HORIZONTAL AUDIT OF THE MANAGEMENT OF SENSITIVE INFORMATION

Internal Audit and Evaluation Division

April 2025

Public Prosecution Service of Canada | Service des poursuites pénales du Canada

Canada

As recommended by the Departmental Audit Committee, subject to approval by the Director of Public Prosecutions, on March 24, 2025.
Approved by the Director of Public Prosecutions on April 24, 2025.

Cette publication est également disponible en français.

This publication is available in HTML formats on the Internet at http://www.ppsc-sppc.gc.ca/eng/

Cat. No. J79-37/2025E-PDF

ISBN: 978-0-660-76650-8

CONTENTS

EXECUTIVE SUMMARY

Background

The Public Prosecution Service of Canada (PPSC) is a prosecuting authority that requires and generates a significant amount of classified and sensitive information. In the context of post-pandemic workplaces, employees have greater flexibility to work outside of the office while having access to a wide range of sensitive and/or protected prosecution file information. Unauthorized disclosure of such information (intentional or accidental) could seriously impact the reputation and integrity of the Department.

Security of information is identified as a key risk for the PPSC in the most recent Corporate Risk Profile exercise. Further, the occurrence of reported breaches of prosecution-related information has increased across the PPSC, especially as it relates to the improper/incomplete vetting of disclosure and/or court documents.

Therefore, senior management has an interest in the assurance that processes and controls are in place and functioning as intended to ensure the safeguarding of sensitive and classified prosecution file information (Protected C, Secret, and Top Secret).

Objective

The objective of the Horizontal Audit of the Management of Sensitive Information is to provide assurance that processes and controls are in place and functioning as intended to ensure the safeguarding of sensitive and classified information related to prosecutions, including the process of vetting court documents for disclosure.

Audit Conclusion

The PPSC has appropriate and functioning processes and controls in place for the management of sensitive information. However, easier access and limiting physical processes would increase efficiency and reduce the risk to the Department.

Communication targeted to the audience, which is more concise and regular, would further support understanding of the requirements for the management of sensitive information by both PPSC employees and agents. Also, supplementing agents' tools and facilities requirements with further detail is needed.

While appropriate training and awareness activities are taking place, more regular and targeted training would further support and promote awareness of the management of sensitive information.

Management of agents' security clearance is in place and functioning. However, not all PPSC employees had the correct security clearance for the work they perform, and some were not updated when due which is non-compliant with the Treasury Board of Canada (TB) Standard on Security Screening. PPSC employee security clearance is dependent on the employee and no monitoring is in place.

Some management of sensitive information reporting mechanisms are in place, but a more proactive approach to monitoring and reporting, particularly of security clearances and agents' facilities and tools, would mitigate risks. Finally, strengthening controls for vetting of court documents could reduce privacy breaches.

Summary of Recommendations

1. PPSC policy instruments regarding the management of sensitive information should have comprehensive language and contain roles and responsibilities for PPSC legal operations staff and agents and should be accessible to all PPSC employees and agents. (Medium)
2. Communication regarding the management of sensitive information to regions and agents should be effective, consistent, and sent regularly. This approach should consider distribution by an appropriate source, regional/agent context, and be concise. (Medium)
3. Mandatory training for PPSC employees should be defined, sufficiently available, occur regularly, and tracked for completion. Mandatory training requirement needs for agents should also be assessed. Consideration should be given to tailoring training to the realities of the management of sensitive information related to prosecution files at the PPSC. (Medium)
4. Implementation of digital solutions should be considered for the secure transfer of information that support improved efficiency and reduce the risk to the PPSC resulting from non-compliant actions. (Medium)
5. There should be awareness and alignment with the TB requirements for the security clearance level appropriate for the work being performed. Security clearances should be maintained in accordance with the TB Standard on Security Screening. (High)

GOVERNANCE PROCESSES

What we expected to find

We expected to find that the PPSC had a clearly documented framework, including roles and responsibilities, to support the management of sensitive information for both PPSC employees and agents.

