Annual Report to Parliament on the Administration of the Privacy Act 2025-2026

Communications Security Establishment Canada

Pursuant to subsection 72(1) of the *Privacy Act*, this document contains the Annual Report to Parliament on the Administration of the *Privacy Act* for 2025-2026 as submitted by the Minister of National Defence.

Table of Contents

Introduction 1
Mandate of the Communications Security Establishment Canada 1
Organizational Structure 2
Delegation Order 4
Performance 2025-2026 5
- Number of Formal Requests 5
- Disposition of Completed Requests 6
- Neither Confirm Nor Deny 7
- Completion Time 7
- Exemptions to the Release of Information 9
- Extension of the Time Limit 9
- Consultations 9
- Summary of Key Issues and Actions Taken on Complaints 10

Education and Training 11
Policies, Guidelines, and Procedures 13
Other Key Initiatives 14
Initiatives and Projects to Improve Privacy 14
Material Privacy Breaches 14
Privacy Impact Assessments 14
Public Interest Disclosure 15

Monitoring Compliance 16
Appendix I: Delegation of Authority 17

Introduction

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

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

This is the thirteenth annual report prepared by the Communications Security Establishment Canada (CSE) and tabled in Parliament in accordance with section 72 of the *Act*. It presents an overview of the agency's activities and describes how the Access to Information and Privacy (ATIP) Office and Privacy Office carried out their responsibilities under the *Privacy Act* during the reporting period from 1 April 2025 to 31 March 2026.

Mandate of the Communications Security Establishment Canada

On August 1st, 2019, the *Communications Security Establishment Act* (*CSE Act*) entered into force as part of Bill C-59 (*An Act respecting national security matters*). The *CSE Act* sets out the five (5) aspects of CSE's mandate:

- helping to protect and defend Canada's most important cyber systems;
- acquiring foreign intelligence in support of the Government of Canada's intelligence priorities;
- conducting defensive foreign cyber operations;
- conducting active foreign cyber operations; and
- providing technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence.

The *CSE Act* provides CSE with a modern set of authorities and enhances the accountability framework with new oversight and review functions.

Organizational Structure

The ATIP Office and Privacy Office are both part of the Review, Transparency and Information Sharing (RTIS) directorate in CSE's Authorities, Compliance and Transparency (ACT) Branch. The Privacy Office, formerly known as the Privacy Policy and Governance Office (PPGO), has continued to evolve since FY 2024-25.

In FY 2025–2026, privacy-related functions supporting compliance with the *Privacy Act*, including policy, risk, training, and awareness, were realigned from Transparency and Information Sharing to the External Review team, with both teams remaining part of the RTIS directorate. This organizational change reflects the increasing strategic importance of privacy across the organization and will enhance CSE's ability to provide effective oversight, guidance, and engagement in response to evolving technologies, operational priorities, and privacy requirements. Looking ahead into next fiscal year, CSE will continue to advance and refine its privacy program to support strong governance, accountability, and service delivery.

The Privacy Office plays a key role in advancing privacy governance and strengthening privacy protections across the organization. During the 2025-2026 reporting period, the Office was comprised of one (1) manager responsible for seven (7) full-time positions, including one (1) supervisor, and six (6) analysts.

Specifically, the Privacy Office is responsible for the following activities:

- Supporting Deputy Chief, Authorities, Compliance and Transparency (ACT), CSE's Chief Privacy Officer in ensuring the institution's programs and activities are in accordance with the requirements of the *Privacy Act* and related policy instruments;
- Identifying and managing privacy risks across the institution, partly by leading or supporting the development of Privacy Impact Assessments, Privacy Needs Analyses, System Identification Documents, Privacy Notice Statements, and maintenance of Personal Information Banks;
- Supporting CSE's legislative compliance obligations under the *Privacy Act*, including the application of associated regulations, policies and guidelines;
- Identifying and managing privacy breaches and material privacy breaches;

- Representing CSE in privacy protection communities of practice;
- Coordinating the annual update of the institution's Info Source publication, which includes a description of the agency's organizational structure and record holdings;
- Drafting and implementing privacy-related policies, internal procedures, guidance documents and working aids; and,
- Providing training to CSE staff on the administration of the *Privacy Act* focusing on the protection of personal information.

The CSE ATIP Office has continued to grow since the last reporting period. The disclosures tasks beyond the processing of requests under the ATIA and PA, have necessitated the creation of a new ATIP team structure. In mid-January 2025, CSE's ATIP Office was divided into two separate teams, ATIP Intake and Proactive Disclosures team and ATIP Operations. The split between the teams is intended to address the backlog of requests, claim time extensions, when possible, streamline ATIP response processes and complaints. CSE's ATIP Office backlog has led to an increased deemed refusal rate and complaints which it now seeks to address with this realignment. Our objective with this modification is to modernize our processes, improve efficiency and facilitate improvements to the ATIP Office's ability to respect legislative timelines. The CSE ATIP Office is working towards processing requests more promptly and has taken positive steps to establish efficient workflows while addressing team growth.

