups) to ensure the coordination and integration of security activities with departmental operations, plans, priorities and functions which facilitate decision-making.
	1.5 The appointed DSO is functionally responsible to the Deputy Head or to the departmental Executive Committee to manage the departmental security program.
	1.6 The formal arrangement between the service provider and the DSO sets appropriate responsibilities between the two.
	1.7 An approved departmental security plan details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security and supporting its implementation.
	1.8 The PPSC has a culture of appropriately setting security requirements based on what is actually required for each position.

APPENDIX B – LIST OF ABBREVIATIONS

CFP	Chief Federal Prosecutor
CIO	Chief Information Officer
CSP	Corporate Service Provider
DDPP	Deputy Director of Public Prosecutions
DG	Director General
DPP	Director of Public Prosecutions
DSO	Departmental Security Officer
EC	Executive Council
IAD	Internal Audit Division
MoU	Memorandum of Understanding
PPSC	Public Prosecution Service of Canada
RSO	Regional Security Officer
SIMC	Security and Information Management Committee
SP	Strategic Plan
TB	Treasury Board