We expected to find regular communication to promote awareness about relevant policies, directives, standards, and guidelines to both PPSC employees and agents.

Conclusion

While appropriate processes are documented and communication is taking place, supplementing agents' requirements with further detail is needed. Also, communication targeted to the audience, that is more concise and regular, would further support understanding of the requirements for the management of sensitive information by both PPSC employees and agents.

Findings

Policies and Processes

We found documented policies and processes have been established to support the proper management of sensitive information for both PPSC employees and agents.

However, roles and responsibilities were defined for PPSC in-house counsel and not legal support staff who are also involved in the handling of sensitive information related to prosecution files.

Policies and processes for agents, namely the Agent Agreement – Terms and Conditions, lacked detail for roles and responsibilities, preservation/retention and disposition of information, as well as tools and facilities. While regional Agent Supervision Units (ASU) reported providing agents with updates related to this topic as they become available, none of the ASUs supplied agents with the PPSC Directive on Information Management as required by the Agent Agreement – Terms and Conditions and not all provided agents with centralized PPSC policies and processes at onboarding, though PPSC employees and agents both manage prosecution files.

Communication

We found regular communication to promote awareness about relevant policy instruments from Security Services and Regional Offices to PPSC employees and all ASUs reported providing these communications to agents.

Further, PPSC policies and processes are available on iNet[A] where PPSC employees can access them, though not agents. We did note that policy instruments were not intuitively found on iNet which could impact awareness of requirements by employees.

While employees and agents indicated there is sufficient communication, comments specified a need for more proactive, clear, and consistent communication from Headquarters, Regional Offices, and ASUs. Concise and regular communications targeted to the audience could improve stakeholder engagement.

Recommendation 1

The Deputy Director of Public Prosecutions and Senior Director General, Corporate Services should ensure PPSC policy instruments regarding the management of sensitive information have comprehensive language for all PPSC legal operations staff and agents, contain roles and responsibilities for all legal operations staff and agents, and are accessible to all PPSC employees and agents. (Medium)

Recommendation 2

The Deputy Director of Public Prosecutions and Senior Director General, Corporate Services should ensure communication regarding the management of sensitive information to regions and agents is effective, consistent, and sent regularly. This approach should consider:

- *distributing communications by an appropriate source (i.e.: Chief Federal Prosecutor for regional distribution)*
- *adding regional/agent context to centralized communication before regional/agent distribution*
- *presenting key points concisely and upfront. (Medium)*

[A] The PPSC's intranet site which is used to securely share the organization's information and computing resources among employees.

What we expected to find

We expected to find training programs effectively deployed to enhance employees' and agents' knowledge and understanding of their responsibilities in protecting sensitive information.

Conclusion

While various forms of training and awareness activities are taking place, more regular and targeted training would further support and promote awareness of the management of sensitive information. Improved awareness should help to reduce the risk of non-compliance.

Training

The PPSC has identified two mandatory training courses for employees related to the management of sensitive information: Security Awareness (COR310) offered by the Canada School of Public Service for all employees and Prosecutions Fundamentals Course (Level 1) offered by the PPSC's Federal Prosecutor Development Program for prosecutors. The latter course includes the vetting of disclosure, though it was indicated this is also learned through on-the-job training.

However, we found only approximately 60% of PPSC employees had records indicating they completed the mandatory Security Awareness training. Also, some employees told us that employee access to Prosecution Fundamentals was not timely due to limited capacity and travel budget constraints. Completion of mandatory training that is not enforced is less effective.

There is no mandatory training for agents regarding the management of sensitive information. We also found a lack of clarity and consistency in what training materials ASUs provide to agents across the regions.

While survey results for agents and employees generally indicated they have sufficient training, employee comments specified a need for more regular training and refreshers, as well as more targeted training, including for the vetting of disclosure. Further, some indicated instructor-led training would provide greater clarity than reading procedures and guidelines.

