

Report on the Administration of the Freedom of Information and Protection of Privacy Act

Tabled in the Legislative Assembly by the Honourable Michael de Jong, Q.C., on
Tuesday, June 27, 2017

REPORT ON THE ADMINISTRATION OF THE
FREEDOM OF INFORMATION AND
PROTECTION OF PRIVACY ACT

2015/2016 & 2016/2017

Contents

- Message from the Minister 1**
- Introduction..... 1**
 - Improved Information Stewardship through a New, Integrated Approach..... 1
 - Accomplishments..... 3
 - Key Challenges 4
 - Looking Ahead 4
- Report on Performance: Access to Information 5**
 - Understanding FOI Request Volumes, Complexity, and Size..... 5
 - Renewing our Focus on Service Culture and Transparency 8
 - Improving FOI Response Timeliness..... 10
 - Focusing on Proactive Disclosure..... 12
 - Improving Productivity and Reducing the Backlog 14
 - Understanding FOI Fees and Costs..... 16
- Report on Performance: Protection of Privacy 17**
 - A Continuing Commitment to a Culture of Privacy Protection..... 17
 - Conducting Privacy Impact Assessments..... 19
 - Personal Information Directory 19
 - Investigating Privacy Incidents and Complaints..... 20
- Looking Ahead: Continuing to Lead the Way in Access to Information and Protection of Privacy 24**

Message from the Minister

In December 2015, responsibility for access to information and privacy, as well as for records management and other information management policy and governance was transferred to the Ministry of Finance, where it was integrated and aligned under the leadership of the Province's first Chief Records Officer. The strategic realignment and integration of these disciplines offered us the opportunity to streamline and enhance policy controls, training and compliance across the information management domains.

As an organization, we set ourselves a strategic goal: to increase accountability, transparency, and public trust in government employees as effective stewards of the valuable information resources in our care. Since government's last report on the administration of the *Freedom of Information and Protection of Privacy Act*, we have taken many steps to enhance our policies and procedures to meet that commitment.

As a direct result of our renewed commitments to accountability and transparency, we now proactively disclose more information than ever before. Since May 2016, more than 2,500 proactive disclosures have been made under eight new Ministerial Directives — the first of their kind. We launched an improved Open Information website, making it easier than ever for British Columbians to find the records they seek, either by downloading previously released material or requesting documents through Freedom of Information (FOI).

We also made an important commitment to a revitalized service culture in FOI. While the *Freedom of Information and Protection of Privacy Act* sets a legal obligation to assist applicants and to respond openly, accurately, completely and without delay to a request, we have made a commitment to go beyond the letter of the law. We see responding to an FOI request as an important public service. To this end, a new FOI search process was developed. Records searches in Ministers' offices are now being coordinated by specially trained, senior public servants. Because of changes in the way we clarify requests with applicants and redirect requests to other ministries or government bodies likelier to have responsive records, we have continued to reduce the number of "no responsive records" responses provided to applicants.

We remain committed to enhancing the culture of privacy protection across government. A new Privacy Management and Accountability Policy sets the legislative and policy direction for all ministries. All ministries now have a dedicated Privacy Officer, and a cross-government privacy community of practice provides the opportunity for all interested staff to learn about emerging issues and trends. By March 31, 2017, updated, integrated and comprehensive training for senior officials had been completed by all Cabinet Ministers, their staff and senior executives across government. New, mandatory training has been completed by over 25,000 employees, further improving awareness of information management responsibilities — with a strong focus on information stewardship, personal information protection and access to information.

Good information management practice involves valuing information as an important and valuable asset and diligently protecting it throughout its lifecycle. Successful management of information is the foundation of good governance, access rights, and the protection of privacy.

I want to extend my thanks to all public servants for their diligence in providing access to information and protecting the privacy rights of British Columbians.

Introduction

Improved Information Stewardship through a New, Integrated Approach

In December 2015, responsibility for government's information management practices, policies and legislation was transferred to the Ministry of Finance from the Ministry of Technology, Innovation and Citizens' Services. At that time, the information management domains (privacy, access to information, records management and elements of information security) were integrated in a new division, the Corporate Information and Records Management Office (CIRMO), under the senior leadership of government's first Chief Records Officer (CRO).