The ATIP Office includes a manager responsible for nine (9) full-time positions working in two (2) teams: ATIP Operations and ATIP Intake. At the end of the reporting period, the ATIP Operations team consisted of one (1) supervisor and four (4) analysts. The ATIP Intake team consisted of one (1) supervisor, two (2) analysts, and one (1) support officer.

In addition to preparing reports for Parliament and Treasury Board Secretariat (TBS), the ATIP Office acts on behalf of CSE as the delegated authority in dealings with TBS, and representatives of the federal Information and Privacy Commissioners regarding CSE's administration of the *Access to Information Act* (ATIA) and *Privacy Act* (PA).

Specifically, the ATIP Operations and ATIP Intake teams are responsible for the following activities:

- Processing requests under the *Access to Information Act* and *Privacy Act;*
- Responding to consultation requests from other government institutions;

- Providing advice and guidance to senior management and staff of CSE on ATIP legislation and policy-related matters;
- Supporting CSE's legislative compliance obligations under the *Acts*, including the application of their associated regulations, policies and guidelines;
- Representing CSE in ATIP Communities of practice, such as the TBS ATIP Community meetings;
- Drafting and implementing internal ATIP procedures, guidance documents and working aids; and,

Providing training and other outreach initiatives to CSE staff on the administration of the *Access to Information Act* and the *Privacy Act*.

Delegation Order

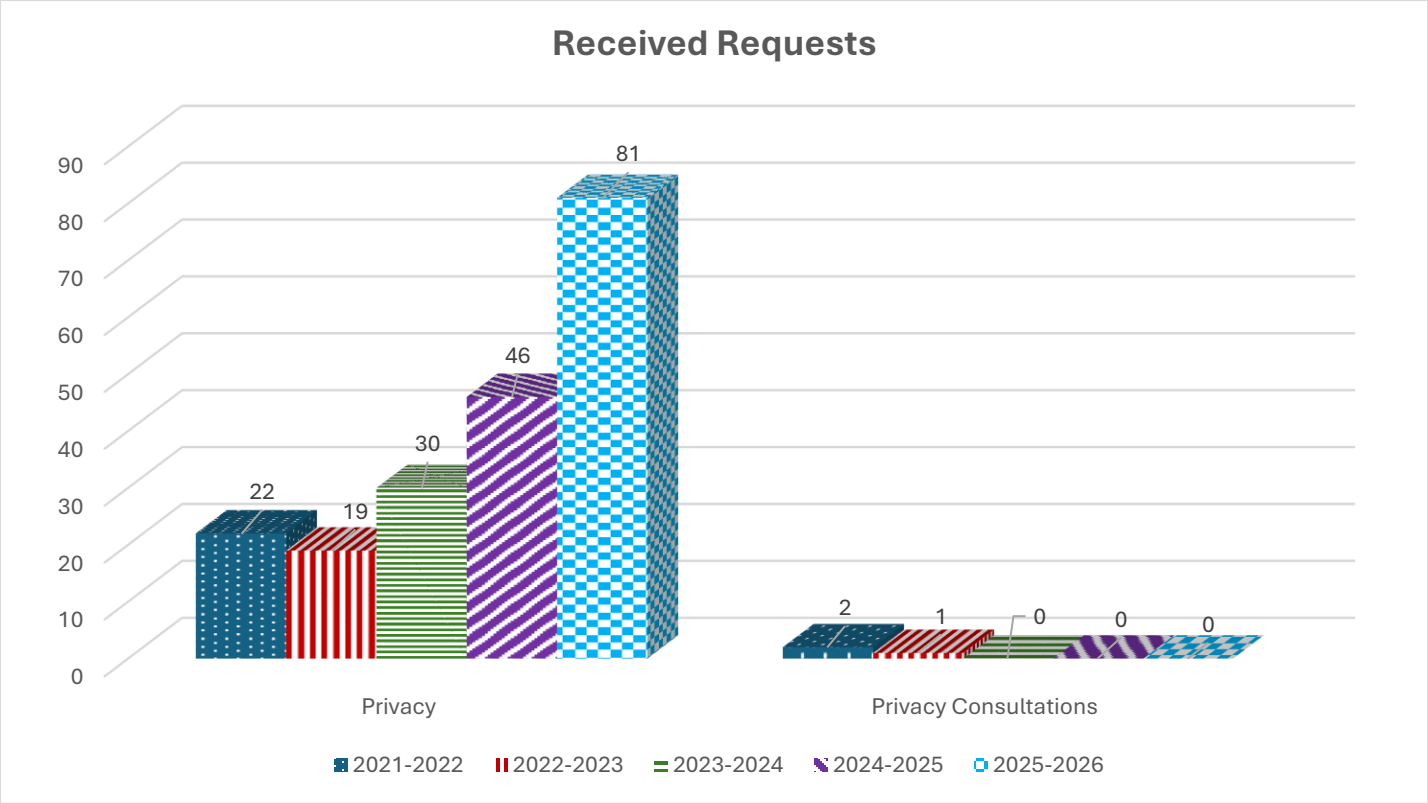
Pursuant to section 73 of the *Privacy Act*, the Minister of National Defence (MND), the Honourable David J. McGuinty, delegated the exercise of *Privacy Act* authorities to designated officials within CSE. The Chief, CSE, the Deputy Chief Authorities, Compliance and Transparency, the Director General, Review, Transparency and Information Sharing, the Director, Transparency and Information Sharing, and the Manager, Transparency and Disclosures hold full delegated authority, except for public interest disclosures under paragraph 8(2)(m), which require the joint approval of the Chief, CSE and the Deputy Chief, Authorities, Compliance and Transparency. Limited authorities are also delegated to the Supervisor, ATIP Operations and the Supervisor, ATIP Intake.