Recommendation 3

The Senior Director General, Corporate Services should ensure mandatory training for PPSC employees is defined, sufficiently available, occurs regularly, and is tracked for completion. The need to identify mandatory training requirements for agents should also be assessed. Consideration should be given to developing and/or providing training tailored to the realities of the management of sensitive information related to prosecution files at the PPSC. (Medium)

OPERATIONAL EFFECTIVENESS AND EFFICIENCY

What we expected to find

We expected to find appropriate facilities and tools in place for employees and agents to efficiently manage sensitive information.

We expected to find security clearances aligned with the level of work performed by agents and PPSC employees.

Conclusion

Providing further training to ensure understanding of processes and tools should strengthen operational effectiveness.

The PPSC has facilities and tools for their employees to manage sensitive information, though improvements could provide easier access and limit physical processes to increase efficiency. Ensuring complete records of agents' tools and facilities would substantiate that they meet these requirements.

The PPSC has tools and processes to manage security clearances though ensuring clarity and understanding regarding the level of security clearance required to perform the work is needed. Monitoring of PPSC employees' security clearances could mitigate the PPSC's non-compliance with the TB Standard on Security Screening.

Findings

Facilities and Tools

Generally, the facilities and tools available to PPSC employees were found to meet requirements for the management of sensitive information, except some regions lack Top Secret rooms. While a process exists to ensure agent firms have the necessary facilities and tools, we could not confirm if agents meet the requirements due to a lack of completed records. We were unable to determine whether this was due to improper document management or to the expected process not being followed to collect and verify this information.

We found the PPSC does not have a secure network that allows for the storage and transmission of Protected C and above information. Instead, processes have a physical approach, such as traveling to a partner agency to collect/view information and temporarily accessing off-network laptops to store and view information. While the tools available may meet requirements, the resulting processes can be time consuming and contribute to a lack of efficiency. This can lead to actions to compensate for the inefficiencies that increase both non-compliance and risk for the PPSC.

The following demonstrate the lack of understanding by employees of what facilities and tools to use and/or how to use them:

- Identifying Case Prep Rooms as Top Secret rooms.
- Leaving electronic tools unattended in public areas with password attached.
- Using inappropriate tools/processes to secure physical information in transit.
- Accepting that sensitive information be sent over our networks due to geographical distances and time required for travel to hand deliver.

Approximately 20% of PPSC employee survey respondents found current processes to be inefficient. Comments indicate a lack of a secure network, limited access to protected rooms, time needed to manually transmit documents, access to standalone laptops, unclear processes, and lack of training as contributing to the inefficiencies.

Security Clearances

We reviewed a sample of security clearances for both PPSC employees and agents. The process to renew agents' security clearance is working as intended as all of those reviewed had an appropriate and valid security clearance for the work they perform.

However, for PPSC employees, we found a lack of clarity in some regions regarding the level of security clearance required to perform their work and not all employees in the sample reviewed had a clearance appropriate for the work they perform. Further, as some employees did not update their security clearance in accordance with the TB Standard on Security Screening, the PPSC is non-compliant with the Standard. The process to update clearance is dependent on the employee taking action and no monitoring process is in place to ensure compliance.

OPERATIONAL EFFECTIVENESS AND EFFICIENCY

What we expected to find

We expected to find monitoring and reporting mechanisms in place to ensure sensitive information is managed properly.

Conclusion

The PPSC has implemented some management of sensitive information reporting mechanisms, but improvements should be made for a more proactive approach to monitoring and reporting, particularly security clearances. Strengthening controls relating to vetting court documents could reduce breaches of this nature.

Monitoring and Reporting

We found the Security, Digital and Knowledge Management Committee has sufficient oversight over the management of sensitive information and is carrying out their mandate.

Monitoring is done by way of site visits by ASUs for agents and on-site floor sweeps of PPSC offices by Security Services for regions. However, we found these have ceased due to the COVID-19 pandemic and travel budget cuts, thereby limiting visibility over the management of sensitive information.

