Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Annual Report to Parliament on the Administration of the *Privacy Act* 2024-2025

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 2024-2025 as submitted by the Minister of National Defence.

Canada

Communications Security Establishment | Centre de la sécurité des télécommunications

Table of Contents

Canada

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 twelfth 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 carried out its responsibilities under the *Privacy Act* during the reporting period 1 April 2024 to 31 March 2025.

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 is part of the Transparency and Information Sharing (TIS) group in CSE's Authorities, Compliance and Transparency (ACT) Branch. As noted in the previous annual report,

this new restructuring was part of CSE's strategic goal to uphold the highest standards of compliance, lawfulness, and respect for the privacy of Canadians.

The Access to Information and Privacy Office includes a manager responsible for fifteen (15) full-time positions working in three (3) teams: ATIP Operations, ATIP Intake and Privacy Policy and Governance (PPGO). At the end of the reporting period, the ATIP Operations team consisted of one (1) supervisor and five (5) analysts. The ATIP Intake team consisted of one (1) supervisor, two (2) analysts, one (1) support officer, and one (1) co-op student, while the PPGO team consisted of one (1) supervisor, four (4) analysts and one (1) co-op student.

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 team 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 Unit's ability to respect legislative timelines. CSE ATIP is working towards processing requests more promptly and has taken positive steps to establish efficient workflows while addressing team growth.

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.*

The Privacy Policy and Governance team is responsible for the following activities:

- Supporting Deputy Chief, Authorities, Compliance and Transparency, 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.