This was in response to former Information and Privacy commissioner David Loukidelis' report on measures government could implement to ensure compliance with information management requirements. Government has accepted the recommendations in that report and, to-date, work to address 20 of Mr. Loukidelis' 27 recommendations is complete or substantially complete. Government also made a commitment to go above and beyond those recommendations, where possible. Recent efforts to reinvigorate proactive disclosure are one example of the ways in which government is meeting this commitment.

1

This strategic realignment and integration of government's corporate information management programs and services enables CIRMO to deliver seamless oversight, guidance and training across the information management domains, with an emphasis on the importance of privacy management and access to information practices. An integrated and holistic approach is essential for fostering public trust in government's ability to appropriately manage government information, especially personal information, throughout its entire lifecycle, from creation to disposal or permanent archival retention.

An important part of that mandate is the administration of the *Freedom of Information and Protection of Privacy Act* (FOIPPA). In this capacity, CIRMO provides comprehensive access and privacy leadership, advice, education and support to public bodies. CIRMO also manages the legislative amendment process for FOIPPA, assesses the potential privacy and access impacts of government activities, and responds to information incidents (including privacy incidents).

CIRMO also plays a lead role in ensuring that all ministries meet their legislated responsibilities in providing access to information under FOIPPA. This includes assisting applicants throughout the Freedom of Information (FOI) request process as well as working with ministries to ensure consistency and a high standard of service excellence in FOI. CIRMO also has responsibility for administering a comprehensive proactive disclosure program that requires the regular, online disclosure of several categories of government information, without the need for an FOI request.

The Province's first Chief Records Officer was designated in December 2015, with a mandate to oversee all corporate information management functions, including records management, privacy, access to information and elements of information security.

The CRO has a broad mandate that also includes oversight over other information management legislation, such as the Information Management Act and Personal Information Protection Act, as well as policies, procedures and operations related to information management.

The Information and Privacy Commissioner, an independent Officer of the Legislature, conducts reviews and investigations to ensure compliance with FOIPPA, mediates disputes and comments on potential FOI and privacy implications of proposed initiatives.

2015/16 & 2016/17 By the Numbers



Accomplishments

Improving Accountability and Transparency

- The Province's first Chief Records Officer was designated and all corporate information management programs and services were integrated into a single division in the Ministry of Finance.
- For the first time since the relevant provision was enacted in 2011, the Minister responsible for the Act exercised his legislative authority to issue eight directives requiring ministries to proactively disclose categories of records – without the need for an FOI request. To date, over 2,500 disclosures have been made under these directives.
- Introduced secondary severing of new FOI request response packages to remove copyright material, making these packages eligible for subsequent publication online on the Open Information website.
- Launched an enhanced Open Information website, providing enhanced search functionality and improved accessibility.
- Published a total of 263 datasets in the BC Data Catalogue.

Enhancing our Culture of Privacy

- Implemented a new corporate Privacy Management and Accountability Policy (PMAP) and established a Ministry Privacy Officer role for every ministry.
- As part of a comprehensive information management training initiative, delivered:
 - tailored privacy and access to information training to all Ministers, Ministerial Office staff, and designated FOI Coordinators, as well as Parliamentary Secretaries and Chiefs of Staff;
 - tailored mandatory privacy training to more than 14,000 service providers; and
 - new, mandatory and comprehensive information management training to over 25,000 government employees.
- CIRMO reviewed 687 Privacy Impact Assessments (PIAs) in the 2015/2016 fiscal year and 719 PIAs in the 2016/2017 fiscal year.

Providing Service Excellence in FOI

- Introduced a new service approach to reinforce that the duty to assist FOI applicants is an important public service and not merely a legislated obligation.
- Established FOI Coordinators in Ministers' offices to enhance and strengthen the FOI process.
- Introduced new file management and severing software to streamline and expedite the administration of Freedom of Information requests.
- Reduced the proportion of "no responsive records" responses by 5 percentage points from 17% in 2015/2016 to 12% in 2016/2017.

A note on the time period covered in this report:

This report covers the time period spanning both the 2015/2016 fiscal year (April 1, 2015 to March 31, 2016) and the 2016/2017 fiscal year (April 1, 2016 to March 31, 2017). The report provides comparisons to the 2014/2015 reporting year.