Being notified of privacy breaches and security incidents is integral to the management of sensitive information and is reliant on reporting by PPSC employees and agents. We found established processes for reporting privacy breaches to the Access to Information and Privacy (ATIP) team, and for reporting security incidents the Security Services team. The process is reactive and dependent on the awareness and willingness of the employee or agent to report. Regions with a higher number of incidents and/or breaches may indicate a lack in their processes as the cause, though this could also be due to other regions under-reporting their incidents and/or breaches. However, in 2022 the ATIP team noted an increasing trend in reported privacy breaches related to vetting of court documents. A recommendation to the Director of Public Prosecutions was made at the time to implement a preventive measure to strengthen controls over vetting, however, these continue to occur and be reported.

There is no monitoring in place for agents' vetting of sensitive information, however, four of the regional ASUs indicated providing guidance, feedback and/or reviewing agents' vetted information.

Finally, though the security module of the software used to record security clearances does not have the capability to extract data, the human resources module does. This could improve the ability to monitor appropriate and valid security clearances efficiently and improve the PPSC's compliance.

Recommendation 4

The Deputy Director of Public Prosecutions and Senior Director General, Corporate Services should consider implementing digital solutions for the secure transfer of information that support improved efficiency and reduce the risk to the PPSC resulting from non-compliant actions. (Medium)

Recommendation 5

The Deputy Director of Public Prosecutions and Senior Director General, Corporate Services should ensure there is awareness of the TB requirements for the security clearance level appropriate for the work being performed. This should include ensuring security clearances align with the work performed and that it is maintained in accordance with the TB Standard on Security Screening (update cycle indicated in Appendix B, section 5). (High)

MANAGEMENT ACTION PLANS

No.	Recommendation	Risk	Management Action Plan	Office of Primary Interest	Target Date
1	The Deputy Director of Public Prosecutions and Senior Director General, Corporate Services should ensure PPSC policy instruments regarding the management of sensitive information have comprehensive language for all PPSC legal operations staff and agents, contain roles and responsibilities for all legal operations staff and agents, and are accessible to all PPSC employees and agents.	Medium	Management agrees with this recommendation. Actions: • The policy instruments will be reviewed, by both the Information Management team and the Security team, and updated, as required, including defining roles and responsibilities for all legal operations staff and agents. • Documents will be available on iNet for employees and for agents, the Knowledge Management or PPSC public website will be used.	Executive Director, Security and Facilities	March 31, 2026
2	The Deputy Director of Public Prosecutions and Senior Director General, Corporate Services should ensure communication regarding the management of sensitive information to regions and agents is effective, consistent, and sent regularly. This approach should consider: • distributing communications by an appropriate source (i.e.: Chief Federal Prosecutor for regional distribution) • adding regional/agent context to centralized communication before regional/agent distribution • presenting key points concisely and upfront.	Medium	Management agrees with this recommendation. Actions: • A communications plan will be implemented to ensure regular communications regarding the management of sensitive information for both employees and agents. The plan will indicate which method will be used for information dissemination and by whom. • If regional context is required, it will be obtained during the development of the material. • A template for communications material will be created ensuring that key points are conveyed upfront.	Executive Director, Security and Facilities	March 31, 2026
3	The Senior Director General, Corporate Services should ensure mandatory training for PPSC employees is defined, sufficiently available, occurs regularly, and is tracked for completion. The need to identify mandatory training requirements for agents should also be	Medium	Management partially agrees with this recommendation. Management considers the available training sufficient for the needs of PPSC's employees and will not develop/provide additional training tailored to the PPSC.	Executive Director, Security and Facilities Directorate and	November 30, 2025