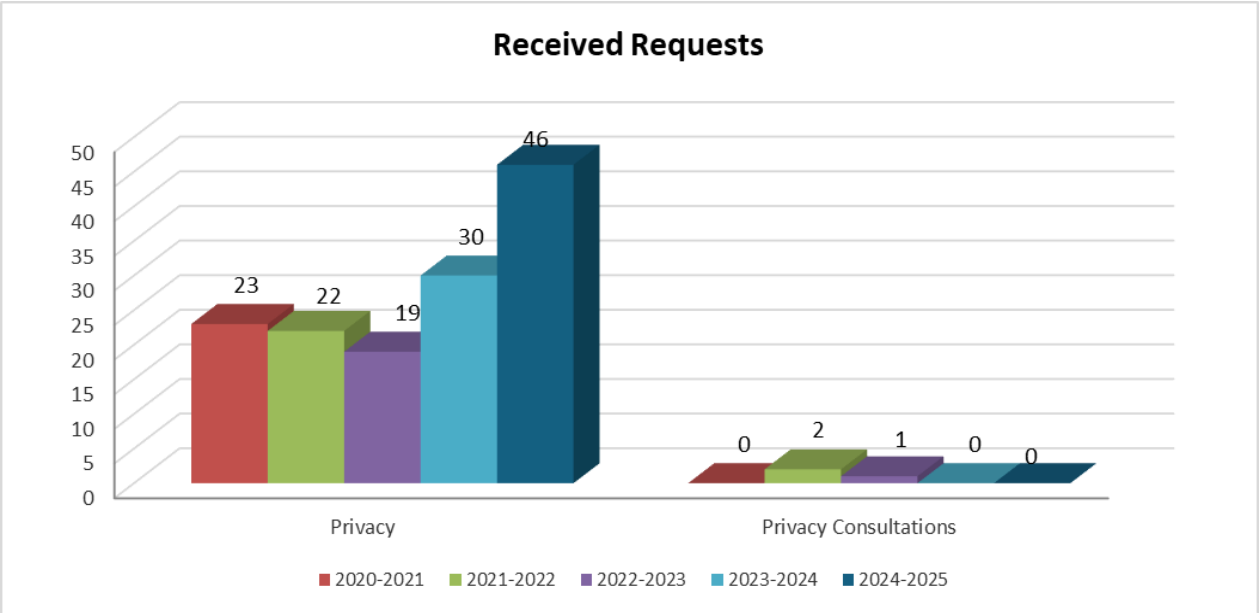
Delegation Order

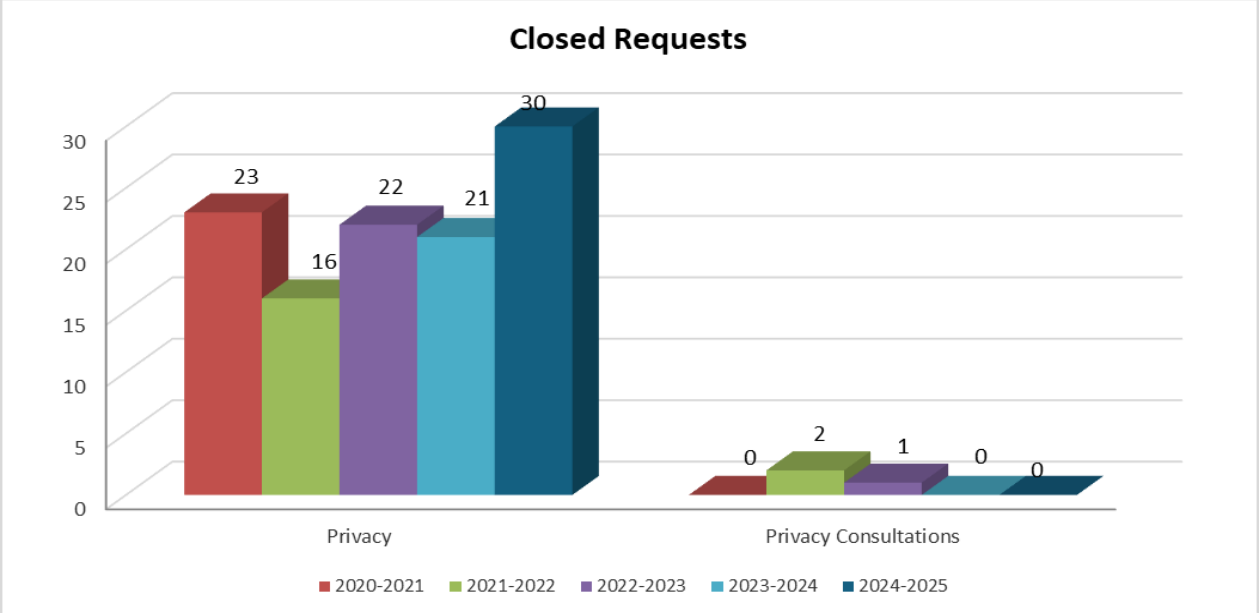
The delegation order in effect at the end of 2024-2025 has been updated from an earlier organizational structure at CSE and a copy can be found in Appendix I of this report. The Minister of National Defence, the Honourable Bill Blair, delegated all authorities under section 73 of the *Privacy Act* to the Chief, CSE, the Deputy Chief, Authorities, Compliance and Transparency, the Director, Transparency and Information Sharing, and to the Manager, Transparency and Disclosures. He also delegated limited authorities to the Supervisor, Access to Information and Privacy Operations and the Supervisor, Privacy Policy and Governance as well as the Manager, Employee and Organization Wellness.

