RCMP

ROYAL CANADIAN MOUNTED POLICE

2024-2025
ANNUAL REPORT TO PARLIAMENT

ADMINISTRATION OF THE *PRIVACY ACT*

2024-2025

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Catalogue No: PS61-42E-PDF
ISSN: 2564-2782

Royal Canadian Mounted Police | Gendarmerie royale du Canada

2024-2025 ANNUAL REPORT TO PARLIAMENT

ADMINISTRATION OF THE *PRIVACY ACT*

Canada

Contents

INTRODUCTION

The Royal Canadian Mounted Police (RCMP) is pleased to present to Parliament, in accordance with section 72 of the *Privacy Act* (PA), its annual report on the management of this Act. The report describes the activities that support compliance with the Act for the fiscal year commencing April 1, 2024, and ending March 31, 2025.

The purpose of the Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and provides individuals with a right of access to that information.

The 2024-2025 fiscal year marks the RCMP's fourth year of its five-year modernization plan for its Access to Information and Privacy (ATIP) program. The RCMP is pleased to report improvements to its performance and program overall and is proud of its ongoing collaboration with our employees across Canada, as well as our network of partnerships with other Government of Canada departments. These improvements are also a testament to the hard work and dedication of the ATIP Branch's employees.

Ensuring that Canadians have timely access to information—enabling them to understand the decision-making process and the challenges faced—is essential to building and maintaining trust in the organization. The RCMP takes these responsibilities seriously and is committed to meeting the expectations of Canadians while protecting the integrity of the investigations undertaken on their behalf. Canadians are encouraged to monitor our work through the public website at https://www.rcmp-grc.gc.ca/en/access-information-and-privacy-programs-modernization-strategy.

ORGANIZATIONAL STRUCTURE

Royal Canadian Mounted Police

As a federal, provincial, territorial and municipal policing body, the RCMP provides federal policing services to all Canadians and policing services under contract to the three territories, eight provinces, and more than 150 communities delivered through more than 700 detachments across Canada, 600 Indigenous communities and three international airports.

The RCMP's mandate is multifaceted and includes preventing and investigating crime; maintaining peace and order; enforcing laws; contributing to national security; ensuring the safety of state officials, visiting dignitaries and foreign missions; and providing vital operational support services to other police and law enforcement agencies within Canada and abroad.

A Commissioner leads the RCMP and is supported by a Senior Executive Committee (SEC) made up of regular members, civilian members and public servants. The role of SEC is to develop, promote and communicate strategic priorities, strategic objectives, management strategies and performance management for the purpose of direction and accountability.

The organization is subdivided into 15 divisions (10 provinces, three territories, Depot Division and National Headquarters in Ottawa), each of which is under the direction of a Commanding Officer or Director General.

National Headquarters includes 10 business lines and is structured as follows: Federal Policing, Contract and Indigenous Policing, Specialized Policing Services, Corporate Management and Comptrollership,

Human Resources, Internal Audit and Evaluation, Professional Responsibility Sector, Strategic Policy and External Relations, Reform Accountability and Culture, and Legal Services.

Access to Information and Privacy (ATIP) Branch

The RCMP established the ATIP Branch in 1983, as the central point of contact for all matters arising from both the *Access to Information Act* (ATIA) and the *Privacy Act* (PA). The ATIP Branch reports through the Chief Digital Officer to the Deputy Commissioner of Specialized Policing Services. The IM/IT Branch was renamed the Digital Program in December 2024. The new Digital Program is responsible for leading the technological transformation of the RCMP, along with Analytics, Data and Information Management and the ATIP Branch. While this is not a common structure within government, it unites Information Management (IM) and Information Technology (IT) with ATIP further enabling the modernization of the ATIP program. These benefits include a more high-profile role for the Branch in areas such as digital records management, open government, and the declassification of historical records.

The ATIP Branch's Director General acts on behalf of the head of the institution as the Departmental Access to Information and Privacy Coordinator. The ATIP Coordinator ensures compliance with both the spirit and the intent of the PA, as well as all associated regulations, policies and guidelines. The Director General position is also tasked with leading the program's broad modernization efforts. The ATIP Branch is made up of 122 employees and 11 consultants who work on requests under both the ATIA and the PA.

Privacy Stream

Led by a Director, the Privacy Stream is made up of two units–one responsible for processing formal personal information requests and the other supports compliance of the RCMP's program delivery with the provisions of the *Privacy Act* and the policies and directives of the Treasury Board of Canada Secretariat (TBS).

Privacy Disclosure Unit: This unit processes all formal requests received under the PA. This stream is made up of four disclosure teams, each with an area of expertise. The first two teams focus on the on-time requests, helping the RCMP meet its obligations under the *Privacy Act.* The third team specifically looks at the most dated backlog files to reduce the risk associated with these requests. The fourth team is responsible for reviewing and responding to complaints received through the Office of the Privacy Commissioner (OPC).

Privacy Management Division (PMD): The Privacy Management Division is divided into three interrelated but distinct teams: Compliance and Advisory Services, Privacy Policy and Transparency, and Incident Management and Permissible Disclosures. These dedicated professionals provide policy advice and expertise to the RCMP on privacy-related issues, including: assessing risks and recommending mitigating measures during program development and modernization; supporting the drafting, review and approval of Privacy Impact Assessments (PIAs) and Privacy Impact Assessment Questionnaires (PIAQs); reviewing RCMP agreements and contracts (e.g. Memorandums of Understanding, Information Sharing Agreements, Requests for Proposal); managing privacy breach reporting, complaints under sections 4 through 8 of the PA, and the informal review of requests under subsection 8(2) of the PA. In addition, the team provides awareness sessions and reviews and creates internal policies that reflect TBS policy, directives and guidance, as well as expectations from the OPC. The team works to ensure the RCMP is meeting its obligations as described in section 4.2 of TBS's Policy on Privacy Protection and the PA.

Access to Information Stream

Led by a Director, the Access Stream is responsible for responding to all formal and informal requests made under the ATIA. This stream is made up of four disclosure teams, each with an area of expertise. The first team focuses on the on-time requests, helping the RCMP meet its obligations under the Act. The second team specifically looks at the most dated backlog files in order to reduce the risk associated with these requests. A third team, made up of highly experienced analysts, is responsible for addressing the most sensitive investigations which may require extensive consultations or unique knowledge in order to process. The fourth team is responsible for reviewing and responding to complaints received through the Office of the Information Commissioner (OIC).

The Access Stream also leads the overall coordination of the proactive publication requirements of Part 2 of the ATIA for the RCMP and works collaboratively with stakeholders to monitor and ensure compliance. This Stream also works closely with partners in Communications, Parliamentary Affairs, the Commissioner's Office and the Minister's Office to ensure horizontal visibility on ongoing trends, including issues with implications to the department, public sentiment, and strategic planning with the view of sharing a common understanding of organizational priorities, and informing existing, or anticipated ATIP requests.

Operational Support Stream

Led by a Director, the Operational Support stream oversees the preliminary phases of a request, provides internal reporting services and digitization of its processes. It consists of two teams: Lead Operations and Innovative Solutions. The Lead Operations team concentrates on the opening, triaging, tasking and importing of all incoming requests. Meanwhile, the Innovative Solutions team is tasked with creating robotic processes (bots) that automate repetitive tasks, thereby enhancing efficiency and optimizing workflows. Additionally, they play a vital role in the management and maintenance of the ATIP case management software and in supporting ATIP operations within the RCMP. They ensure the accuracy of data, manage user access, and provide statistical reports to bolster ATIP operations. The team also includes the Centre of Excellence for all rich media requests, including those from the Body Worn Camera (BWC) initiative and BWC footage contained in operational files.

When tasking requests, the Lead Operations team works closely with divisional Liaison Officers (LOs) and record holders, known as the Office of Primary Interest (OPIs). Some responsibilities of the LOs and OPIs include:

Liaison Officers: LOs are responsible for forwarding all requests to the appropriate personnel (i.e. OPIs) within their business lines or divisions. Other responsibilities include tracking submissions to ensure responsive records are sent by OPIs to the ATIP Branch; ensuring responses are on time; and documenting and communicating internal RCMP ATIP processes to all who facilitate the processing of requests. In 2022, the RCMP Contract Management Committee was consulted on an initial pilot to expand its ATIP footprint in the divisions. At that time, five divisions were transferred funds from National Headquarters to support limited capacity to serve as a proof of concept and identify challenges. The initial results of this pilot have been extremely successful, with divisions reporting increased visibility and carriage of ATIP requests moving through the divisions. Due to conflicting priorities and increasing demands, as well as a of lack of funding, the pilot couldn't continue past the first year.