Key Challenges

Challenges in Access to Information

- B.C. receives more FOI requests per year than Alberta, Saskatchewan and Manitoba combined.
- FOI requests continue to grow in number, size and complexity.
- While strides have been made in reducing the number of overdue requests, there is still a backlog, caused by significant volume increases in requests over the past six years. This backlog affects timeliness and workload pressures.
- Major events of public interest generate significant volumes of FOI requests and pose unique challenges related to the size, scope and complexity of these requests.
- A small number of high-volume users of the FOI system generate significant workload pressures on the system, impacting government's ability to provide client-centered services to the thousands of others who are making requests for information. In 2016/2017, two requestors were responsible for 29% of all general requests.¹ One of these two requestors generated 65% of all media-related FOI requests.

Challenges in Protection of Privacy

- Evolving technological innovations, research practices and even trade agreements with provisions related to the cross-border flow of data require a nimble and diligent approach to privacy protection.
- An increasingly mobile and technologically-enabled workforce introduces additional potential privacy risks. Legislation, policy and practice must keep pace to ensure B.C. remains a leader in this area.
- As ministries develop new initiatives to better meet the evolving needs of their clients, there is a need to streamline Privacy Impact Assessment processes while maintaining the comprehensive nature of the reviews. This will help protect personal information while permitting ministries to effectively carry out their mandated functions.

4

Looking Ahead

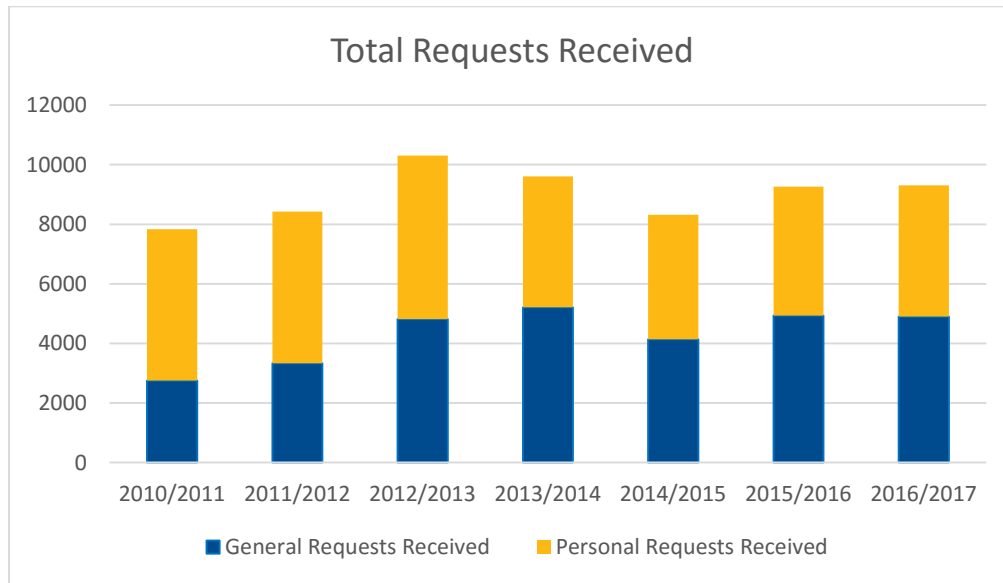
- Government is exploring new technologies to make responding to FOI requests and protecting privacy more efficient and secure.
- We will continue to focus on proactive disclosure of information.
- Government is taking an integrated approach to awareness, education, policies, procedures, and practices across the information management domains.
- We have a strong culture of privacy protection and freedom of information, championed by committed senior leaders and supported by an information management discipline that values and protects its information assets.
- We have committed to accountability and transparency and an enhanced service culture in FOI, supported by strong senior executive leadership across the organization.
- Government continues to adapt its approach to new innovations and developments in technology and citizen service.

¹ A "general" FOI request is a request for records of a non-personal nature that potentially could be released, in whole or in part, to anyone. This is distinct from "personal" requests, made by an individual for their own information.