Performance 2024-2025

Number of Formal Requests

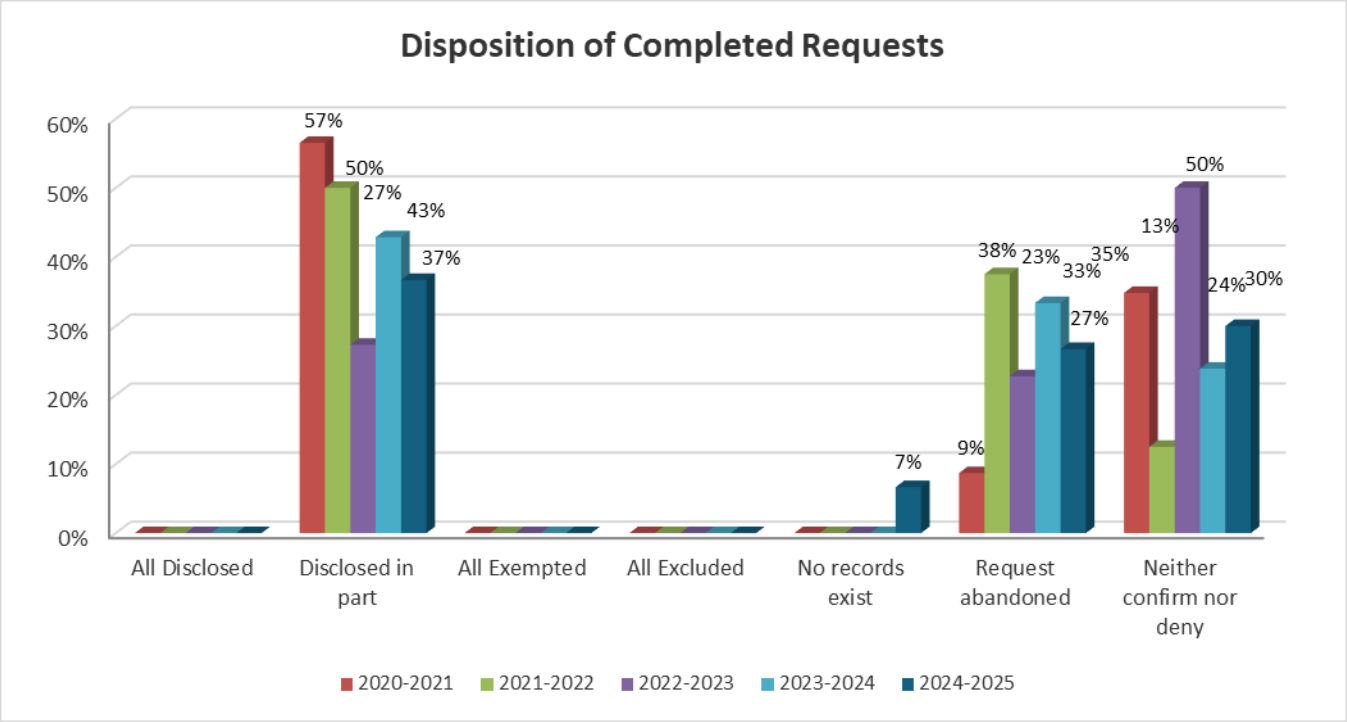
During this reporting period, CSE received forty-six (46) requests under section 12(1) the *Privacy Act*, which is an increase from the previous fiscal year when thirty (30) new requests were received. In addition, fourteen (14) requests outstanding from the previous reporting period were carried over and eighteen (18) from more than one reporting period ago, giving CSE a total of seventy-eight (78) requests to process. By the end of 2024-2025, CSE closed thirty (30) requests and carried forward forty-eight (48) into 2025-2026.





Disposition of Completed Requests

CSE closed 30 requests during this reporting period. Of these, eleven (11) (37%) were disclosed in part, none (0) were disclosed in full and eight (8) (27%) were abandoned by the applicants. Two (2) (7%) requests resulted in no records being found. There were also nine (9) (30%) requests where the existence of records was neither confirmed nor denied, which is a significant increase from five (5) records in 2024-2025. There were no requests which were exempted or excluded in full.



Neither Confirm Nor Deny

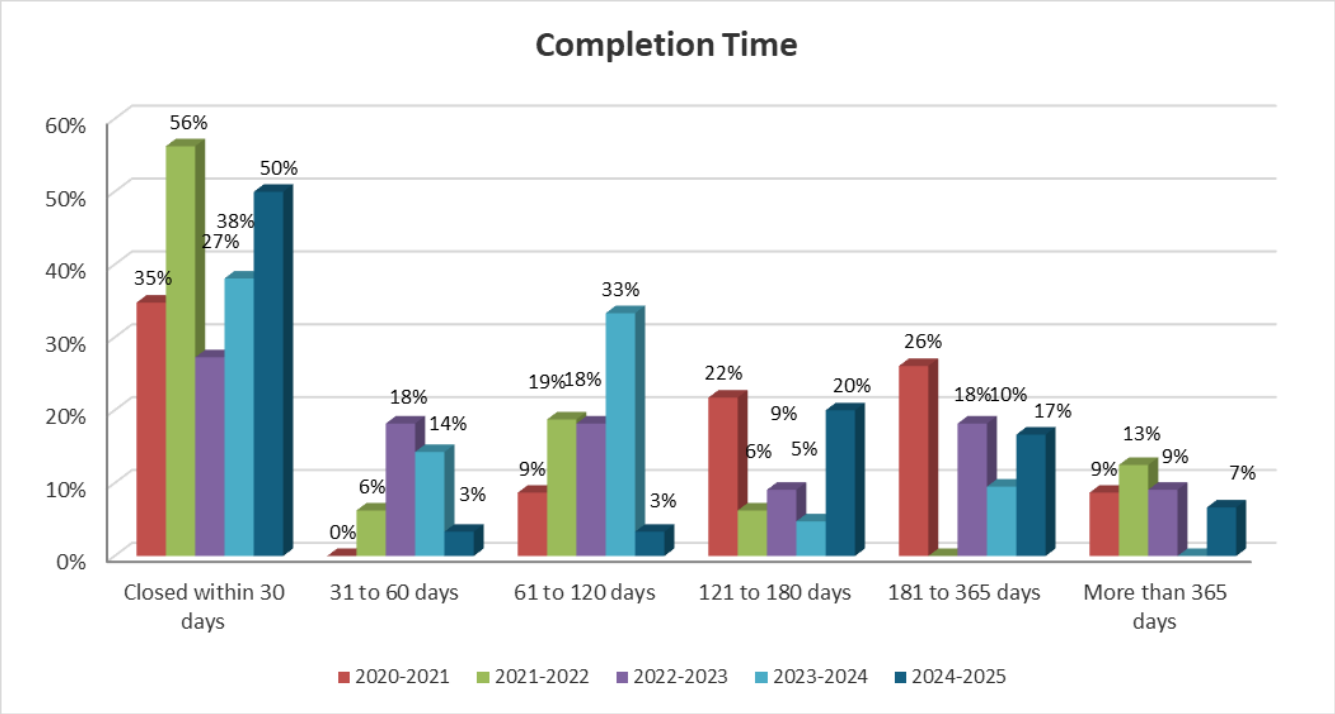
Section 16(2) of the Act indicates that institutions do not have to tell a requester whether personal information exists. Section 16(2) was designed to address situations in which the mere confirmation of a record's existence (or non-existence) would reveal information that could be protected under the 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 nine (9) times during the 2024-2025 fiscal year.

