PRIVY COUNCIL OFFICE

Risk Assessment of Personal Information Holdings

Audit and Evaluation Division

Final Report

August 19, 2016

Table of Contents

Acronyms Used in this Report

ADM-CSB	Assistant Deputy Minister, Corporate Services Branch
ATIP	Access to Information and Privacy
GAPP	Generally Accepted Privacy Principles
GoC	Government of Canada
HR	Human Resources
IM	Information Management
IMSO	Information Management Senior Official
PCO	Privy Council Office
PIA	Privacy Impact Assessment
PIBs	Personal Information Banks
RBAP	Risk-Based Audit Plan
SECOPS	Security Operations
TB	Treasury Board

1.0 Introduction

Canadians value their privacy and the protection of their personal information. They expect government institutions to respect the spirit and requirements of the *Privacy Act* (The Act). Recognizing that this protection is an essential element in maintaining public trust in government, the Government of Canada (GoC) is committed to protecting the privacy of individuals with respect to the personal information that it has under its control.

2.0 Authority

This Risk Assessment of Personal Information Holdings was approved by the Clerk as part of the Privy Council Office (PCO) 2015-16 to 2017-18 Risk Based Audit Plan (RBAP).

3.0 Objectives

The objectives of this Risk Assessment are to:

i. Identify the risks associated with the protection and management of personal information under PCO's control;

ii. Assess the relative significance of the risks in terms of the likelihood of each risk occurring and its impact should it occur;

iii. Determine whether existing controls as described by management and subjected to limited testing during this Risk Assessment are likely to prevent or mitigate the occurrence of the risks of greatest concern.

4.0 Scope

The scope of this Risk Assessment is department-wide in nature. It identifies and documents PCO's personal information holdings, where those holdings exist, and provides information on the controls and processes PCO is using to manage these holdings. The scope includes consideration of the Personal Information Banks (PIBs) contained in the *Info Source* system which describe categories of personal information collected by PCO including how that information is to be handled, used, retained, and disposed of. Given that this was a risk assessment and not an audit, limited testing of controls was done.

5.0 Context

Questions about the extent to which PCO has holdings of personal information and how these are managed were raised during each of the last two annual audit planning processes. This resulted in the inclusion of this Risk Assessment project in the Clerk-approved RBAP. The Act and the associated Privacy Regulations formed the backdrop for this Risk Assessment as they provide the legal framework for the creation, collection, retention, use, disclosure, accuracy and disposition of personal information in the administration of programs and activities by government institutions. The impact on PCO's reputation from any deficiencies in information management practices over personal information holdings was considered high.

The results of this Risk Assessment will be used to inform management decision making and future annual RBAP planning processes.

6.0 Approach, Methodology and Assessment Criteria

In 2009, the Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants, Inc. established a Privacy Task Force which developed a framework for privacy protection known as the *Ten Generally Accepted Privacy Principles* (GAPP). While these principles were developed based on various international privacy policies, regulatory requirements and best practices, they are consistent with GoC authorities on privacy and personal information holdings. The Ten Principles are: (1) Management; (2) Notice; (3) Choice and consent; (4) Collection; (5) Use, retention and disposal; (6) Access; (7) Disclosure to third parties; (8) Security for privacy; (9) Quality; and (10) Monitoring and enforcement.

In conducting audits and risk assessments in the area of privacy and personal information holdings, these Ten Principles are often used as standard benchmarks and as a source of criteria. For practical reasons, they can and have been framed in section 7.0 below into five (5) broad categories of (i) Governance and Accountability; (ii) Compliance Monitoring; (iii) Risk Management; (iv) Safeguards; and (v) Awareness.

The approach and methodology for this Risk Assessment involved risk identification, risk analysis, and risk evaluation. In conducting this Risk Assessment, the project team:

- Interviewed management and staff;
- Gathered, reviewed and analyzed key documentation including The Act, the associated Privacy Regulations, and other applicable authorities including Treasury Board (TB) policies, standards and guidelines; and
- Conducted limited walkthrough tests of key processes and controls.

Risk Assessment results were communicated with line management and a draft report was prepared and provided for acceptance to the Assistant Deputy Minister, Corporate Services Branch (ADM-CSB) in her role as PCO's Information Management Senior Official (IMSO). Draft project reports prepared by PCO's Audit and Evaluation Division are tabled at PCO's Audit Committee for review and acceptance, after which they are jointly recommended to the Clerk for formal approval.