Office of Primary Interest: As the record holders, some of the OPIs' responsibilities include providing electronic copies of the responsive records; reviewing records for duplication; ensuring that the

information falls within the scope of the request; notifying the ATIP Branch if records are voluminous; and advising the Branch or LO if an extension is required.

DELEGATION ORDER

The Minister of Public Safety is responsible for administering requests made to the RCMP under both the *Access to Information Act* and the *Privacy Act*. In accordance with section 73 of the *Privacy Act*, the Minister delegates authority to departmental senior management, including the ATIP Coordinator, to carry out the Minister's powers, duties and functions under the Act in relation to formal requests. A copy of the signed Delegation Order is included in Appendix A. Of note, this Delegation Order is currently being updated to reflect the current operating structure of both the ATIP Branch and the RCMP as a whole.

PERFORMANCE FOR 2024-2025

This section provides an overview of the RCMP's performance with respect to records requested under the PA for the 2024-2025 reporting year.

During the 2024-2025, the ATIP Branch remained operational reporting period and continued to work closely with its partners and stakeholders in finding solutions and reviewing processes to ensure that it responded to Canadians' requests in a satisfactory and timely manner. However, it continued to face challenges that resulted in response delays to requests submitted. Despite its legislative responsibilities, certain realities prevented the RCMP from responding on time, including

- Operational requirements that called for RCMP members and employees to be redeployed on an urgent basis. This includes the National Wildfire response, police assistance at protest activities and security for major events and visits, to name a few.
- The RCMP still relies heavily on paper-based processes.
- The extensive search for records often required (more than 750 locations throughout Canada).
- The switch from the Immigration, Refugee and Citizenship Canada (IRCC) ATIP portal to the TBS portal in March 2023 continues to obligate the RCMP to seek clarification from the vast majority of requesters for information that was previously mandatory on the IRCC portal.
- Significant recruitment, training, awareness and retention efforts in the ATIP Branch continued in light of the lack of experienced ATIP analysts in the wider ATIP community. The Branch is working diligently to develop new analysts through a Professional Development Program, and these efforts will show results in the years to come.

The RCMP recognizes the importance of complying with legislated timelines and why it continues to overhaul its program and address these issues by:

- Devoting resources to improve the timeliness of responses.
- Modernizing/streamlining policies and procedures within the program and across the organization to enhance operational efficiency.
- Expanding training and awareness campaigns for all RCMP personnel to ensure they understand their obligation to respond within legislated timeframes.
- Investing in new technologies and automation to increase efficiencies and decrease the total workload.

Compliance

In alignment with the Treasury Board Secretariat's performance target of closing 90% of personal information requests within legislated timelines, the RCMP demonstrated notable progress in improving compliance. In the 2024–2025 fiscal year, the Branch achieved a compliance rate of 71% for requests closed within the legislated time frames under the Act—an increase from 61% in the previous fiscal year. This upward trend reflects ongoing efforts to enhance the timeliness and efficiency of our access to information and privacy processes. The increase is due, in part, to modifications in processes within the Branch resulting in efficiencies, increased efforts in human resources (staffing, training, retention) and the utilization of contractors to complete complex late files to address legislative compliance.

As demonstrated in Table 1 below, significant efforts were undertaken to conclude many backlog requests resulting in more files closed and more pages processed than the previous reporting period. Of note, 1,083 requests were concluded as abandoned when requesters failed to provide sufficient information at the outset to process their request. These requests would have positively influenced the compliance rate.

Table 1: Compliance and Pages Processed

	Compliance	Pages Processed	Requests Closed
2024-2025	71.6%	1,050,872	10,424
2023-2024	61.8%	424,073	6,882
2022-2023	55.0%	284,890	3,212
2021-2022	46.0%	547,847	4,081

Requests Received and Closed

The RCMP received a total of 9,232 new requests under the *Privacy Act* in 2024-2025. In addition, there were 5,987 requests outstanding from the previous reporting periods for a total of 15,219 requests. Of these, 10,424 requests were completed and 4,795 carried over to the 2025-2026 fiscal year.

Privacy requests cover the personal information of requesters in a variety of records and mediums (e.g. audio/video), including information on police operational files, such as motor vehicle collisions and employment files.

There has again been an increase in the number of requests received compared to the previous reporting period. The number of requests received increased by 18% compared to the previous fiscal year (7,808 requests received) and increased by 94% compared to the 2022-2023 fiscal year (4,741 requests received). The increase in the number of privacy requests received is a direct result of the Branch's efforts to educate requesters, including adding guidance to the TBS portal advising requesters to use the PA to request their own personal information. This has benefited requesters as privacy requests can be made free of charge, provides them with an expanded right of access, and grants requesters the right to correction, none of which exists under the ATIA. The increase here correlates to a decrease in requests made under the ATIA.

Completion Time and Extensions

The ATIP Branch completed 4,289 (41%) requests in 30 days or less. During the reporting period, 2,977 (28.5%) requests were completed within 31-60 days, 761 (7.3%) were completed in 61-120 days, and 2,387 (22.8%) were completed in more than 121 days.

Section 15 of the *Privacy Act* allows institutions to extend the statutory time limits to respond to a request beyond 30 days.

For the requests closed during the 2024-2025 reporting period, the RCMP sought a total of 7,038 extensions under section 15(a)(i), which pertains to unreasonable interference with operations.

No extensions under section 15(a)(ii) were taken for consultations.

Disposition of Completed Requests

Of the 10,424 requests completed in the 2024-2025 fiscal year, the dispositions of completed requests were as follows:

Table 2: Disposition of Completed Requests

Disposition	Requests	Percentage
All disclosed	437	4.2%
Disclosed in part	5031	48%
All exempted	719	6.8%
All excluded	0	0%
No records exist	656	6.2%
Request abandoned	3541	34%
Neither confirmed nor denied	40	0.3%
Total	**10,424**	**100%**

Consultations for Other Institutions

During the current reporting period, the RCMP completed 116 consultations, totalling 4,845 pages reviewed. Of the 116 completed consultations, 46 were received from other Government of Canada institutions and 70 were received from other organizations. This is a marked decrease from the previous reporting period where RCMP reviewed 105 requests and 12,156 pages. The RCMP continues to put an

equal focus on consultations as a service to the ATIP community and in line with the expectations of the Privacy Commissioner.

Table 3: Completion Times for OGD Consultations

Completion times	**Consultations**
1 to 15 Days	23
16 to 30 Days	10
31 to 60 Days	8
61 to 120 Days	0
121 to 180 Days	2
181 to 365 Days	3
More than 365 Days	0
Total	**46**

Active Outstanding Requests from Previous Reporting Periods

At the conclusion of the 2024-2025 fiscal year, a total of 4,795 requests were outstanding. Of those outstanding, 17% were carried over within legislated timelines and 83% were carried over beyond legislated timelines. The significant work done to eliminate the backlog of requests can be seen at Table 6 and in the numbers below. The legacy backlog has been reduced by approximately 30%, from 6.4 million pages to 4.6 million pages over the reporting period. While there is still a backlog of requests to process, they are much more recent, and this demonstrates the efforts made to improve the service the RCMP is providing to the public. The fiscal years where the carried over requests were received in are as follows:

Table 4: Active Requests from Previous Reporting Periods

Fiscal Year PA requests were received	Open requests that are within legislated timelines as of March 31, 2025	Open requests that are beyond legislated timelines as of March 31, 2025	Total
Received in 2024-2025	839	1106	1945
Received in 2023-2024	0	904	904
Received in 2022-2023	0	1138	1138
Received in 2021-2022	0	648	648
Received in 2020-2021	0	154	154
Received in 2019-2020	0	1	1
Received in 2018-2019	0	1	1
Received in 2017-2018	0	0	0
Received in 2016-2017	0	1	1
Received in 2015-2016 or earlier	0	3	3
Total	**839**	**3956**	**4795**

Active Outstanding Complaints from Previous Reporting Period

At the conclusion of the reporting period, a total of 170 complaints were outstanding. The fiscal years where the outstanding complaints were received are as follows:

Table 5: Active Complaints from Previous Reporting Periods

Fiscal Year Open Complaints Were Received	Number of Open Complaints
Received in 2024-2025	89
Received in 2023-2024	61
Received in 2022-2023	12
Received in 2021-2022	1
Received in 2020-2021	1
Received in 2019-2020	0
Received in 2018-2019	4
Received in 2017-2018	1
Received in 2016-2017	0
Received in 2015-2016 or earlier	1
Total	**170**

TRAINING AND AWARENESS

Continuous learning is a priority for the RCMP and the ATIP Branch is no exception. ATIP Branch staff are encouraged to seek out relevant courses and other learning opportunities to enhance their knowledge and to improve their skills.