Completion Time

During the 2024-2025 fiscal year, sixteen (16) of the completed requests made under the *Privacy Act* were closed within the legislative timeframe, representing 53% of all completed requests. None of these requests included extensions beyond the initial 30 days. CSE closed fifteen (15) requests within 1-30 days; one (1) between 31 and 60 days; seven (1) between 61 and 120 days; six (6) between 121 and 180 days; five (5) between 181 and 365 days; and two (2) took more than 365 days to process. In general, the requests received during 2024-2025 involved information of a highly sensitive nature resulting in greater complexity in fulfilling them. CSE processed a total of 9,379 pages in 2024-2025 compared to 1,666 pages in 2023-2024. Of the total requests carried over into 2025-2026, twenty-five (25) (52%) were received during the 2024-2025 reporting period.

Open Requests outstanding from previous reporting periods

Reporting period received	Within Legislated timelines	Beyond Legislated timelines	Total
2015-2016 or earlier	0	3	3
2016-2017	0	1	1
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	4	4
2023-2024	0	6	6
2024-2025	9	16	25
Total	**10**	**38**	**48**



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 eleven (11) requests to protect information which could be reasonably expected to be injurious to the defense of Canada. Section 26 was applied in ten (10) 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

One (1) extension, based on Section 15 (a)(ii) of the *Privacy Act* relating to internal consultation, was taken on requests under the *Privacy Act* during the 2024-2025 fiscal year.

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).

CSE received three (3) complaints during fiscal year 2024-2025 and closed three (3) complaints against CSE. CSE provided information to the OPC in relation to all complaints as requested.

One (1) of the complaints received in the current reporting period alleged that CSE had not provided responsive records within the prescribed time periods. The remaining two (2) were complaints alleging that CSE had not appropriately applied exemptions under the PA. CSE made representations to the OPC regarding complaints as requested and will continue to work with the OPC to resolve them in a timely manner. No additional actions were taken on the files in question.

One (1) of the closed complaints was found to be well founded and resolved. The remaining two (2) were closed at the early resolution stage with no findings.

At the end of the reporting period, the OPC had eight (8) 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
2015-2016 or earlier	0
2016-2017	0
2017-2018	0
2018-2019	0
2019-2020	0
2020-2021	0
2021-2022	3
2022-2023	2
2023-2024	1
2024-2025	2
Total	**8**

Education and Training

CSE continues its commitment 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.

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.

In addition to this, the ATIP Office delivered 20 informal briefings and one-on-one training sessions during the reporting period upon request as well as participating in two (2) awareness sessions for co-op students.

In 2024-2025, 398 employees completed the online privacy awareness training module, which is a training program deployed in 2019-2020 that aims to improve the availability of privacy awareness training to CSE employees. All CSE employees are required to complete this training module at the beginning of their career at CSE and then once every two years.

Additional privacy educational initiatives in 2024-2025 included promoting privacy awareness through Privacy Awareness Week (PAW) at CSE from May 27th to 31st, 2024. The theme for the week was "Privacy and Technology: Improving Transparency, Accountability, and Security". Throughout the week, the PPGO shared best practices and various materials and resources with employees to raise awareness of privacy and technology including practical tips for strengthening privacy and security when using technology in the workplace and at home.