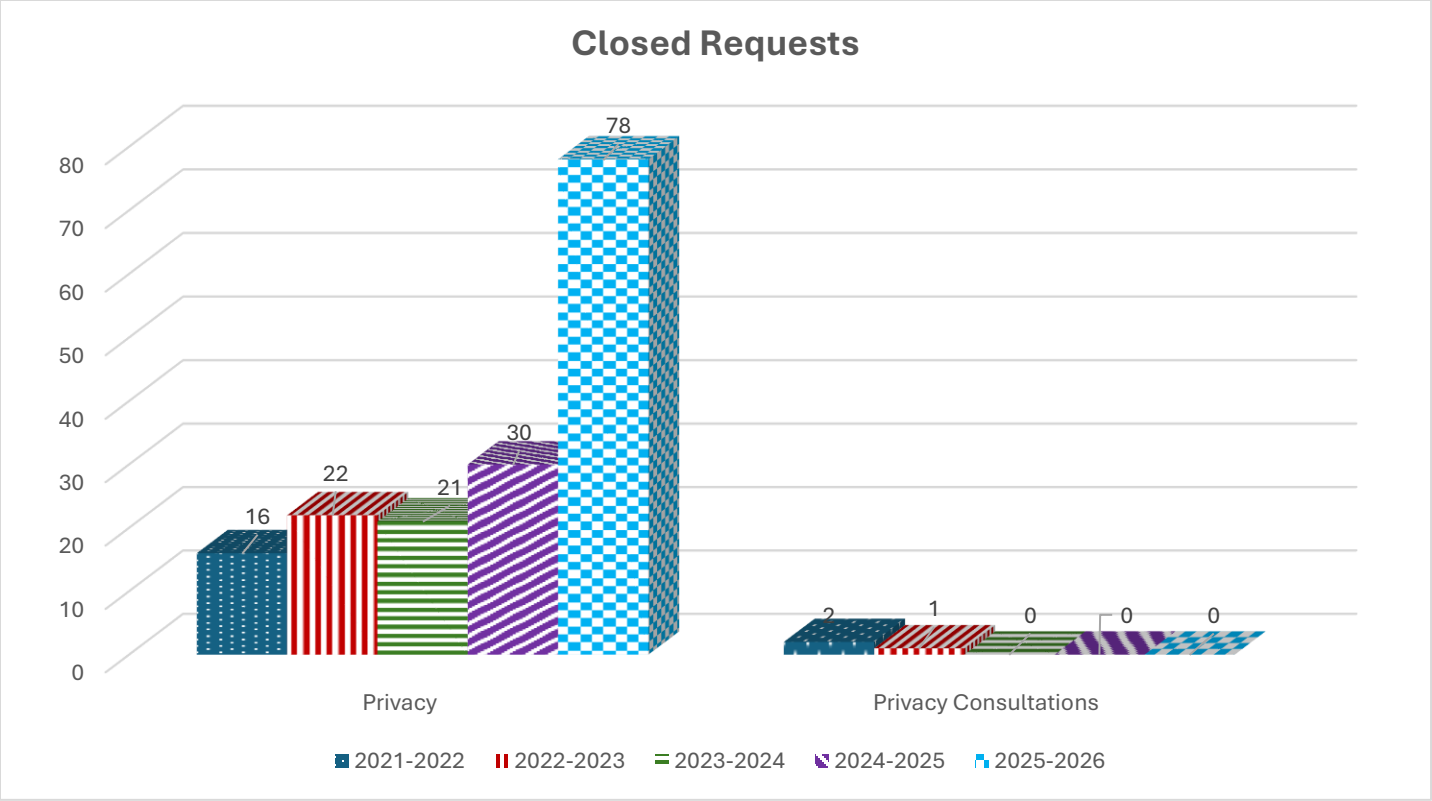
At the end of FY 2025–2026, CSE's *Privacy Act* Delegation Order was updated to align with organizational changes and evolving operational requirements. The updates included new and revised delegated authorities, expanded authority for certain disclosures related to employee wellness and CSE's Assistance Program (CAP), and changes to ensure continued accountability and effective privacy governance across the organization. A copy of the updated *Privacy Act* Delegation Order can be found in the Appendix I this report.