In the 2024-2025 reporting period, the ATIP Branch instituted an internal and informal training curriculum called "A Slice of Learning." These monthly sessions provide an opportunity for all employees to learn about the inner workings of the Branch, along with a variety of topics intended to assist in their daily work. Topics this year included ATIP statistical reporting, how to prepare to be an affiant, summaries of the Canadian Access and Privacy Association (CAPA) and Canadian Bar Association (CBA) ATIP conferences, responding to complaints, data detox, and occupational health and safety.

The ATIP Branch had the opportunity to meet with the senior management of F Division (Saskatchewan) and Depot Division to speak about ATIP and the legal obligations of all employees to comply with the Acts. In person sessions such as this are invaluable as they provide a chance for both sides to ask questions and address issues unique to the Division. This visit also allowed for the ATIP Branch to meet with the curriculum development team for Depot and opened the conversation for updating the training received

by all in-coming police officers. These updates will be developed over the next reporting period and are a key piece in the ATIP Branch's modernization efforts and in line with TBS guidance.

Ad-hoc training continued throughout the year with a total of nine sessions being delivered to 599 employees across the country. A highlight of these presentations was the E Division (British Columbia) Information Governance Days of Summer Sessions. Led by the E Division Information Governance group, this two-week program was open to all employees in the Division and touched on a wide variety of topics that affect information management and governance. As the biggest Division, and utilizing unique records management systems, the ATIP Branch relies on the expertise within the Division to ensure we can respond to requests in a timely manner. Other sessions included employees from Federal Policing, Corporate Reporting and Governance, Strategic Policy, and the Information Professionals Summit in Ottawa led by the RCMP for employees currently working in information management and governance.

Since joining the Digital Program in May 2023, the ATIP Branch has been incorporated into the student outreach program which liaises with post-secondary institutions to connect students to co-op placements and post-secondary recruitment. Three sessions were held this year in the National Capital Region, reaching students across the city with an interest in law enforcement and data.

The RCMP's *Access to Information and Privacy Fundamentals* online course is available to all RCMP employees through the organizations' online learning platform. In addition to increasing their knowledge of the ATIA and the PA, this course also provides employees with a better understanding of their responsibilities when responding to information requests and best practices when managing personal information. In 2024-2025, 886 RCMP employees successfully completed the course.

In addition to the above, ATIP's Privacy Management Division organized 41 privacy awareness sessions reaching over 645 employees, including special events for both Privacy Awareness Week and Data Privacy Week.

POLICIES, GUIDELINES AND PROCEDURES

Throughout this reporting period, the ATIP Branch continued to modernize and update internal policies and procedures to ensure alignment with current reporting standards. These changes will continue to be developed and instituted in the 2025-2026 reporting period.

ATIP Modernization

In November 2020, the OIC released the results of a systemic investigation of the RCMP's ATIP program entitled *Access at issue: The need for leadership*. The report was highly critical of the RCMP's ATIP program and identified 15 recommendations for improvement. Subsequently, the Minister of Public Safety issued a Directive to the RCMP to action the recommendations of the OIC's review and submit a strategy outlining a way forward to be developed in consultation with TBS. In response, the RCMP developed a strategy entitled *Access Granted: Restoring Trust in the RCMP's Access to Information Program*, supported by an action plan outlining initiatives to modernize the program.

The RCMP began implementation of the strategy in the 2021-2022 reporting period and is committed to seeing it through over the course of a five-year period. Since then, the RCMP ATIP Branch undertook advancements in human resources, technology, policy and procedures. The objective being to increase compliance rates and enhance public transparency. The RCMP posted the strategy and is providing

updates on the RCMP external website. We encourage all Canadians to visit the site and monitor our progress at https://www. rcmp-grc.gc.ca/en/access-information-and-privacy-programs-modernization-strategy.

Over the reporting period, the RCMP continued to make progress in implementing the strategy. While more details can be found on our external website, some key initiatives include:

Pillar One: Our People

- To improve the internal services provided to the organization, the Privacy Management Division has been strengthened to ensure the RCMP is able to provide expert services in privacy policy and the management of personal information to all areas of the organization.
- The Operations Stream has been bolstered to include system administrators who are responsible for the technical support of the ATIP case management software and analytics positions to interpret data and assist with long-term planning and process improvements.
- The ATIP Branch strengthened its commitment to diversity and inclusion by partnering with LiveWorkPlay, a non-profit organization that supports neurodivergent talent, enabling the recruitment of individuals whose unique perspectives and skills enhance the organization's innovation, resilience, and inclusive culture. The ATIP Branch currently employs four individuals from LiveWorkPlay in a variety of roles throughout the Branch. As a result, the RCMP was awarded the LiveWorkPlay Inclusive Employer award for 2024-2025. Talks are underway to expand the program to other areas of the RCMP.
- The Professional Developmental Program has begun to show successes. The first candidates have been assessed and are being promoted via the program criteria. This program is essential for the ATIP Branch to train and retain new analysts by demonstrating a career path and growth opportunities within the program and the RCMP.

Pillar Two: Our Tools

- The RCMP worked closely with TBS on updates to the ATIP Online Request Portal. These updates, outlining required information to submit a request, have resulted in a savings of approximately $80,000 since October 23, 2024. More than 1,000 incomplete requests have been closed immediately following opening, resulting in a reduction in work to task and review records where no consent or proper identification has been provided.
- As the RCMP deploys BWCs across the country to front-line officers, ATIP Branch has expanded its capabilities to review these new records along with other rich media formats. The deployment of video vetting software has allowed the RCMP to release more video than ever before as the tools to process it have been improved. Preliminary analysis indicates that processing BWC video files requires significantly more time than initially anticipated. As data remains limited, the full impact of BWC-related requests is not yet clear. The Branch will continue to monitor developments closely and adjust its strategy and resource planning as more accurate information becomes available.
- Three automation processes (RPA) have been put into production within the ATIP Branch. The first bot addresses duplicate records. Eligible records are now deduplicated prior to being uploaded to our case management software. In the first four months of use, 18,000 pages of duplicates were located and removed. This has reduced analyst workload and workloads for our OPIs on consultations since they are not looking through duplicate records. Two more bots have just come online and their effectiveness is currently being monitored.

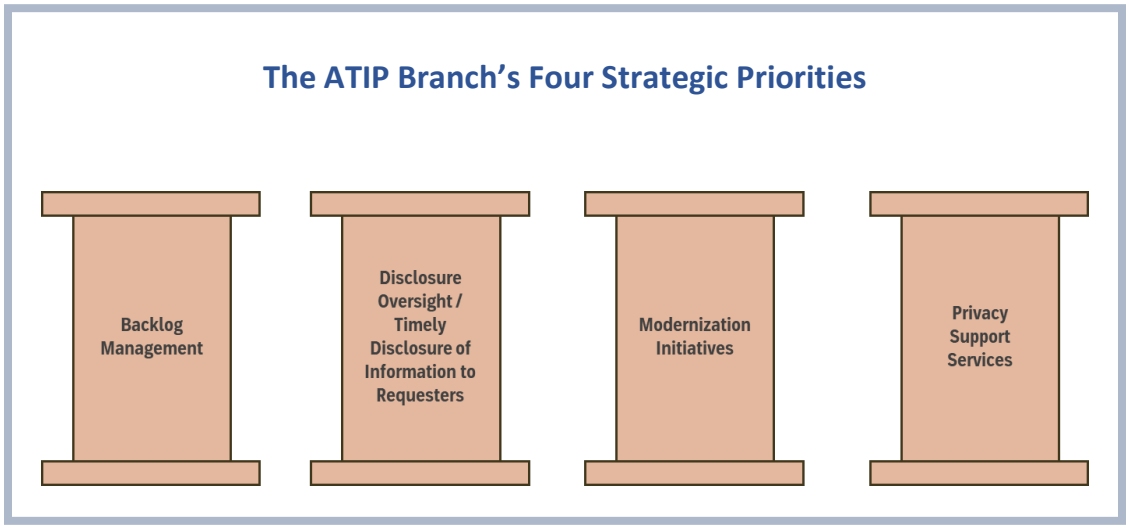
The case management software used by RCMP ATIP Branch is at the end of its life and will no longer be supported after June 30, 2026. All institutions currently using this outdated software are now required to prioritize the modernization of their case management systems, begin onboarding a new platform by June 2025, and complete the full transition by June 2026.TBS has approved two new ATIP software solutions, both of which have been evaluated against criteria established by the ATIP community and meet all mandatory requirements. The current legacy system is obsolete, and its failure could lead to information loss and significantly disrupt or delay the processing of ATIP files. However, funding sources for the replacement and modernization of the existing system have yet to be identified and secured.