Report on Performance: Access to Information

Understanding FOI Request Volumes, Complexity, and Size

The Volume of FOI Requests has Generally Increased over Time



5

Between 2010/2011 and 2012/2013, the number of FOI requests received by government steadily increased, before decreasing somewhat in 2014/2015. In the timeframe covered by this report, the number of requests received has levelled off at a rate that is approximately 19% higher than the 2010/2011 levels.

In the 2015/2016 fiscal year, the B.C. government received 4,932 general and 4,329 personal requests — a total of 9,261 FOI requests. Comparing the 2015/2016 fiscal year to the prior fiscal year, this represents a 19% increase in general requests and a 4% increase in personal requests. There was an 11% increase in the total number of requests received. In the 2016/2017 fiscal year, government received a total of 9,310 requests — 4,905 general requests and 4,405 personal requests. These volumes are generally consistent with the number of requests received in 2015/2016.

While the numbers of requests received and closed annually provide important insights into the demands on and operations of the FOI system, they cannot be used as the sole measure of the volume of work. These statistics alone do not reflect the size or complexity of the requests, and should be interpreted in context.

The Scope and Complexity of FOI Requests has Increased over Time

There are several notable, emerging trends in the way the FOI system is being used. More than ever before, applicants are requesting a wide array of non-traditional records including e-mail message tracking logs, mobile device app inventories and all emails sent from the accounts of specified government officials. Responding to these new types of requests in a manner consistent with FOIPPA requires substantial time and attention to ensure the appropriate balance is maintained between public access and the protection of personal and sensitive information.

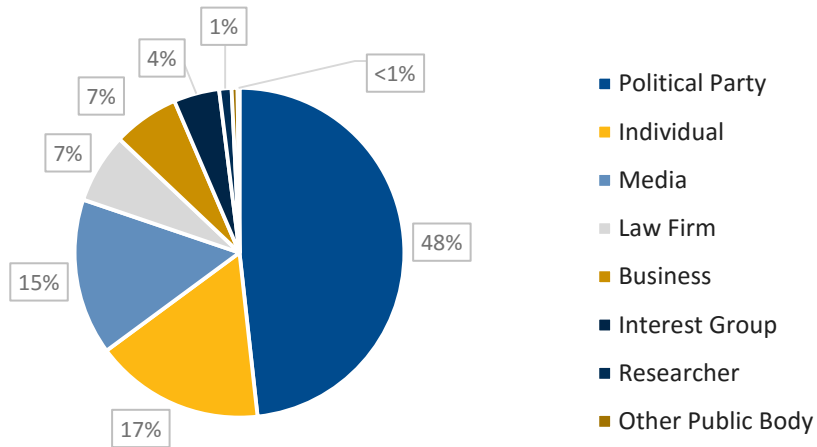
Applicants are also interested in information about large and complex government programs or current events. This type of request can present unique challenges, including reviewing considerable volumes of responsive records, complex consultations, and added workloads for program staff who are concurrently managing both requests for information and the emergent issue itself. Records related to these types of requests are often also still in active development and use by program area staff, which can mean carrying out searches in several locations.

Another factor affecting the complexity of responding to requests is the increase in cross-government requests². The number of cross-government requests has more than doubled since 2010/2011. These requests require additional levels of administrative involvement to ensure that all ministries consistently interpret and cross-reference the requests.

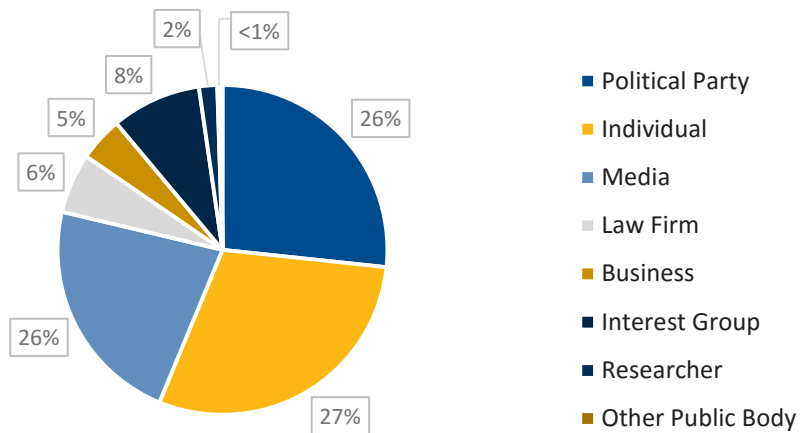
Additionally, voluminous requests have continued to place significant demands on the system.