7.0 A Privacy Management Framework Based on the GAPP

The following depiction presents a Privacy Management Framework based on grouping the Ten GAPP Principles into five (5) broad categories, as described above.

Governance and Accountability	**Compliance Monitoring**	**Risk Management**	**Safeguards**	**Awareness**
Management	Monitoring and enforcement	Collection Use, retention + disposal Disclosure to 3rd parties Quality	Security for privacy	Notice Access Choice and consent

PCO has internal control structures and mechanisms in place that relate directly or indirectly to the management of privacy matters and the handling and safeguarding of personal information holdings. As discussed in section 6.0 above, this Risk Assessment identified risks to the protection and management of personal information under PCO's control (see Appendix A).

The table below presents the results of this Risk Assessment against the five broad categories above and shows the Risk Assessment team's assessment of PCO's current posture against each category. The three-tiered legend which follows the table applies Low, Moderate and/or High ratings to indicate areas of strength or areas of concern.

	Risk Assessment of Personal Information Holdings	Rating
1	Governance and Accountability	🟩
2	Compliance Monitoring	🟩
3	Risk Management	🟩
4	Safeguards	🟩
5	Awareness	🟩

Rating Legend	
🟩	Low area of concern
🟨	Moderate area of concern
🟥	High area of concern

The sections which follow present description information on each the five (5) GAPP categories which support the project team's assessment of each category based on evidence gathered during this Risk Assessment.

7.1 Governance and Accountability

PCO has a formal structure of governance committees which manage all of the Departments activities and priorities. This formal structure includes Executive Committee supported by Corporate Management Advisory Committee, the Human Resources Advisory Committee and the PCO Audit Committee. Senior management also meet regularly as PCO Operations Committee where issues can be raised with the Clerk, including any threats or risks to PCO's personal information holdings. There are also a number of supporting committees which contribute to the governance and accountability mechanisms and processes at PCO.

Project interviews indicated that roles and responsibilities for the collection, disclosure, use and retention of personal information are communicated and understood. The Director of the Access to Information and Privacy (ATIP) Division is the designated Privacy Officer for the Department. The key secretariats and program areas that manage personal information include the Human Resources (HR) Division, Senior Personnel Secretariat, Youth Secretariat, Security Operations (SECOPS), and the Executive Correspondence Unit. The PCO Records Operations Unit within Corporate Information Services Division provides support for managing personal information holdings. This Risk Assessment indicated that there is a constructive working relationship between these business units and the ATIP Division and that per the TB *Directive on Privacy Impact Assessments*, Privacy Impact Assessments (PIAs) are carried out by the various business units and ATIP Division before new programs are set up. These activities are carried out under the leadership of senior officials in the ATIP Division.

In keeping with the 2014 TB *Policy on Privacy Protection* and other related authorities, PCO has standard PIBs registered with the TB Secretariat. These PIBs contain holdings of personal data on PCO employees. Under the auspices of the Privacy Officer, these PIBs are updated annually by the ATIP Division's Client Services Unit to reflect changes in PCO's personal information holdings. Appendix B presents an inventory of PCO's PIBs.

7.2 Compliance Monitoring

PCO must comply with applicable authorities including the *Privacy Act,* the *Policy on Privacy Protection*, the *Policy on Government Security,* the *Directive on Privacy Impact Assessments* and the *Directive on Privacy Practices.* PCO has established procedures, systems and other controls for the collection, retention, use, disclosure and disposition of personal information, and there are procedures in place which afford employees the opportunity to challenge compliance and seek redress if they feel their privacy or personal information may have been compromised.

PCO has a mature Information Management (IM) framework in place. A recent PCO audit in the area of IM concluded the Department has demonstrated compliance with the vast majority of the requirements of the TB *Policy on Information Management* and the *Directive on Recordkeeping*. To realize the strategic goals of the Government pertaining to risk mitigation and safeguarding of strategic information assets, the Department has developed a set of policy instruments to define and support PCO's IM outcomes and accountabilities. Specifically, management established a *Policy on Information Management* which came into effect on January 1, 2014. The policy sets out PCO's objectives, policy requirements, and accountabilities related to IM.