Pillar Three: Our Procedures

- The Branch collaborated with the Canadian Firearms Program (CFP) to redirect information requests for firearms information that can be better addressed directly.
- Website and client portal updates were implemented to guide clients on accessing information without submitting a formal ATIP request. These efforts led to a 24% reduction in ATIP taskings to the Specialized Police Service business line during this reporting period.
- The Triage team established a few years ago has made great strides. Over the last two years, employee retention and training on this team has allowed for these analysts to grow, and their work can be seen in the reduction of pages processed. This team regularly speaks with applicants to assist with properly scoping requests, understanding RCMP jargon and ensuring requests are complete prior to any tasking or review being done. This has reduced the workload both within the ATIP Branch but also with the OPIs who have clearer direction on what is being requested.
- Due among other things to the effective triage efforts, the ATIP Branch achieved a 25% reduction in its overall workload. By carefully scoping requests at the outset, staff were able to limit the volume of documents requiring review and processing. As a result, the number of pages received dropped significantly reaching the lowest level in the past decade.
- High-quality data is critical for enabling informed, data-driven decisions, identifying trends, and effectively managing workloads within the ATIP Branch. It also ensures accurate reporting to the Chief Digital Officer and RCMP senior management. To improve data integrity, three targeted training sessions on data entry and reporting standards were delivered early in the reporting period. As a result, data accuracy improved significantly—from 69% in November 2024 to 94% by February 2025.
- The drafting of standard operating procedures (SOPs) remained a priority in this reporting period. To facilitate training and ensure consistency, SOPs have been drafted to address digital evidence, active police investigations, and how to treat records unique to the RCMP.
- To support business continuity and the shortcomings of the current case management software, ATIP collaborated with IT to ensure a full backup of the database is in place should anything happen. As seen in other institutions, the volatility of the database is a key concern and is a leading factor in the evaluation of new software solutions.

As the original 5-year modernization strategy is set to conclude in the next reporting period, the ATIP Branch is looking to the future and how to continue building on the successes seen in the last four years. The four strategic priorities that the Branch will be focusing on are:

1) Clearing the legacy backlog;
2) Disclosure oversight and improved compliance;
3) Advancing modernization initiatives; and
4) Providing robust privacy support services to the RCMP.

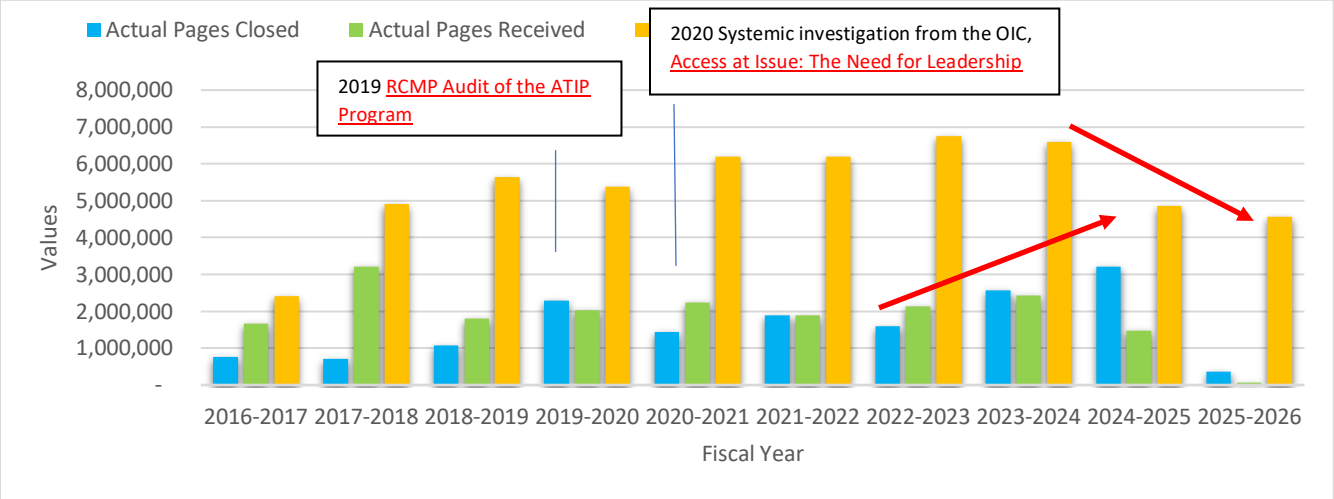


Tackling the Legacy Backlog: A Strategic Success

To address the legacy backlog by 2029, the Branch adopted a targeted strategy: temporarily leveraging experienced and high-performing consultants to accelerate file processing. This approach is already delivering strong results—nearly 30% of the legacy backlog was cleared in 2024–2025, with the volume reduced from 6.4 million to 4.6 million pages over the fiscal year. Notably, the Branch successfully closed almost all backlog files received prior to March 1, 2020.

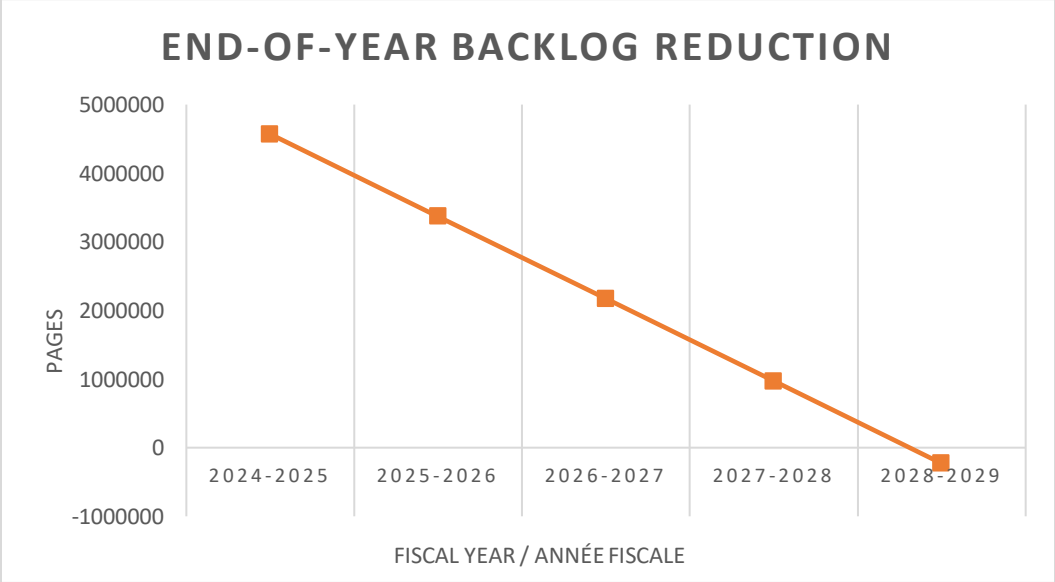
This progress allows indeterminate staff to focus on current and incoming requests, improving overall responsiveness and efficiency.

Table 6: Backlog Accumulation and Reduction



Based on current processing capacity, the ATIP Branch anticipates resolving the legacy backlog—comprised of outstanding files from 2020 to 2025—by the 2028–2029 fiscal year, as outlined in Table 7.

Table 7: Anticipated Backlog Reduction



Closing the Production Gap: A Sustainable Strategy for Timely Information Disclosure

To prevent the creation of a new and compounding backlog, the Branch is implementing a comprehensive and forward-looking strategy to close its annual production gap and ensure timely responses to ATIP requests. The Branch receives approximately two million pages for review each year, while Branch employees currently process 1.2 million pages, resulting in a growing shortfall of 800,000 pages annually.

To eliminate this gap and align capacity with demand, the Branch has already started to implement the following three key measures and will continue to do so in the next fiscal year:

- **Boost Analyst Productivity (+20% workload reduction)**
  As most ATIP analysts are still early in their careers, there is strong potential for growth. With continued training and experience, productivity is expected to increase by 20%, enabling analysts to process more files efficiently as they deepen their understanding of the ATIP legislation.
- **Reduce Page Volume Through Triage and Negotiation (-15% workload reduction)**
  By equipping analysts with negotiation skills and focusing on early triage, the Branch aims to reduce the volume of pages requiring review by approximately 300,000 pages. This will be achieved by working with requesters to narrow the scope of their requests to only the most relevant information.
- **Leverage Automation to Increase Speed and Reduce Workload (-10% workload reduction)**
  The rollout of automation tools is expected to both accelerate processing and reduce manual workload by an estimated 200,000 pages, allowing analysts to focus on more complex tasks.