Performance 2025-2026

Number of Formal Requests

During this reporting period, CSE received eighty-one (81) requests under section 12(1) the *Privacy Act*, which is an increase from the previous fiscal year when forty-six (46) new requests were received. In addition, twenty-four (24) requests outstanding from the previous reporting period were carried over and twenty-three (23) from more than one reporting period ago, giving CSE a total of forty-seven (47) requests to process. By the end of 2025-2026, CSE closed seventy-eight (78) requests and carried forward fifty (50) into 2026-2027.

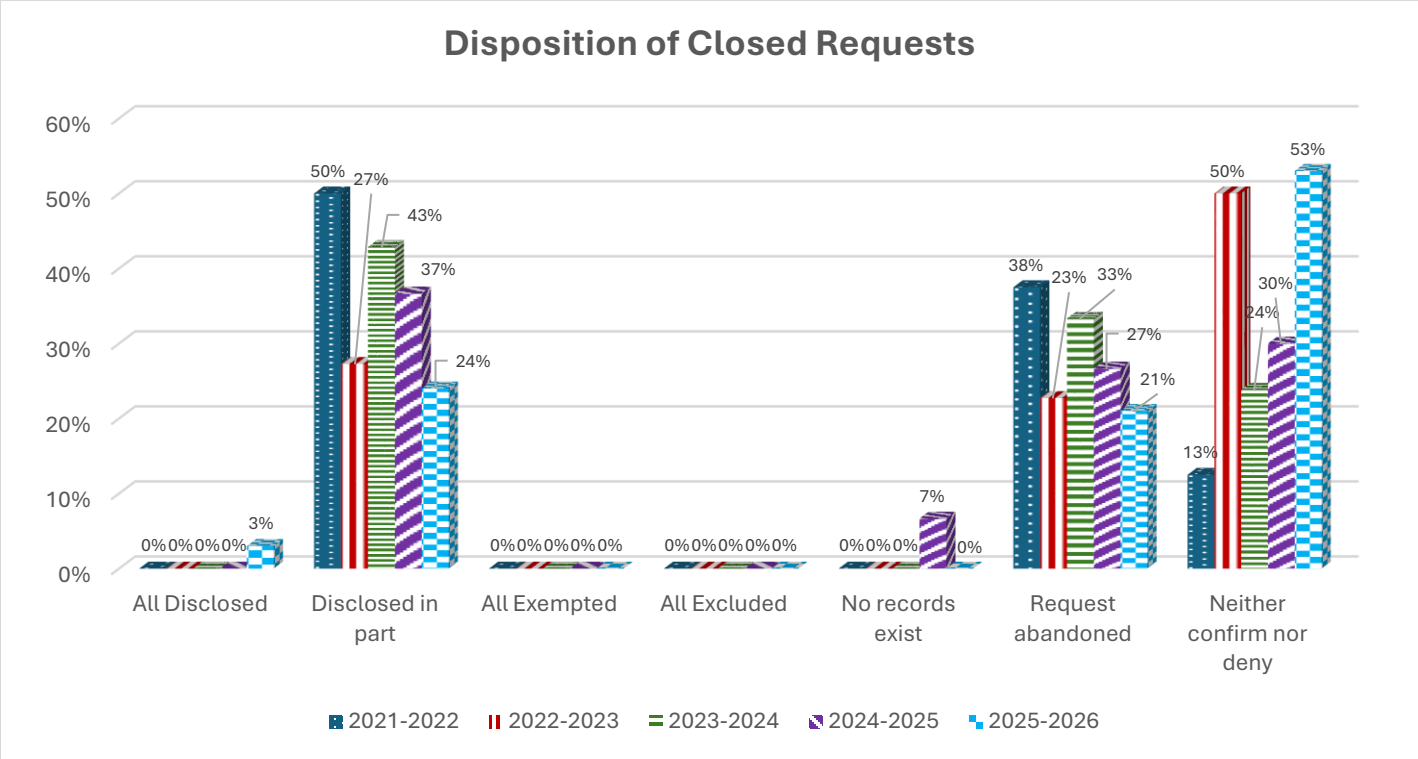




Disposition of Completed Requests

CSE closed 78 requests during this reporting period. Of these, nineteen (19) (24%) were disclosed in part, two (2) (3%) were disclosed in full and sixteen (16) (21%) were abandoned by the applicants. Zero (0) requests resulted in no records being found. There were also forty-one (41) (53%) requests where the existence of records was neither confirmed nor denied, which is a significant increase from

nine (9) records in 2024-2025. There were no requests which were exempted or excluded in full.



Neither Confirm Nor Deny

Section 16(2) of the *Act* indicates that institutions do not have to tell a requester whether personal information exists. Section 16(2) was designed to address situations in which the mere confirmation of a record's existence (or non-existence) would reveal information that could be protected under the *Act*. It is recommended that the application of section 16(2) be limited to circumstances where the confirmation or denial of the existence of a record would be injurious to Canada's foreign relations, the defence of Canada, law enforcement activities, or the safety of individuals. When notifying a requester that it is invoking this provision, institutions must also indicate the part of the *Act* on which a refusal could reasonably be expected to be based if the record existed. As noted above, the application of subsection 16(2) was used forty-one (41) times during the 2025-2026 fiscal year.