In the fall of 2024, PPGO provided training for approximately 50 employees from Corporate Services, Human Resources and Labour Relations management. The training focused on the legislative and policy requirements relevant to each teams' work and provided guidance on the identification and management of a privacy breach.

Collectively, these efforts provided opportunities to showcase privacy across the organization, resulting in a greater number of program managers and stakeholders consulting with CSE's ATIP Operations, ATIP Intake and Privacy Policy and Governance teams. The team's support included guidance on CSE privacy policies, procedures, and best practices for managing personal information.

In addition, 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 privacy policy suite includes a broad-scoped CSE Administrative Privacy Policy which 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. Note that the policy clarifies that privacy awareness training is mandatory for all CSE staff.

In 2024-2025, PPGO updated its Privacy Office Protocol. This Protocol outlines best practices for PPGO personnel when handling personal information for both administrative and non-administrative purposes. It helps ensure that individuals' personal information is handled by PPGO in a manner that reduces privacy risks to those concerned.

PPGO also undertook a review and update of its privacy related standard operating procedures (SOPs) in 2024-2025 including its Privacy Breach SOP, to ensure it reflected the latest updates in keeping with OPC and TBS privacy policy and guidance.

The ATIP Operations team continues to seek new opportunities to improve the efficiency and timeliness of processing requests. In fiscal year 2024-2025, this included improvements to the *ATIP Manual* outlining how to respond to access requests, access consultations, privacy requests and privacy consultations; and flow charts illustrating the ATIP Operations team's processes.

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 Operations team 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 the time our team can devote to access and privacy requests. This time is not represented in the statistical reporting, but accounts for approximately 1.77 FTE for the reporting period, a decrease from 2 in 2023-2024.

Initiatives and Projects to Improve Privacy

During the 2024-2025 reporting period the PPGO initiated the development of a risk assessment tool to standardize the assessment of privacy risks associated with a program or activity area to determine its overall risk level.

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 37 requests via this service, representing approximately 80% of the total requests received. 13% of requests were received by email and the remaining 7% through regular mail.

Material Privacy Breaches

One (1) material privacy breach was reported to the Office of the Privacy Commissioner and the Treasury Board of Canada Secretariat related to the reporting period of April 1, 2024, to March 31, 2025. The breach involved the disclosure of sensitive personal information by CSE to an employee's medical doctor as part of a fit to work assessment. While the disclosure of some of the personal information may have been warranted for the purposes of the assessment, not all personal information warranted disclosure.

In response to the breach, PPGO delivered hybrid privacy breach training to approximately 50 employees from Corporate Services, Human Resources and Labour Relations management. This training covered HR's Privacy Act obligations as well as related TBS policy instruments. In addition, as a mitigation measure to promote greater awareness on privacy obligations, the PPGO worked with the responsible areas to develop and implement privacy informed standard operating procedures.

Privacy Impact Assessments

During the 2024-2025 reporting period, CSE did not complete any Privacy Impact Assessments (PIA).

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.

CSE made two public interest disclosures (PID) in the 2024-2025 reporting period. Both cases involved child exploitation material uncovered by or disclosed to CSE and both were disclosed to the Royal Canadian Mounted Police (RCMP). In the first case, CSE disclosed social media group names and in the second, CSE disclosed an email address. As required, CSE notified the OPC prior to both disclosures.

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, in order 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.

One (1) material privacy breach occurred at CSE during the related reporting period of April 1, 2024, to March 31, 2025. As part of PPGO's obligations, all breaches were reported to the Office of the Privacy Commissioner and the Treasury Board of Canada Secretariat.

Appendix I: Delegation of Authority

COMMUNICATIONS SECURITY ESTABLISHMENT

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, under the provisions of the *Privacy Act* and related regulations set out below for each position.

- Chief, Communications Security Establishment: 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, Communications Security Establishment
- 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: subsection 8(2) (use and disclosure) except for paragraph 8(2)(m) (public interest disclosure), paragraph 14(a) only when no record exists (notice) and section 15 (extension of time limits).
- Supervisor, Privacy, Policy and Governance: subsection 8(2) (use and disclosure) except for paragraph 8(2)(m) (public interest disclosure).
- 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.

This delegation order replaces all previous delegation orders.

Dated at Ottawa this 20 day of March 2024.

The Honourable Bill Blair, P.C., C.O.M., M.P.
Minister of National Defence