Together, these measures are projected to bring the number of pages received and processed into balance, effectively eliminating the production gap and preventing the creation of a new backlog. This will ensure that the majority, if not all, of the information requested can be reviewed and disclosed within the same fiscal year, significantly improving service to Canadians.

The graph below highlights the current production gap of 800,000 pages per year, clearly showing the imbalance between incoming and processed pages.

Table 8: Annual ATIP Page Volume: Received vs. Processed

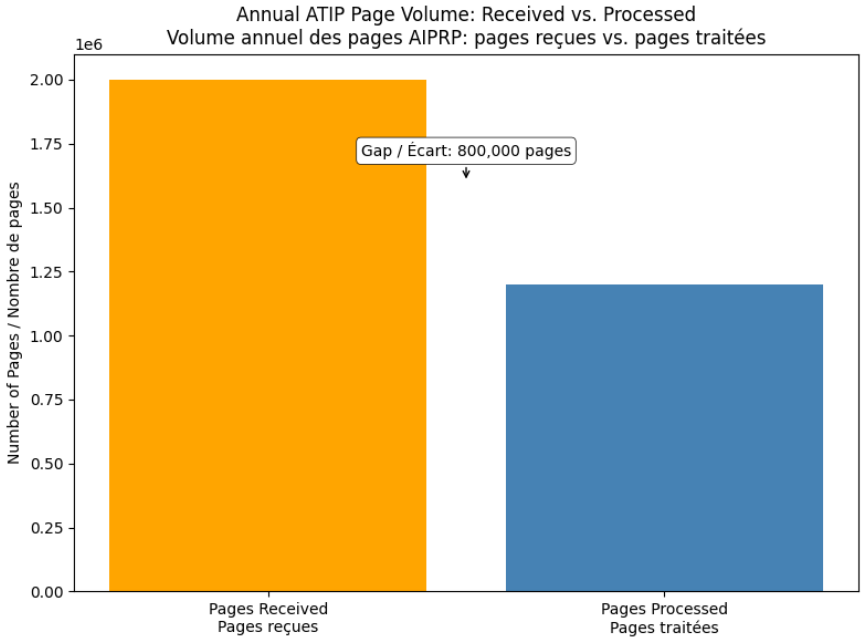
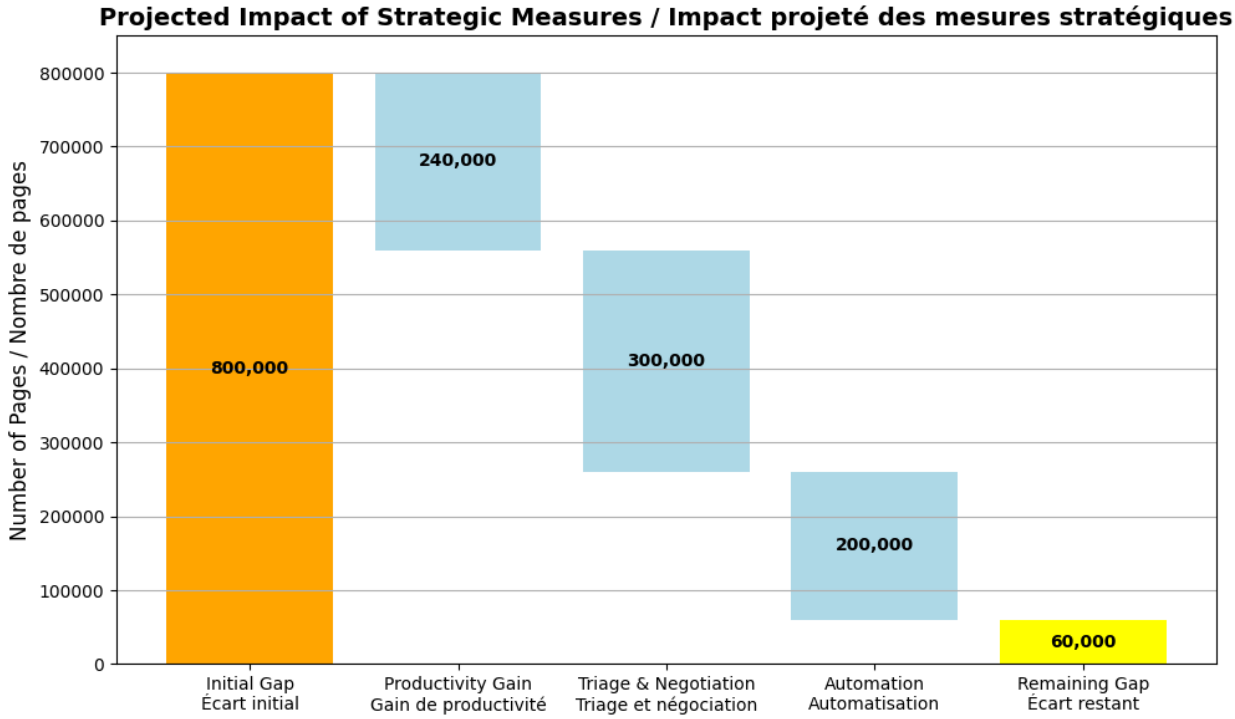


Table 9: Projected Impact of Strategic Measures on Page Processing

This chart breaks down how each of the three key measures—productivity boost, triage/negotiation, and automation—contributes to closing the 800,000 page gap.



Providing Robust Privacy Support Services to the RCMP

Trust is earned—and lost in breaches. As such, strong privacy practices are the foundation for protecting Canadians' data and preserving their trust in public institutions.

In today's digital landscape, data protection is reputation protection. High-profile privacy breaches—such as those experienced by Desjardins, Equifax, and Capital One—have shown how the mishandling of personal information can lead to devastating financial losses, legal consequences, and irreparable damage to public trust.

To prevent similar outcomes, the RCMP's Privacy Management Division plays a vital role in supporting the organization through escalating data privacy challenges. The Branch acts as a privacy shield, helping to ensure that the personal information of Canadians is collected, used, retained, and disclosed in full compliance with the *Privacy Act*.

The class action lawsuits involving Desjardins, Equifax and Capital One resulted in settlements in the 100s of millions of dollars and effected millions of individuals. While some of the more severe examples, these cases underscore the financial and reputational risks of inadequate privacy safeguards. Beyond financial and legal costs, breaches erode public confidence and invite increased scrutiny from the media, Parliament and global regulators enforcing stricter data protection laws.

The ATIP Privacy Management Division provides expert guidance and oversight to ensure that all RCMP programs, technologies, and operations meet privacy obligations, thereby increasing Canadians' trust in the RCMP. Key contributions include:

- Enabling Legal Compliance and Risk Mitigation
    - Conducting Privacy Impact Assessments (PIAs) to ensure lawful handling of personal data.
    - Preventing high-risk initiatives such as what was seen with the use of Clearview AI, negating the risk of being summoned before Parliament, as seen with On-Device Investigative Tools.
- Supporting Modernization and Transparency
    - Contributing to the National Technology Onboarding Process (NTOP) to assess privacy risks in emerging technologies.
    - Updating ATIP policies to reflect recommendations from the Mass Casualty Commission (MCC.
    - Managing Info Source and Personal Information Banks to promote transparency.
- Navigating Emerging Threats
    - Helping the RCMP navigate the complexities of artificial intelligence (AI), cybersecurity, and evolving digital threats.
    - Facilitating the lawful disclosure of personal information while protecting individual rights.

By embedding privacy into every layer of its operations, the RCMP is not only protecting sensitive information, building public trust; reducing institutional risk; and reinforcing its commitment to transparency and accountability.

INITIATIVES AND PROJECTS TO IMPROVE PRIVACY

PMD is responsible for supporting the RCMP in privacy policy compliance and proposing effective mitigation strategies to compliance risks. During this reporting period, PMD completed the following initiatives to help improve both privacy compliance and internal processes:

- Updated internal SOPs on 8(2)s, breaches, complaints, privacy inquiries and training requests.
- Streamlined the privacy breach reporting process, including the development of a new reporting form, a dedicated breach email and guidelines for RCMP employees will be implemented in the first quarter of the 2025-2026 fiscal year.
- Improved file management in APCM to ensure accurate statistics could be extracted.

- Developed a Public Interest Disclosure Guideline and reporting form, along with a decision matrix to guide decision makers when determining if a public interest disclosure meets the invasion of privacy test. This will be officially launched in summer 2025.