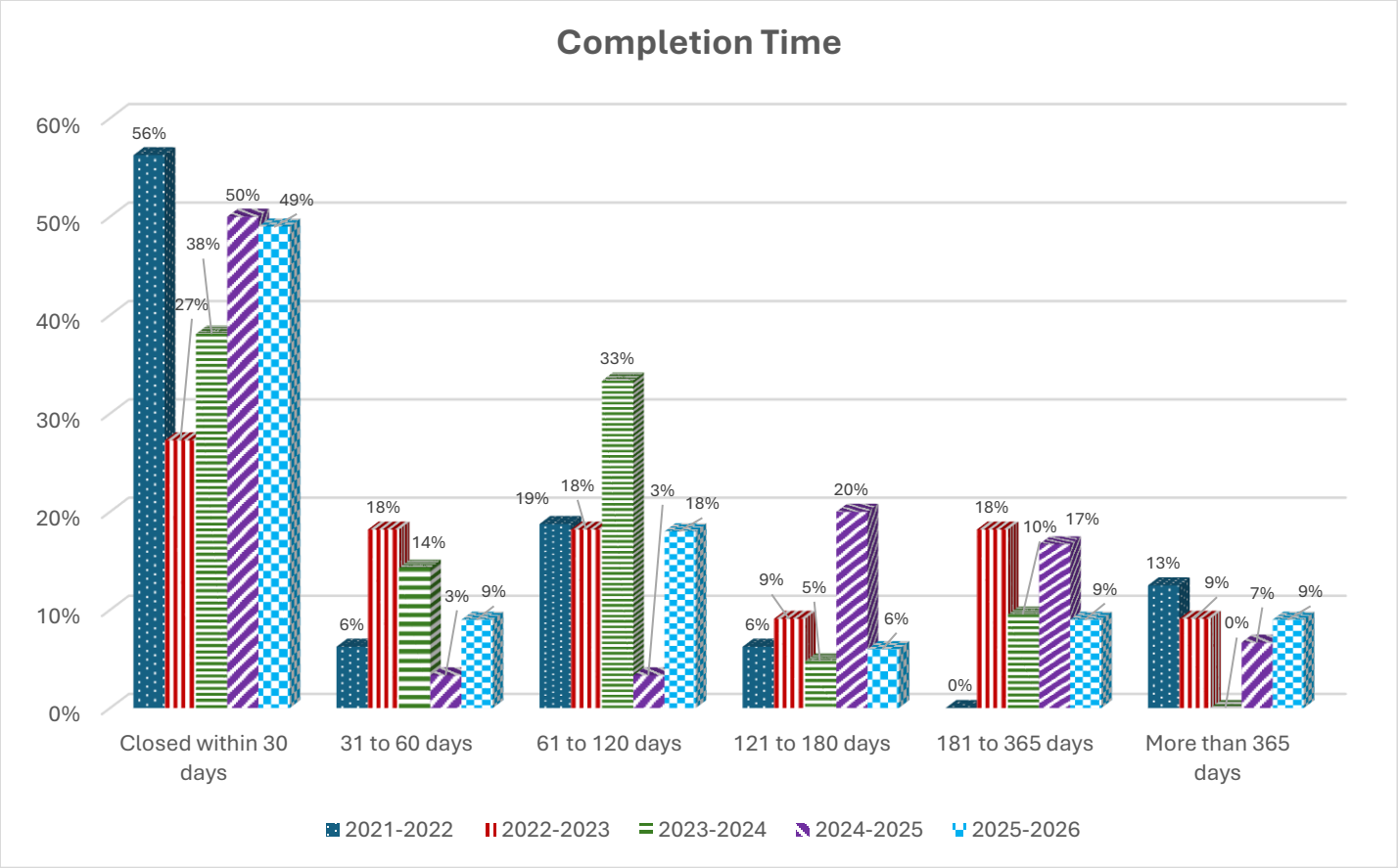
Completion Time

During the 2025-2026 fiscal year, thirty-nine (39) of the completed requests made under the *Privacy Act* were closed within the legislative timeframe, representing 50% of all completed requests. One (1) of these requests included an extension beyond the initial 30 days. CSE closed thirty-eight (38) requests within 0-30 days; seven (7) between 31 and 60 days; fourteen (14) between 61 and 120 days;

five (5) between 121 and 180 days; seven (7) between 181 and 365 days; and seven (7) took more than 365 days to process. In general, the requests received during 2025-2026 involved information of a highly sensitive nature resulting in greater complexity in fulfilling them. CSE processed a total of 9,386 pages in 2025-2026 compared to 9379 pages in 2024-2025. Of the total requests carried over into 2026-2027, twenty-four (24) (48%) were received during the 2025-2026 reporting period.