² A cross-government request is one that is directed to four or more Ministries.

General FOI Requests by Applicant Type
2015/2016



General FOI Requests by Applicant Type
2016/2017



Renewing our Focus on Service Culture and Transparency

Improving the FOI Service Experience for Applicants

The “duty to assist” is a positive legislated duty to make every reasonable effort to respond openly, accurately, completely and without delay to a request for access to information under FOIPPA. In government’s view, the “duty to assist” goes beyond meeting the letter of the law and involves providing an excellent service experience to each applicant.

In December 2015, government received the Loukidelis report and accepted the recommendations it contained. In March 2016, government made a public commitment in the Legislature to improvements in this area, including enhanced accountability and oversight and revised policies and procedures to ensure:

- Clarification of requests is done in a manner that assists the applicant to access the information they want in a timely way, and where appropriate, by an employee with knowledge of the ministry’s records and business;
- Searches for responsive records are thorough and well-documented;
- Better explanations and information are provided to applicants about why no records may have been located in response to a request;
- A designated career public servant is responsible for overseeing requests in Ministers’ offices; and
- All staff are trained and have a clear understanding of their roles and responsibilities.

Designated FOI Coordinators have now been established in all Ministers’ offices. New, mandatory training is also in place for all staff. Staff in Ministers’ offices have completed a tailored training program, which is consistent with and builds upon corporate information management requirements.

8

CIRMO continues to work with ministries to clarify requests in the best interests of the applicant, to transfer requests where appropriate, and to provide information and explanations where no records are located.

Taking Meaningful Action to Reduce the Number of “No Responsive Records” Responses

Since 2013, when the Information and Privacy Commissioner released a report on the issue, government has been successful in significantly reducing the number of “no responsive records” responses.

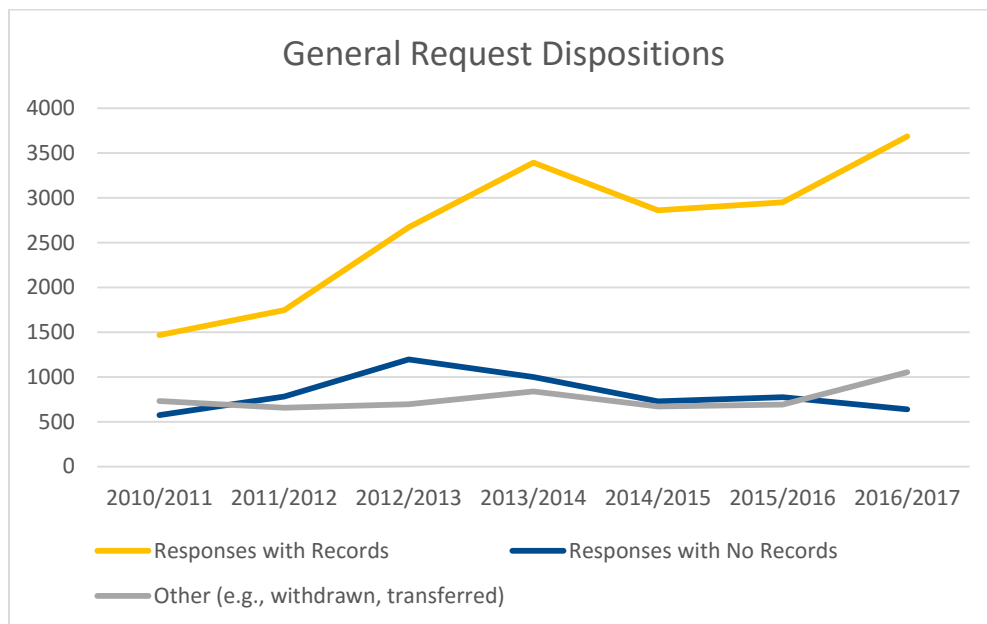
In the time period covered by this report, a new training and education program has been implemented with a focus on redefining and redirecting requests when there would otherwise be no records.