Following the October 2024 TBS policy updates to PIA requirements, PMD updated its SOPs on Privacy Impact Assessment Questionnaires (PIAQs, now called Privacy Checklists) and PIAs. PMD also updated its PIA Handbook, an internal guidance document for program-areas conducting PIAs and facilitated an info session on the new PIA requirements.

To address commitments made as part of ATIP's Modernization Action Plan, PMD conducted a gap analysis of its existing policies compared with TBS privacy policy suite, including recent updates to the Directive on Privacy Practices. From there, PMD developed a policy development plan, consulted with internal stakeholder groups and began work drafting new policy pieces. This work will continue into 2025-2026 with the goal of implementing new departmental ATIP policies by end of next fiscal year.

During the 2024-2025 fiscal year, PMD also continued its collaboration with internal groups to embed privacy into existing processes, including the forms development group to include privacy notices into new and modified forms; the MOU policy centre to standardize privacy clauses in agreements involving personal information and to generate publication summaries; and with Procurement to raise awareness of privacy requirements in contracts.

SUMMARY OF KEY ISSUES AND ACTIONS TAKEN ON COMPLAINTS

Complaints and Investigations

During this reporting period, the RCMP continued to work collaboratively with the OPC to address complaints made under sections 4 through 8 of the *Privacy Act* related to the RCMP's collection, correction, retention, use, disclosure and disposal of personal information. Some of the key highlights of those complaints are below:

Use of unencrypted USB storage devices

In July 2022, the Office of the Privacy Commissioner (OPC) self-initiated a complaint against the RCMP concerning a lost unencrypted USB containing five years of operational data affecting over 1,700 individuals and found by an individual in the criminal community who was actively copying and selling the information. In March 2024, the OPC provided their Preliminary Report of Findings which found that the RCMP had contravened the disclosure provision of the *Privacy Act*, recommending that the RCMP implement a series of measures to strengthen its safeguards related to the use of USB storage devices. The RCMP accepted the OPC's recommendations and in May 2024, a DG-level USB Working Group was formed to examine various options to cease the use of USBs while in the interim piloting solutions to significantly reduce their use and reminding employees that all storage devices being used to store protected information must be encrypted.

After a lengthy investigation, the OPC's Final Report in March 2025 concluded that the complaint against the RCMP was well-founded and unresolved despite earlier recommendations. Recognizing RCMP's efforts to mitigate and respond to the breach, the OPC indicated that the RCMP had not committed to implementing its recommendations within a specific timeline. In particular, the OPC required the RCMP to strengthen USB device controls to prevent data breaches by ensuring only secure, approved USB devices are used, backed by an alert system for unauthorized connections.

The RCMP is actively working on a plan to eliminate the use of unencrypted USB storage devices, except for those limited and specific cases where it is impossible to do so. The RCMP is leveraging alternative tools including LiquidFiles; M365 OneDrive and OneNote; and the Digital Evidence Management System (DEMS); and of course, encrypted USB keys.

In collaboration with other Divisions, NHQ Division's Digital Program is moving away from unencrypted USB keys. The RCMP has implemented several initiatives to strengthen information security across its divisions. In E Division, British Columbia, a "USB Bounty" program was launched in March 2025 to phase out unencrypted USB devices by replacing them with compliant ones, with plans to scale the initiative nationally. K Division, Alberta, deployed a system that prompts encryption when an unencrypted USB is connected and is exploring a broader rollout. Additionally, K Division launched the Criminal eFile (CreF) program, enabling digital disclosure of investigative files via an online portal, with LiquidFiles serving as an alternative for larger files. To further enhance secure communication, K Division also introduced the "USB Free" pilot, using LiquidFiles to share Protected B information with external partners, supplemented by a wide distribution of approved encrypted storage devices.

In response to the OPC's recommendation, the RCMP is actively evaluating secure and scalable enterprise solutions to enhance USB device controls and prevent data breaches. A new initiative—allowing only encrypted USB devices—is currently underway and is expected to launch in Fall 2025.

Use of the polygraph for security screening

In January 2025, the OPC self-initiated a compliance investigation against the RCMP, amongst other departments, relating to the privacy implications of its use of the polygraph for security purposes. The RCMP provided its representations to the OPC in late January outlining that the polygraph is only used for security screening in limited and specific circumstances. In fact, there was only one instance of this in the previous five years. The RCMP also committed to amending its existing PIA by the end of 2025, to reflect that current screening polygraph practices cannot be used solely to decide whether a clearance is issued and that the results are only used as a tool in weighing the totality of the information.

The RCMP is currently awaiting a response from the OPC.

Disclosure of medical information for independent medical examinations

In January 2019, the RCMP received notice from the OPC that it was investigating a complaint made by an employee (RCMP member) alleging the RCMP contravened the *Privacy Act* when it disclosed their personal medical information to an external doctor for an independent medical examination without consent. On March 25, 2021, the RCMP received the OPC's report of findings which ultimately found that the complaint was well-founded. Since that time, significant work has been done to address this complaint including a new personal health information policy and updated consent forms which are in the final stages of consultation.

Non-conviction information for vulnerable sector checks

In November 2014, the RCMP received notice from the OPC that it was investigating a complaint alleging the RCMP contravened the *Privacy Act* when it considered non-conviction information as relevant for the purpose of vulnerable sector checks. In addition to this complaint, the OPC was also investigating two others dealing with the same issue. The OPC found that the RCMP's practice of including non-conviction

information broadly, including mental health incidents, in vulnerable sector checks was not proportional or minimally intrusive and that the RCMP had contravened section 7 of the *Privacy Act* by using this information without the individual's informed consent. Following the OPC's recommendations, the RCMP agreed to update its vulnerable sector check consent form and policy to address the OPC's concerns.

Since receiving the OPC's findings and recommendations in March 2021, the RCMP's Operational Policy and Compliance Unit has continued its work on revising its national policy governing vulnerable sector checks (VSCs). While significant progress has been made, the finalization of the updated policy has been delayed due to legislative changes and the need to align with updated federal directives.

In late 2022, Bill C-5 amended the *Controlled Drugs and Substances Act* (CDSA), changing how simple possession convictions are handled and as a result, in 2024, there were updates to the Ministerial Directive on the Release of Criminal Records Information to the RCMP and the Canadian Criminal Real Time Identification Services' (CCRTIS) Dissemination Policy. The RCMP national policy has been revised to reflect these changes.

In addition to incorporating recent legislated changes, the RCMP has completed a draft policy that addresses the findings of the OPC, including updates to the consent form and policy provisions to align with OPC recommendations and concerns related to the disclosure of non-conviction information in vulnerable sector checks.

The revised policy, along with six updated forms and new appendices, is currently under internal review and will undergo divisional consultation shortly. These updates represent a significant step toward finalizing a modernized and compliant approach to police record checks, balancing public safety with individual privacy rights.

Disclosure Complaints

As part of the modernization strategy, a team of disclosure analysts dedicated specifically to review and respond to complaints received through the OPC was created to enable the RCMP to respond more efficiently to complaints. For the 2024-2025 reporting period, the RCMP received and provided the following under the PA:

Section 31 – the RCMP received 303 section 31 notices, which represents 2.9% of all requests closed during the reporting period. The majority of the complaints received relate to delays and deemed refusals, which can be attributed to the substantial increase of requests received over the reporting period; the ongoing RCMP backlog; and the complex and/or voluminous nature of requests. Under this section, the OPC formally notifies the institution of their intent to investigate a complaint received.

Section 33 – the RCMP received 278 section 33 notices. Under this section, the OPC requests representations from both the complainant and the institution pursuant to an ongoing complaint investigation.

Section 35 – the RCMP received 147 section 35 notices. Under this section, the OPC issues a finding report, which may include recommendations, for founded complaints upon the conclusion of the investigation.

Court Action

There were seven court proceedings actioned with respect to privacy requests processed within fiscal year 2024-2025 and none were discontinued/concluded nor dismissed in this reporting period.

MATERIAL PRIVACY BREACHES

As Canada's national police service, the RCMP is trusted to handle and protect the personal information of Canadians with professionalism and integrity, a job it takes very seriously. To safeguard personal information in its care, the RCMP has strict policies and procedures in place to prevent unauthorized access and disclosure across the organization; however, even with these rigorous procedures in place privacy breaches still occur, often because of human error. With every privacy breach, the RCMP takes steps to improve its processes to ensure similar incidents do not occur again.

When a privacy breach is detected, the ATIP Branch follows TBS's guidelines to determine the privacy risks and reports all breaches deemed material to the OPC and TBS.