Open Requests outstanding from previous reporting periods

Reporting period received	Within Legislated timelines	Beyond Legislated timelines	Total
2016-2017 or earlier	0	4	4
2017-2018	0	0	0
2018-2019	0	0	0
2019-2020	1	1	2
2020-2021	0	4	4
2021-2022	0	3	3
2022-2023	0	3	3
2023-2024	0	3	3
2024-2025	0	7	7
2025-2026	10	14	24
Total	**11**	**39**	**50**



Exemptions to the Release of Information

The most common exemptions applied at CSE were sections 21 and 26 of the *Privacy Act*. Section 21 was applied in twenty (20) requests to protect information which could be reasonably expected to be injurious to the defense of Canada. Section 26 was applied in nineteen (19) requests to protect information about an individual other than the applicant. The application of these exemptions is consistent with previous reporting periods.

Extension of the Time Limit

Eight (8) extensions, based on Section 15 (a)(ii) of the *Privacy Act* relating to internal consultation, were taken on requests under the *Privacy Act* during the 2025-2026 fiscal year. Five (5) extensions were taken based on Section 15(a)(i) on requests with a large volume of pages resulting in interference with operations.

Consultations

CSE received no (0) consultations from other government departments.

Summary of Key Issues and Actions Taken on Complaints

Individuals who are not satisfied with the processing of their privacy request or who feel that their personal information has been improperly collected, used or disclosed can file a complaint with the Office of the Privacy Commissioner of Canada (OPC). The ATIP Office processes complaints directly related to requests for personal information. The Privacy Office responds to complaints related to improper collection, use or disclosure outside of the request process.

CSE received nine (9) complaints during fiscal year 2025-2026 and closed eight (8) complaints against CSE. CSE provided information to the OPC in relation to all complaints as requested.

Of the eight (8) request-related complaints received in the current reporting period, three (3) alleged that CSE had not provided responsive records within the prescribed time periods. The remaining five (5) were complaints alleging that CSE had not appropriately applied exemptions under the PA. CSE made representations to the OPC regarding complaints as requested and continues to work with the OPC to resolve them in a timely manner. One (1) delay complaint and two (2) exemption complaints were closed at the early resolution stage with no findings.

Six (6) of the closed complaints were related to requests for personal information. Two (2) were carried forward from the 2024-2025 reporting period. Two (2) of the closed complaints related to delays in the processing of the related requests. Both were found to be well founded and resolved on the release of the information to the requestor. The remaining four (4) were due to allegations of inappropriately applied exemptions. Two (2) were found to be well founded and resolved through the release of additional information to the complainant. One (1) was closed with no finding and one (1) was found to be not well founded.

The Privacy Office responded to the OPC in relation to two (2) complaints during the 2025-26 reporting period. The first complaint involved an ongoing OPC investigation into a data breach at another Government of Canada department pertaining to access to personal information under their control. Although the complaint was not directed at CSE, CSE supported the completion of OPC's investigation through the provision of feedback on the OPC's findings to contextualize CSE's role and operational considerations associated with the monitoring and detection of government infrastructure noting the challenges posed by an evolving threat landscape. CSE was informed that this complaint is conditionally closed and that the other department accepted both of OPC's recommendations which were issued to them.

The second complaint which was directed at CSE alleged that CSE inappropriately collected personal information during a security screening process. CSE provided information and submissions to support the OPC's investigation which was concluded during the reporting period. Based on the

OPC's investigation, the allegations in the complaint were not well-founded and the OPC closed the complaint. The matter is considered resolved.

At the end of the reporting period, the OPC had five (5) open complaints with CSE. CSE continues to work closely with the OPC to resolve complaints received in previous reporting periods in an efficient manner.

Active Complaints from previous reporting periods

Reporting period received	Number of Open Complaints
2016-2017 or earlier	0
2017-2018	0
2018-2019	0
2019-2020	0
2020-2021	0
2021-2022	3
2022-2023	0
2023-2024	1
2024-2025	1
2025-2026	0
Total	**5**

Education and Training

CSE is committed to the ongoing learning and development of its employees and provides comprehensive privacy awareness training sessions to ensure all employees are up to date on their responsibilities regarding the management of personal information in both mission and non-mission-related activities.

In 2025-2026, 312 employees completed CSE's online privacy awareness training module to strengthen their understanding and awareness of privacy at CSE, including: the rights and obligations

of employees; the roles and responsibilities of the Privacy Office; Privacy Principles pertaining to the collection, use, access, retention, and disclosure of personal information. All CSE employees are required to complete this training module at the beginning of their career at CSE and then once every three years.

In addition to CSE's standard privacy training, the Privacy Office also undertook initiatives designed to increase awareness and educate employees on *Privacy Act* obligations setting the foundation for a robust and sustainable privacy management framework. This included organizing special events and raising awareness throughout Privacy Awareness Week (PAW) where the Privacy Office promoted best practices and shared various materials and resources with employees through in-person and virtual presentations and workshops highlighting the importance of the protection of personal information. For instance, the Privacy Office delivered a workshop to CSE stakeholders in public-facing offices to demystify Public Interest Disclosures, their purpose and the process for disclosures at CSE including injury test thresholds. A presentation was also delivered to CSE employees to highlight privacy as a collective responsibility and the respective roles of the organization and its employees in managing privacy risks.