PCO's IMSO (the ADM-CSB) issued the PCO *Directive on Recordkeeping* on January 1, 2014 pursuant to the Department's *Policy on Information Management*. The Directive supports the governance and accountability processes outlined by the policy and sets out key recordkeeping processes including the identification, capture, and retention of records of business value. These processes help PCO manage its strategic information assets, including personal information holdings in accordance with GoC requirements and specifications.

As well, PCO complies with GoC retention and disposition requirements. Risk Assessment results indicate that there is controlled access to information storage both with respect to information in paper and in electronic format. The results of walk-through tests indicated that secure filing cabinets with combination locks are used for storing personal information as per the required GoC standards. PCO applies standard operating procedures for the disposition of information assets including personal information holdings.

As noted above, PIAs are carried out in PCO under the auspices of the ATIP Division before new programs are set up. The goals of the PIA *Guidelines* include the effective communication of "privacy risks not addressed through other departmental mechanisms" and "ensuring that privacy protection is a key consideration in the initial framing of a project's objectives and activities." By conducting the necessary PIAs, PCO mitigates against potential risks to privacy protection. This further reinforces the positive business relationship noted during this Risk Assessment between ATIP (headed by the Privacy Officer) and various PCO business units.

7.3 Risk Management

PCO has a risk management framework in place to support the management of personal information holdings. PCO has controls and procedures in place to ensure the limited collection, use, disclosure and retention of personal information. The aggregate of risk management mechanisms and controls, including access controls to computers and other electronic devices, are consistent with the GAPP and mitigate against the risk of unauthorized access to PCO's personal information holdings by unauthorized persons. Further, opportunities are available through the People Soft system and through other methods for employees to continually ensure the accuracy of their own personal information via confidential and safe means.

The holdings are stored in protected areas with well-secured controlled access points. Files are stored in secure cabinets with combination locks and, in the case of the ATIP Division, special ATIP software is used to collect personal information. Information is only shared on a strictly need-to-know basis and if required, personal information elements are either transmitted through PCO's secured CABNET network system, or if by hand, in locked security briefcases or stamped packages in double wrapped envelopes in compliance with required security practices. Overall, project results indicated these risk management practices prevail throughout PCO.

Risks are also managed through monitoring and supervision of staff. This facilitates the prompt escalation of issues for resolution by management and staff. In the ATIP Division for example, periodic meetings are held to ensure staff are updated on relevant files and issues, which is a practice that also serves to mitigate risks. As well, there are regular performance reviews to ensure that any performance issues are promptly addressed.

PCO's HR Division and SECOPS also play an important upfront role in risk management by ensuring all persons hired by the Department are security screened and undergo the necessary background checks. Thus, all employees who handle sensitive and personal information have been subjected to the required background checks before receiving their security clearances. This constitutes another layer of risk mitigation in the management of personal information.

While it is difficult to mitigate against or fully prevent a wilful breach of privacy and/or the intentional leakage of personal information, the access controls and layers of supervisory controls described above are designed to detect and thus mitigate against this risk. The protocols relating to the transmission of personal information through electronic means (transmitted through CABNET) and handling of documents also serve as controls to mitigate against the risk of a breach of privacy. Further, in addition to fostering an ethics and value-driven culture and atmosphere, PCO's whistleblower mechanisms for disclosure of potential wrongdoing also serve as a deterrent against potential intentional wrongdoing.

7.4 Safeguards

This Risk Assessment indicated that the various PCO business units that hold personal information have safeguards in place to protect personal information. While the electronic nature of repositories that store information such as InfoXpress and People Soft have inherent risks associated with them because they are electronic systems, through the institution of safeguards such as the use of encryption and secure passwords, unauthorized personnel are prevented from gaining access to restricted information. In addition to highly-restricted and controlled access including the use of alarm systems at repositories where personal information holdings are kept, there are well-secured GoC approved cabinets with combination locks and storage repositories with specific codes to store such data. Walk-through testing conducted by the project team indicated that the storage areas and facilities are secured from day-to-day environmental threats and hazards.