No.	Recommendation	Risk	Management Action Plan	Office of Primary Interest	Target Date
	assessed. Consideration should be given to developing and/or providing training tailored to the realities of the management of sensitive information related to prosecution files at the PPSC.		Managers are responsible to ensure that employees have completed mandatory training. Human Resources tracks training taken by employees and will consider a process to provide completion data to managers. Actions: • Information on training, and guides available on iNet, will be included as part of the communications plan. • Agents will be informed that they are required to take course COR310. Section 7.2 of the Agent agreement will be amended. Regional Agent Supervision Units will monitor for completion.	Executive Director, Agent Affairs Program	
4	The Deputy Director of Public Prosecutions and Senior Director General, Corporate Services should consider implementing digital solutions for the secure transfer of information that support improved efficiency and reduce the risk to the PPSC resulting from non-compliant actions.	Medium	Management agrees with this recommendation. Actions: • The Chief Security Officer will engage with our partners, Shared Services Canada and the Communication Security Establishment, to identify digital solutions for a segregated secure network. This would allow the PPSC to send, receive, view and manipulate Protected C, Secret, Top Secret, and SIGINT information within the Government of Canada, and with investigative agencies (e.g.: RCMP, Department of Fisheries and Oceans, Environment and Climate Change Canada, Canada Border Services Agency, Justice Canada) including secure email, data transfer, and digital storage of highly classified information. • As this work will require funding, options will be determined, and a concept case will be submitted for decision by the Senior Leadership Committee. • Determine solutions, through the eDisclosure project, that will enable us to intake evidence from the investigative agencies, share with defense counsel, and store it, up to the Protected B level.	Executive Director, Security and Facilities	March 31, 2026
5	The Deputy Director of Public Prosecutions and Senior Director General, Corporate Services should ensure there is awareness of the TB requirements for the security clearance level appropriate for the work being performed. This should include ensuring security clearances align with the work performed and that it is maintained in accordance with the TB	High	Management agrees with this recommendation. A new Security Screening Directive came into effect January 6, 2025, which requires security level updates for many PPSC employees. TBS has allowed two years for implementation. Actions: • Information will be communicated to managers regarding security levels – both the changes to come from the Directive and a reminder	Executive Director, Security and Facilities	April 6, 2027

No.	Recommendation	Risk	Management Action Plan	Office of Primary Interest	Target Date
	Standard on Security Screening (update cycle indicated in Appendix B, section 5).		to only assign work according to the employee's level of security clearance. • Direction will be provided for managers to review the security levels of all positions. • A new tool will be implemented to determine the security level required for any new position. • PeopleSoft reminder emails will be updated to include a warning regarding the severity of not renewing their security clearance. • Managers of employees with overdue clearances will be included on reminder emails generated by PeopleSoft. • For those that are approaching their renewal date and haven't acted, the security team will escalate their file to their manager (timeframe for the notification to be determined).		

APPENDIX A – AUDIT INFORMATION

Statement of Assurance

The audit was conducted in conformance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and with the Treasury Board Policy and Directive on Internal Audit as supported by the results of the external quality assurance assessment.

Scope

The scope of the horizontal audit included Protected C, Secret, and Top Secret information related to prosecution files, both in-house and agents, in all PPSC offices except for the Northern regions (Nunavut, Northwest Territories, and Yukon).

Methodology

The audit methodology included, but was not limited to:

- Interviews and surveys with headquarters, regional staff and management, and Agent Supervision Units.
- Surveys with agents.
- Review and analysis of data, documented policies, practices, procedures, and directives.

Audit Criteria

1	The PPSC has implemented a defined and documented framework to support the proper management of sensitive information (Protected C and above).
2	The Department has the facilities, tools, and oversight in place for the effective and efficient management of sensitive information.
3	Training and awareness programs are effectively deployed to enhance employees' and agents' knowledge and understanding of their responsibilities in protecting sensitive information.

APPENDIX B – LIST OF ACRONYMS/ABBREVIATIONS

ATIP	Access to Information and Privacy
ASU	Agent Supervision Units
PPSC	Public Prosecution Service of Canada
TB	Treasury Board of Canada