Another awareness building initiative undertaken this year by the Privacy Office was the delivery of a CSE-wide privacy awareness presentation as part of CSE's Operational Compliance week in January 2026. This presentation highlighted how privacy responsibilities are coordinated across CSE and how employees are supported in handling personal information appropriately. It also explored the collaborative approach between the Privacy Office, Policy, and Compliance teams to help the organization meet its privacy obligations while enabling employees to carry out their work effectively and responsibly.

Furthermore, the Privacy Office proactively engaged with TBS to support the consistent interpretation and application of privacy requirements under the *CSE Act* and the *Privacy Act*. The Office also worked with senior management and teams in various areas across CSE to increase awareness of privacy impact assessment obligations and promote sound privacy practices, further strengthening the organization's privacy governance framework.

In addition to this, the ATIP Office delivered 10 informal briefings and one-on-one training sessions during the reporting period to approximately 21 individuals as well as participating in awareness sessions for co-op students.

These training sessions were delivered to specific audience groups such as operational units, corporate teams, new staff and coop students on a regular and *ad hoc* basis.

New employees are required to complete an online training session "Privacy Awareness" within three months of their start date. CSE also encourages employees to take advantage of access to information and privacy courses offered through the Canada School for Public Service (CSPS).

Policies, Guidelines, and Procedures

The CSE's organizational privacy policy outlines CSE's obligations to manage and protect personal information during its corporate functions in accordance with the *Privacy Act*, its regulations, and Treasury Board Secretariat (TBS) policies relating to privacy. It also outlines the mandatory requirement for all CSE staff to complete privacy awareness training.

Throughout this reporting period, the Privacy Office reviewed its administrative privacy policy as well as provided input into CSE's operational policy suite from a privacy perspective. CSE's operational policy suite was updated as part of broader changes and modernization efforts including compliance with its privacy obligations under the *CSE Act* and *Privacy Act*.

This year, CSE's Privacy Office continued to review and update its internal privacy standard operating procedures (SOPs) and processes including Privacy Impact Assessments, Privacy Breaches and Public Interest Disclosures to strengthen engagement and improve the quality of these products. These procedures and processes were also updated to ensure alignment with TBS privacy policies and directives as well as the implementation of OPC's reporting standards and on-line tools.

CSE's internal policies and processes will continue to be reviewed, refined and instituted in the 2026–2027 reporting period.

There were no new collections or consistent use of Social Insurance Numbers reported to the Privacy Office throughout the reporting period.

CSE requires that privacy considerations be addressed in contracts, agreements, and arrangements involving personal information, including those with service providers, as appropriate. Contractual requirements are informed by relevant legislation, policy, privacy, and security obligations.

The teams are also actively recruiting new hires both internal and external to the federal government. It is important to note though that CSE's hiring process is conducted in three phases which can take anywhere from 6-12 months or longer thereby making it challenging to respond quickly to staffing needs.

Other Key Initiatives

It is important to note that the ATIP Office also supports the work of the National Security Intelligence Review Agency (NSIRA), the National Security and Intelligence Committee of Parliamentarians (NSICOP), and the Intelligence Commissioner (IC) by reviewing their documents, which contain sensitive CSE information, and providing unclassified versions that can be shared openly with the public.

Non-ATIP related requests have impacted on the time our team can devote to access and privacy requests. This time is not represented in the statistical reporting, but accounts for approximately 0.974 FTE for the reporting period, a decrease from 1.77 in 2024-2025. This reduction largely reflects NSIRA's shift to formal consultations with CSE under the *Access to Information Act*.

Initiatives and Projects to Improve Privacy

CSE has been using the ATIP Online Management Tool (AOMT) which replaced the ATIP Online Request Service (AORS) in this reporting period. The AOMT is a centralized website developed by TBS that enables users to complete access to information requests and submit them to any of the institutions that are subject to the Government of Canada's *Privacy Act*. CSE received 67 requests via this service, representing approximately 83% of the total requests received. 15% of requests were received by email and the remaining 2% through regular mail.

The ATIP Office is in the process of onboarding to the AMANDA software. This will be implemented in the 2026-2027 reporting period and will help to modernize and streamline processes and enhance monitoring to improve compliance.

Material Privacy Breaches

No (0) material privacy breaches were reported to the Office of the Privacy Commissioner and the Treasury Board of Canada Secretariat in the reporting period.

Privacy Impact Assessments

During the 2025-2026 reporting period, CSE completed a Privacy Impact Assessment (PIA) on the disclosure of Canadian Identifying Information (CII) under section 43 of the *Communications Security*

Establishment Act (*CSE Act*). Specifically, this PIA assesses the privacy risks and controls associated with disclosures made in support of CSE's mandate, including requirements for secure handling, rigorous review and approval, and verification of the receiving partner's lawful authority and operational need for Canadian Identifying Information. CSE's PIA on the Disclosure of CII was approved by CSE in August 2025 and was submitted to both the OPC and TBS for their review. CSE will post the unclassified summary for this PIA on CSE's website in FY 2026-2027.