There are several layers of supervisory control over access and use of PCO facilities. In PCO business units such as ATIP, HR and the Senior Personnel Secretariat, security sweeps are conducted on a daily basis to ensure that there are no residual elements that may facilitate privacy breaches or pose a risk to privacy protection. SECOPS also has extensive safeguards and controls in place over its personal information holdings. As well, information management specialists from the Records Operations Unit within Corporate Information Services Division are assigned to assist key business units such as HR and the Senior Personnel Secretariat to manage day-to-day affairs relating to personal information holdings. These information management specialists are co-located in the respective business areas but report to the Manager of the Records Operations Unit.

Another layer of control can be found in the Department's Information Management framework. PCO, as part of its 2011 Recordkeeping Transformation Strategy, developed and is now using Recordkeeping Accountability Instruments in all major business units. These function as a control and oversight mechanism to safeguard the integrity of PCO's strategic information assets. This 2011 Strategy was developed to serve as a roadmap for implementing GoC policies and standards on strategic information management. The Recordkeeping Accountability Instrument requires senior officers in the various business units who are duly designated for that function to sign off on the integrity and safeguarding of information resources of business value in their respective branches and secretariats. As previously noted, the Department's IM Policy designates the ADM-CSB as PCO's IMSO to oversee the protection of PCO's strategic information assets.

When taken as a whole, the Department has an information management system with appropriate safeguards in place to promote the protection and integrity of its strategic information assets, including personal information holdings.

7.5 Awareness

PCO has a culture of awareness of privacy matters consistent with the GAPP. Employees in general appear to be aware of their rights and responsibilities of access to and correction of their personal information that is under the Department's control. Procedures and mechanisms are in place to support openness, transparency and individual access to one's personal information. Members of the general public who may be engaged with PCO through the Governor-in-Council appointment processes are also provided with these same rights and access opportunities.

The ATIP Division's Client Services Unit provides training and guidance to PCO staff to sensitize them on privacy matters and ATIP requests. The Unit's services are displayed on the Department's intranet site and business areas are invited to request training. This Unit provides one-on-one training as well as group training to groups of up to twenty on an as requested basis. In addition to any training provided by this Unit, employees can also receive training from both internal sources and from sources outside the Department.

PCO also has a strong Values and Ethics culture which is regularly reinforced through information distributed to all personnel. There is a clear "tone at the top" message against wrongdoing and unethical behavior. PCO's Values and Ethics Code was approved in April 2012, at which time all PCO executives, managers and employees were provided with copies of The Code and were required to officially acknowledge receipt of this document. The Code is now an integral part of the information package handed out to all new employees. Under the leadership of a Values and Ethics Champion at the Assistant Secretary level and supported by a team from HR, the Code is actively promoted. In addition to highly relevant information on PCO's intranet, there are cyclical publications and periodic publicity events to highlight the Code and ethical practices. The focus and emphasis on Values and Ethics plays a key role in sensitizing employees about potential acts of wrongdoing such as intentional privacy breaches or personal information leaks.

There are also readily available information materials on the Department's intranet site and publications available to employees on how to report suspicions of wrongdoing. These confidential avenues are not only provided by HR but by SECOPS and the Senior Disclosure Officer as well. One such instrument is the "*The PCO Process for Disclosure of Wrongdoing*." Such materials provide PCO personnel with the necessary information to understand the role of the Senior Disclosure Officer, the Public Servants Disclosure Protection Act and the protection afforded to employees under The Act.

Additionally, PCO promotes compliance with GoC policies and directives on PIAs. This function also serves as a mechanism to heighten awareness of safeguarding privacy and the integrity of the Department's personal information holdings. The *Guidelines on Privacy Impact Assessment* state that "a key goal of the PIA is to effectively communicate the privacy risks not addressed through other departmental mechanisms. The PIA is intended to contribute to senior management's ability to make fully informed policy, system design and procurement decisions." These Guidelines further outline as part of their specific goals "promoting awareness and an understanding of privacy issues" as well as "providing decision-makers with the information necessary to make informed policy, system design or procurement decisions based on an understanding of the privacy risks and the options available for mitigating those risks." Thus, by consistently conducting PIAs at PCO before the introduction of new programs and setting up of new organization entities, the culture and awareness of protecting personal information and privacy are promoted, thus helping to mitigate associated risks.

Individually and collectively these awareness mechanisms provide employees with easy access to information that is designed to improve awareness about managing personal information. However, when asked about areas where PCO could look for improvements in general, the response offered most often was to find ways to continue to improve employee awareness.