During fiscal year 2024-2025, PMD received and reviewed 182 possible privacy breach reports of which 23 were deemed material and reported to the OPC and TBS, 121 were deemed non-material, and 38 were determined not to be privacy breaches. Out of the 23 material privacy breaches reported, four incidents resulted from the loss of records either due to human error or issues during mail transmission, while another four stemmed from the inadvertent loss of electronic storage devices. The remaining incidents involved the unauthorized collection, access, use and disclosure of RCMP databases.

Actions taken as a result of these breaches include:

- Conducting regular audits to identify and promptly mitigate any misuse of RCMP databases.
- Updating naming conventions.
- Reviewing, and updating processes and procedures to ensure privacy is a consideration.
- Reminding employees to ensure Privacy Impact Questionnaires are completed for new initiatives.
- Ensuring documents, emails, and storage devices are password protected/encrypted when sharing and/or storing protected information.

Given the RCMP's commitment to safeguarding personal information and minimizing potential harm to the affected individuals stemming from such incidents, PMD continues to educate RCMP employees across the country on their responsibilities to protect personal information and have developed tools to assist in this regard.

PRIVACY IMPACT ASSESSMENTS

During the reporting period, the RCMP completed 10 privacy impact assessments (PIAs), and one fulsome privacy assessment for a national security activity. The titles and summaries are included below.

Collection and Use of Open-Source Information from the Internet

Open-source information (OSI) refers to any information gathered or retrieved from the internet, the deep or dark web, and, in certain instances, commercially acquired information. In accordance with its mandate, the RCMP collects open-source information pertinent to predicated investigations to identify issues and relevant facts, and to develop and advise RCMP partners on security and safety matters. The PIA looked at open-source information collection in an operational context, excluding administrative contexts and security screening purposes. In order to ensure that the RCMP's collection and use of OSI complies with the *Privacy Act*, the Federal Policing Open-Source Program developed a set of policy instruments to enable a consistent operating framework for all open-source information practitioners. The program also oversees the integration of third-party tools that facilitate the conduct of this activity, in collaboration with the National Technology Onboarding Program. Based on this assessment, privacy impacts associated with the collection, use, disclosure and retention of open-source information from the internet by the RCMP are expected to be moderate.

For the full summary: Collection and use of open source information from the Internet | Royal Canadian Mounted Police

Police Transitions

The RCMP provides contract policing to 8 provinces and 3 territories, as well as 150 municipalities and First Nations communities under 20-year Police Service Agreements. In recent years, several municipal jurisdictions have indicated their intention to end their police service agreements with the Government of Canada and establish new municipal police services, such as Surrey (British Columbia) and Grande Prairie (Alberta). In other situations, there has been a change in the boundaries of policing jurisdiction. The PIA sought to ensure that the RCMP implements the necessary mitigating measures regarding the transfer of personal information during a transition of policing duties. In such situation, the RCMP will only hand over files of ongoing and relevant investigation files—which include personal information—to the other policing service. Specific details and requirements to ensure the safe handling of personal information are to be specified in a Memorandum of Understanding between the two police services.

For the full PIA summary: Police Transition | Royal Canadian Mounted Police

Blue Force Tracking (BFT)

BFT provides incident commanders and members on duty with a map of the GPS location of each member to enhance officer safety. It was implemented to meet a key officer-safety recommendation from the MacNeil Report after the 2014 incident in Moncton, New Brunswick, which resulted in the death of three RCMP officers. BFT employs a geo-spatial infrastructure for situational awareness in a General Duty policing environment using applications called Android Team Awareness Kit (ATAK) and Windows Team Awareness Kit (WinTAK). The PIA assessed these applications finding that BFT would be considered a medium risk program. Through the implementation of administrative and technical safeguards, privacy risks are expected to be reduced to an acceptable level.

For the full summary: Blue Force Tracking (BFT) | Royal Canadian Mounted Police

MyCFP Enhancements, Release 1, Program Increment 1

The RCMP Canadian Firearms Program (CFP) is modernizing its service delivery to avert significant error rates, be synchronous with changes to legislation and meet client expectation of reliable and efficient service. The "MyCFP" portal enhancements provide new functionalities to the cloud-based solution Canadian Firearms Public Digital Services Solution: the submission of online applications for a Minor's Licence, for applications under the Aboriginal Peoples of Canada Adaptations Regulations (Firearms), and Fee and Photo Waivers. The scope of the PIA is restricted to changes in how the Canadian Firearms Program collects personal information related to these enhancements.

For the full summary: MyCFP Enhancements, Release 1, Program Increment 1 | Royal Canadian Mounted Police.

MyCFP Enhancements, Release 1, Program Increment 2

The RCMP Canadian Firearms Program (CFP) is modernizing its service delivery. The "MyCFP" portal enhancements provide new functionalities to the Canadian Firearms Public Digital Services Solution. This phase of updates will allow members of the public to use the portal to submit four additional types of applications that were previously paper only. A PIA was completed to ensure the RCMP meets its legal obligations under the *Privacy Act*, and to ensure that privacy risks are identified, assessed and mitigated related to the following new services available on the portal: application for a carrier licence (first application only), application for a firearms licence for businesses or a museum (first application only), shooting club or shooting range approval application (first application only), and shooting club membership submission.

For the full summary: MyCFP Enhancements, Release 1, Program Increment 2 | Royal Canadian Mounted Police

National Child Exploitation Crime Centre

The RCMP National Child Exploitation Crime Centre (NCECC) is a national program within the Sensitive and Specialized Investigative Services Branch that is mandated to reduce the vulnerability of children to Internet-facilitated sexual exploitation under Canada's *National Strategy for the Protection of Children from Sexual Exploitation on the Internet*. As the lead RCMP Program, the NCECC is responsible for operationalizing the National Strategy's objectives by identifying victimized children; investigating and supporting criminal justice outcomes; developing and deploying innovative technologies; providing criminal intelligence support; and strengthening the capacity of municipal, territorial, provincial, federal, and international police agencies through research, training, technology, intelligence and investigative support.

The program-level PIA considers the personal information handling practices of the NCECC to ensure the RCMP meets its legal obligations under the *Privacy Act*, and to ensure that privacy risks are identified, assessed, and mitigated, including in the use of operational technologies. To increase transparency, the RCMP created a new personal information bank specific to NCECC activities. The bank documents NCECC's

matching activities, including face matching to quickly sort, group and categorize large amounts of similar data to expedite human review and evaluation.

For the full summary: National Child Exploitation Crime Centre | Royal Canadian Mounted Police

National Digital Forensics Program

The RCMP National Digital Forensics Program's mandate is to implement lawful technological techniques using Digital Forensics Access Tools to search and seize digital criminal activity data from lawfully seized electronic devices. Digital Forensics Access tools are tools or techniques utilized to access digital evidence, which may vary depending on the hardware, software and network configurations of the lawfully seized devices. Data is extracted under warrant or lawful authority and in compliance with the *Canadian Charter of Rights and Freedoms*. A PIA was completed to ensure that the RCMP's use of Digital Forensics Access tools meets its legal obligations under the *Privacy Act* and to promote transparency with the public. The assessment found that the privacy impact associated with the use of these tools is expected to be low.

For the full summary: National Digital Forensics Program | Royal Canadian Mounted Police

Body Worn Cameras (BWC) and Digital Evidence Management System (DEMS)

In 2020, the Government of Canada announced funding for the implementation of a National BWC Program for the RCMP. As part of the program, the RCMP will deploy up to 15,000 BWCs to frontline officers. Once fully implemented, all RCMP officers interacting with the public will be equipped with a BWC while on duty. BWCs will be used in plain sight to capture audio/visual recordings of interactions and incidents between uniformed police officers and members of the public.

The purpose of the PIA was to ensure that the RCMP operates its BWCs in a privacy sensitive manner. The PIA reviewed the lifecycle of personal information collected through BWCs and an assessment of core features and functionality of the RCMP's BWC and DEMS where the videos will be stored. The RCMP addressed most privacy issues in the PIA process. Risk mitigation measures, implemented prior to the program's launch and monitored on an ongoing basis, are expected to reduce the program's overall privacy risk to a low or acceptable level.

For the full summary: Body Worn Camera (BWC) and Digital Evidence Management Service (DEMS) | Royal Canadian Mounted Police

Race-Based Data Collection Initiative Project

The collection, analysis and disclosure of disaggregated race-based data is a priority for the RCMP and the Government of Canada to address systemic racism. The RCMP will adopt a "phased approach" to collecting, analyzing and reporting perceived race-based data (a member's perception of an individual's race or Indigenous identity). Members of the public will not be asked to self-identify. Data extracted from a select number of locations will eventually be used to publicly report trends and develop action plans. As a first step, the RCMP initiated a pilot which was the subject of this PIA. In scope of the pilot and the PIA are the collection of perceived race-based data and perceived Indigenous identity in selected locations,

data quality assessments to enable analytics of de-identified data and public reporting in relation to use of force, wellness checks and arrests.