Public Interest Disclosure

Subsection 8(2) of the *Privacy Act* describes the circumstances under which a government institution may disclose personal information under its control without the consent of the individual to whom the information relates. Such disclosures are discretionary and are subject to any other Act of Parliament.

Paragraph 8(2)(m) stipulates that an institution may disclose personal information for any purpose where, in the opinion of the head of the institution, the public interest in the disclosure clearly outweighs any invasion of privacy that could result from it or where the disclosure would clearly benefit the individual to whom the information relates.

During the 2025-2026 reporting period, CSE made four (4) public interest disclosures pursuant to section 8(2)(m) of the *Privacy Act*. Two cases involved child exploitation material uncovered by and or disclosed to CSE. In both cases, contact information and other pertinent information was disclosed to the Royal Canadian Mounted Policy (RCMP). As required, CSE notified the OPC in writing prior to these two disclosures.

The third disclosure involved a threat to life situation which was reported to local law enforcement authorities including the RCMP. CSE determined that the disclosure of personal information would clearly benefit the individual to whom the information is related. Given the nature and time-sensitivity involved with this situation, CSE disclosed contact information and other necessary information to the authorities prior to the notification in writing to the OPC.

The last disclosure involved an immediate threat to public safety and life which was reported to law enforcement authorities including the RCMP. CSE disclosed contact and other pertinent information to prevent serious and immediate harm to the public. While this disclosure was reported to the OPC after the fact, as a public interest disclosure, it was later confirmed that the authority to undertake this urgent disclosure was approved under section 46 of the *CSE Act* in parallel with the *Privacy Act*.

Monitoring Compliance

Using our case management software, the ATIP Office continues to produce reports on the time taken to process requests. These reports are shared with our ATIP Coordinator throughout the fiscal year. The ATIP Operations team tracks all requests and reports bi-weekly to the team manager on any issues and/or delays in processing requests. This provides an opportunity for the manager to triage requests or allocate resources, for example, to meet legislated timelines. CSE's Executive Committee (made up of DM and ADM level executives) is also informed of the status of *Privacy Act* requests on an ad-hoc basis.

Like many other government departments, CSE is experiencing a backlog in responding to requests for information. The ATIP Operations team has implemented mechanisms and tools to address this backlog such as the team's bi-weekly tracker for requests for information and access consultations. The ATIP supervisor and manager are briefed weekly on the number of new requests, closed requests, and are alerted to any backlogs by ATIP analysts. This is an opportunity to discuss how best to triage requests and allocate resources as required to meet legislated timelines.

The Privacy Office did not conduct active privacy monitoring during the reporting period.

Privacy breaches and incidents are reported to and managed by the Privacy Office as they occur and are reported to the Chief and Chief Privacy Officer where required.

No (0) material privacy breaches occurred at CSE during the current reporting period of April 1, 2025, to March 31, 2026.

Appendix I: Delegation of Authority

COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

PRIVACY ACT DELEGATION ORDER

The Minister of National Defence, pursuant to section 73 of the *Privacy Act*, hereby designates the persons holding the positions set out below, or the persons occupying on an acting basis those positions, to exercise the powers, duties and functions of the Minister of National Defence as the head of the Communications Security Establishment Canada (CSE), under the provisions of the *Privacy Act* and related regulations set out below for each position.

- Chief, CSE: full authority, except joint authority under paragraph 8(2)(m) (public interest disclosure) with the Deputy Chief, Authorities, Compliance and Transparency

- Deputy Chief, Authorities, Compliance and Transparency: full authority, except joint authority under paragraph 8(2)(m) (public interest disclosure) with the Chief, CSE

- Director General, Review, Transparency, and Information Sharing: full authority, except for paragraph 8(2)(m) (public interest disclosure).

- Director, Transparency and Information Sharing: full authority, except for paragraph 8(2)(m) (public interest disclosure).

- Manager, Transparency and Disclosures: full authority, except for paragraph 8(2)(m) (public interest disclosure).

- Supervisor, Access to Information and Privacy Operations: paragraph 14(a) only when no record exists (notice) and section 15 (extension of time limits).

- Supervisor, Access to Information and Privacy Intake: paragraph 14(a) only when no record exists (notice) and section 15 (extension of time limits).

- Manager, Employee and Organization Wellness: paragraph 8(2)(m) (public interest disclosure) when it is believed that there is a duty to report child abuse under provincial or territorial legislation as part of their official duties; or where it is believed that there is a threat of harm to self or other.

- Supervisor, Counselling and Advisory Program: paragraph 8(2)(m) (public interest disclosure) when it is believed that there is a duty to report child abuse under provincial or territorial legislation as part of their official duties; or where it is believed that there is a threat of harm to self or other.

- Counsellors, Counselling and Advisory Program: paragraph 8(2)(m) (public interest disclosure) when it is believed that there is a duty to report child abuse under provincial or territorial legislation as part of their official duties; or where it is believed that there is a threat of harm to self or other.

This delegation order replaces all previous delegation orders.

Dated at Ottawa this 18 day of March 20 26.

The Honourable David McGuinty, P.C., M.P.
Minister of National Defence