8.0 Risk Assessment Conclusion

PCO has a framework of management controls and other mechanisms in place for managing personal information holdings. While this Risk Assessment identified risks to the management of these personal information holdings, the limited testing performed suggests that a high level of compliance with applicable authorities is being achieved, and that controls in place are highly likely to mitigate and materially contribute to the prevention of the occurrence of the risks of greatest significance. With this framework of controls in place, the residual risk of a material breach in the Department's personal information holdings is considered low.

APPENDIX A – Significance of Identified Risks

This Appendix presents the list of potential risks to the effective management of PCO’s personal information holdings (below) and assesses their individual significance based on the Risk Assessment Team’s estimation at the end of the project and after considering mitigating controls that are in place of both the likelihood of the risk occurring and the impact on PCO should the risk occur.

The following table shows that likelihood and impact are estimated using a Low/Medium/High ratings scale, while the determination of significance at the conclusion of the project (based on the combination of likelihood and impact after considering mitigating control) is assessed for each risk as being either Negligible, Material or Critical.

While the impact of a risk may be estimated in the Medium or High range, the key variable is the likelihood of a given risk occurring.

Likelihood	Impact	Significance
High	**High**	**Critical**
Medium	**Medium**	**Material**
Low	**Low**	**Negligible**

Risk	***Likelihood***	***Impact***	***Significance***
Governance and Accountability			
1. There is a risk roles, responsibilities and accountabilities for collection, disclosure, use and retention of personal information are not well-defined and communicated.	*Low*	*Low*	*Negligible*
2. There is a risk program areas managing personal information are not clearly defined.	*Low*	*Low*	*Negligible*
3. There is a risk legal injury and reputational damage may occur in the event of a breach in personal information holdings.	*Low*	*High*	*Material*
4. There is a risk applicable processes/controls are not formally documented.	*Low*	*Low*	*Negligible*
5. There is a risk there is a lack of a comprehensive listing of PCO's personal information holdings.	*Low*	*Low*	*Negligible*
Compliance Monitoring			
1. There is a risk that the reasons for the collection of personal information are not disclosed to employees thereby undermining transparency and openness principles.	*Low*	*Low*	*Negligible*
2. There is a risk there are not effective monitoring processes and controls in place over the collection, retention and use of personal information.	*Low*	*Medium*	*Negligible*
3. There is a risk compliance exercises including Privacy Impact Assessments are not carried out periodically to ensure applicable laws and regulations are being followed.	*Low*	*Medium*	*Negligible*
4. There is a risk there are not effective controls in place to ensure the collection, retention, use, disclosure and disposition of personal information are carried out in accordance with applicable TB policies and directives.	*Low*	*Medium*	*Negligible*
Risk Management			
1. There is a risk PCO does not have an effective risk management framework in place to manage risks associated with collection, disclosure, use and retention of personal information.	*Low*	*Medium*	*Negligible*
2. There is a risk the types of repositories that store personal information may have peculiar inherent risks which have not been adequately addressed.	*Low*	*Medium*	*Negligible*
3. There is a risk there are not adequate systems or processes in place to ensure that in the event of privacy breaches, such issues can be quickly detected and remedied.	*Low*	*Medium*	*Negligible*

Safeguards			
1. There is a risk that there are not adequate safeguards in place to protect personal information in accordance with the *Privacy Act, Policy on Privacy Protection*, *Policy on Government Security, Directive on Privacy Impact Assessments,* the *Directive on Privacy Practices as well as other applicable GoC requirements and the GAPP.*	*Low*	*Medium*	*Negligible*
2. There is a risk that personal information holdings may be stored in areas and in conditions where they may be subjected to environmental hazards.	*Low*	*Medium*	*Negligible*
Awareness			
1. There is a risk employees may not be aware of their rights and responsibilities pertaining to access to their personal information.	*Low*	*Medium*	*Negligible*
2. There is a risk that employees who are not actively involved in the day-to-day management of personal information holdings may not be fully aware of the importance to PCO of ensuring the effective management of such personal information.	*Low-Medium*	*Medium*	*Negligible-Material*
3. There is a risk that PCO does not have a privacy management framework in place consistent with applicable GoC requirements and the GAPP.	*Low*	*Medium*	*Negligible*
4. There is a risk that Managers and personnel who handle personal information are not adequately trained on how to manage such information.	*Low*	*Medium*	*Negligible*
5. There is a risk that there are some weaknesses in the Department's management of personal information holdings which can facilitate an intentional or unintentional breach of the Department's personal information holdings.	*Low*	*Medium*	*Negligible*

APPENDIX B – Personal Information Banks

TBS defines Personal Information Banks (PIBs) as “descriptions of personal information that is organized or intended to be retrievable by a person’s name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.”