For the full summary: Race-Based Data Collection Initiative project | Royal Canadian Mounted Police

Assault-Style Firearms Compensation Program Phase 1 - Business

The "Assault-Style Firearms (ASF) Compensation Program Phase 1 - Business" is a multi-institutional PIA led by Public Safety Canada and supported by its partners, the RCMP and Employment and Social Development Canada (ESDC)/Service Canada. This PIA aims to facilitate the self-declaration of ASF owners; the collection, validation, and destruction of ASFs; and issuing compensation.

For the full summary: Assault-Style Firearms Compensation Program Phase 1 - Business | Royal Canadian Mounted Police.

ADVISORY SERVICES

In addition to reviewing PIAs, PMD provided advice and guidance to business lines on completing questionnaires to determine the need for a PIA, Treasury Board Submissions, Memoranda to Cabinet, Memoranda of Understanding and privacy notice statements, as well as facilitating engagements with the Office of the Privacy Commissioner.

Privacy Impact Assessment Questionnaires

During the reporting period, PMD reviewed 66 PIAQs, from all sectors of the organization (Federal Policing, Contract and Indigenous Policing, Specialized Policing Services, and Internal Services). Eighteen of the PIAQs reviewed were part of the National Technology Onboarding Program (NTOP) assessment process. As per RCMP policy, PMD is a key stakeholder of the NTOP assessment process. PMD participates in meetings with business lines and vendors and assesses whether the onboarding of the new technology requires a PIA or any other mitigating measures to ensure the RCMP's compliance with the *Privacy Act* and TBS policies.

In accordance with the requirements of the Policy on Privacy Protection, the RCMP regularly notifies the OPC and TBS of emerging initiatives that may have an impact on the privacy of Canadians. During the reporting period, the RCMP submitted three notifications. PMD also continues to meet with the OPC and TBS to provide updates on key files on a regular basis.

Memoranda of Understanding/Information Sharing Agreements

During the reporting period, the PMD reviewed 58 MOU/ISAs from all sectors of the organization (Federal Policing, Contract and Indigenous Policing, Specialized Policing Services, and Internal Services) ensuring they complied with TBS policy requirements for arrangements involving personal information.

Privacy Notices

During fiscal year 2024-2025, PMD drafted 109 privacy notice statements for clients looking to either create new forms or update existing forms collecting personal information.

Engagements with the Office of the Privacy Commissioner

In addition to regular file updates, the RCMP engaged in five consultation sessions with the OPC. For example, the RCMP sought the OPC's advice on the Race-Based Data Collection initiative, as well as on the privacy implications related to the transition of police jurisdiction prior to submitting the respective PIAs. The RCMP also met with the OPC on the following initiatives:

NG 911

Next Generation (NG) 9-1-1 has been mandated by Canadian Radio-television and Telecommunications Commission (CRTC) for all 9-1-1 call handling services in Canada. The goal of these sweeping changes is to enable new tools for first responders which should result in faster response times, and more accessible communication during emergencies. The changes will eventually enable the caller to provide more information to 9-1-1 dispatchers, including sending video/photo and medical information, but begins with changes to the backend systems. The RCMP is undertaking several PIAs to document the impact these changes will have on privacy and mitigate any risks. As part of these efforts, on February 18, 2025, the RCMP engaged in a consultation session with the OPC on the preliminary privacy analysis of these impacts and sought their feedback.

Draft RCMP Facial Recognition Policy (FRT)

The RCMP's National Technology Onboarding Program (NTOP) sought the OPC's advice on its draft policy on FRT through an advisory consultation facilitated by PMD. The draft policy takes into consideration, amongst other things, the OPC's "Privacy guidance on facial recognition for police agencies" and the 2022 Standing Committee on Access to Information, Privacy and Ethics (ETHI) report, "Facial Recognition Technology and the Growing Power of Artificial Intelligence." The draft policy establishes definitions, limits, and internal processes that must be followed prior to the use of FRT by the RCMP. At the time of writing, the RCMP continues to consult internally and externally on its draft policy.

PUBLIC INTEREST DISCLOSURES

During the 2024-2025 fiscal year, 29 disclosures were made pursuant to paragraph 8(2)(m) of the *Privacy Act*. The majority of disclosures were related to the duty status of RCMP members subject to discipline. The remaining disclosures were associated with the release of dangerous offenders into communities across Canada and aviation accidents.

In accordance with subsection 8(5) of the PA, the OPC was notified of all such disclosures in writing.

MONITORING COMPLIANCE

The ATIP Branch frequently makes use of comprehensive reporting tools to monitor compliance and maintain accountability, as well as to identify process improvements.

Time taken to process PA requests

The ATIP Branch monitors the time taken to process PA requests by retrieving statistics from the case management software on a daily, weekly, monthly and quarterly basis. These statistics provide information on the compliance rate, the number of files completed on time and those that are delayed,

as well as complaints both received and closed. Performance dashboards are also key tools to further identify trends and assist the ATIP Branch in strategically developing efficiencies. The Branch's management team reviews the weekly and monthly reports to manage workload and to determine any upcoming issues where processes could be improved. The reports and dashboards are provided to senior management in an effort to improve accountability.

The ATIP Branch continues to work on bolstering its data reporting function by onboarding new technology and processes. This new technology will enable the ATIP Branch to be more strategic and transparent by automatically capturing pertinent data to assist with its planning and public reporting, as well as to identify areas where efficiencies may be found.

APPENDIX A - DELEGATION ORDER

Access to Information Act and Privacy Act Delegation Order

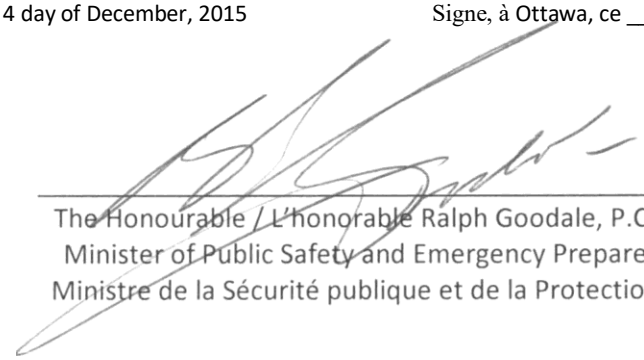
The Minister of Public Safety and Emergency Preparedness, pursuant to section 73 of the *Access to Information Act* and of the *Privacy Act*, hereby designates the persons holding the position set out in the schedule hereto, or the persons occupying on an acting basis those positions, to exercise the powers and functions of the Minister as the head of a government institution, that is, the Royal Canadian Mounted Police, under the section of the Act set out in the Schedule opposite each position. This designation replaces and nullifies all such designations previously signed and dated by the Minister.

SCHEDULE

Position	**Privacy Act and Regulations**	***Access to Information* Act and Regulations**
Commissioner of the RCMP	Full Authority	Full Authority
Chief, Strategic Policy and Planning Officer		
Departmental Access to Information and Privacy Coordinator		
Commanding Officers	Authority for 8(2)(j) and 8(2)(m)	N.A.
Officer in Charge, Policy, Processing and External Relations	Full Authority except 8(2)(j) and 8(2)(m)	7, 8(1), 9, 11(2) to 11(6) (inclusive), 12(2) and all mandatory exemptions (13(1), 16(3), 19(1), 20(1) and 24(1)) and 6(1) and 8 of the Regulations
Manager, Processing and Triage		
Manager, Quality Control		
Non-Commissioned Officers and public servants in charge of ATIP unit		
Non-Commissioned Officers and public servants in charge of ATIP Branch (analysts)	14 and 15 for all records; 17(2)(b), 19 to 28 (inclusive) for all employee records as designated in InfoSource; For all other records requiring mandatory exemptions in their entirety (19(1), 22(2) and 26) of the Act; 9 and 11(2) of the Regulations	7, 8(1) and 12(2)(b) and all records exempted in their entirety by mandatory exemptions (13(1), 16(3), 19(1), 20(1) and 24(1)) of the Act; 6(1) and 8 of the Regulations

Signed, at the City of Ottawa, this 4 day of December, 2015

Signe, à Ottawa, ce __ jour de _____ , 20



The Honourable / L'honorable Ralph Goodale, P.C., M.P.
Minister of Public Safety and Emergency Preparedness
Ministre de la Sécurité publique et de la Protection civile