Treasury Board has developed Standard Personal Information Banks to describe personal information that may be created, collected and maintained by most government institutions to support common internal functions, programs and activities. The following are the key personal information banks listed:

Title	Bank Number	Related Record Number
Access to Information Act and Privacy Act Requests	PSU 901	PRN 930
Accounts Payable	PSU 931	PRN 914
Accounts Receivable	PSU 932	PRN 914
Acquisition Card	PSU 940	PRN 914
Applications for Employment	PSU 911	PRN 920
Attendance and Leave	PSE 903	PRN 941
Business Continuity Planning	PSU 903	PRN 928
Canadian Human Rights Act - Complaints	PSU 933	PRN 926
Discipline	PSE 911	PRN 926 & PRN 946
Disclosure of Wrongdoing in the Workplace	PSU 906	PRN 926 & PRN 931
Disclosure to Investigative Bodies	PSU 913	PRN 937
Electronic Network Monitoring Logs	PSU 905	PRN 932
Employee Assistance	PSE 916	PRN 922
Employee Performance Management Program	PSE 912	PRN 946
Employee Personnel Record	PSE 901	PRN 920
Employment Equity and Diversity	PSE 918	PRN 942
Executive Correspondence	PSU 902	PRN 943
Evaluation	PSU 942	PRN 916
EX Talent Management	PSU 934	PRN 920
Governor In Council Appointments	PSU 918	PRN 938
Grievances	PSE 910	PRN 926
Harassment	PSE 919	PRN 922 & PRN 926
Hospitality	PSU 908	PRN 933 & PRN 935
Human Resources Planning	PSU 935	PRN 949
Identification Cards and Access Badges	PSE 917	PRN 931

Internal Audit	PSU 941	PRN 916
Internal Communications	PSU 915	PRN 939
Library Services	PSU 936	PRN 944
Lobbying Act Requirements	PSU 937	PRN 904
Members of Boards, Committees and Councils	PSU 919	PRN 938
Occupational Health and Safety	PSE 907	PRN 922
Official Languages	PSE 906	PRN 923
Outreach Activities	PSU 938	PRN 904
Parking	PSE 914	PRN 901
Pay and Benefits	PSE 904	PRN 941
Personnel Security Screening	PSU 917	PRN 920 & PRN 931
Professional Services Contract	PSU 912	PRN 912
Public Communications	PSU 914	PRN 939
Real Property Management	PSU 948	PRN 948
Recognition Program	PSE 920	PRN 940
Relocation	PSU 910	PRN 936
Security Incidents and Privacy Breaches	PSU 939	PRN 931
Security Video Surveillance and Temporary Visitor Access Control Logs and Access Badges	PSU 907	PRN 931
Staffing	PSE 902	PRN 919 & PRN 920
Training and Development	PSE 905	PRN 927
Travel	PSU 909	PRN 934 & PRN 935
Values and Ethics Code for the Public Sector and Organizational Code(s) of Conduct	PSE 915	PRN 920 & PRN 926
Vehicle, Ship, Boat and Aircraft Accidents	PSE 908	PRN 922 & PRN 945

APPENDIX C – List of Interviewees (by title)

1. Executive Director – Human Resources Division
2. Executive Director – Security Operations
3. Privacy Officer and Director - ATIP
4. Deputy Director - ATIP
5. Chief, Client Services Division - ATIP
6. Policy Analyst - ATIP
7. Director, Compensation and Leadership Development - Senior Personnel Division
8. Director, Appointments - Senior Personnel Division
9. Manager, Records Operations - Corporate Information Services Division, Corporate Services Branch
10. Senior Policy Analyst – Youth Secretariat
11. Policy Advisor - Youth Secretariat
12. Deputy Chief Information Officer and Director of IT Operations – Information Management Services and Technology Directorate