In 2013, the Information and Privacy Commissioner issued a report on the increase in the proportion of general FOI requests that had resulted in no responsive records being located — at that time, the report noted that 25% of general requests had this outcome. In the years following that report, government has intensified its efforts to reduce the proportion of responses to general FOI requests where an applicant is provided with a response indicating there are no responsive records.

In 2015/2016 the proportion of “no responsive records” responses was 17% of general requests. By the end of the 2016/2017 fiscal year, the proportion of “no responsive records” responses decreased significantly to 12% of general requests closed in this year. This represents a 13 percentage point reduction in the proportion of “no responsive records” responses since the 2013 report was published.

The improvements in 2015/2016 and particularly in 2016/2017 are attributable to government’s recent commitment to service excellence in FOI request processing, including a commitment to work with applicants to direct their requests to another ministry or public body more likely to hold the records, and to ensuring that requests are interpreted in a manner that meets the needs of the applicant.

Updated training is also focused on encouraging staff to provide better explanations in cases where no records are located. This helps applicants in understanding why the records they are requesting would not typically be held by the office to which they directed their request.



Improving FOI Response Timeliness

Maintaining Overall On-Time Performance

On-time performance — which measures whether a request is closed within the timelines defined in FOIPPA³ — remains a critical priority for government. Updates on corporate FOI performance are posted publicly in the [BC Data Catalogue](#) on a quarterly basis.

Fiscal Year	General Requests Received	General Requests Closed	General Requests % On Time	Personal Requests Received	Personal Requests Closed	Personal Requests % On Time	Overall % On Time ⁴
2010/2011	2,756	2,774	91	5,073	5,165	95	93
2011/2012	3,329	3,182	86	5,094	5,030	93	90
2012/2013	4,819	4,566	85	5,487	4,958	89	87
2013/2014	5,216	5,235	78	4,395	4,597	69	74
2014/2015	4,141	4,262	81	4,176	4,115	76	79
2015/2016	4,932	4,415	72	4,329	4,394	76	74
2016/2017	4,905	5,380	80	4,405	4,477	81	80

In the 2015/2016 fiscal year, overall on-time performance decreased by five percentage points compared to the prior year. Although on-time performance for personal requests remained unchanged at 76%, the overall decrease in this measure was attributable to general requests, where performance declined from 81% to 72%.

10

Performance on this measure improved in the 2016/2017 fiscal year, with overall on-time performance at 80%.

Breaking this measure down to examine performance at the level of request types offers additional insight. In 2016/2017, on-time performance for general requests improved over the previous year by eight percentage points (to 80%), while performance for personal requests increased five percentage points (to 81%).

On average, in the 2016/2017 fiscal year, requests were processed within 46 business days of being received by a ministry. This includes cases where an extension had been taken to allow the ministry to process the request within 60 or more business days.

Government continues to make strides to improve its timeliness rate, including undertaking business process reviews and continuous improvements and making investments in enhanced technology. These initiatives are detailed below. However, consistently high volumes of requests, greater complexity of requests and a focus on reducing the backlog of overdue requests can impact on-time performance and the overall average number of business days request may remain overdue before they are closed.

³ A public body must respond not later than 30 business days after receiving a request, unless the time limit is extended under one of the limited circumstances set out in section 10 of the Act (or unless the request is transferred to another public body for response).

⁴ "Overall Percent On Time" is determined by taking the weighted average of General Percent On Time and Personal Percent On Time.

Improving Performance at the Ministry Level

Improvements to government's overall performance are the result of the collaborative effort of all ministries, and while individual ministry results will fluctuate over time, there is a positive trend toward increased timeliness, with some ministries achieving substantial improvements. More than half of all ministries have seen an increase in overall timeliness in 2016/2017 compared to 2015/2016. Notably, the Ministry of Aboriginal Relations and Reconciliation increased its performance by 25 percentage points. CIRMO continues to work with ministries to provide additional training on best practices, and to reallocate staff resources as available. As part of a commitment to continuous improvement, ministries and IAO work together to understand what approaches are working well, and share those best practices across government.

Focusing on Proactive Disclosure

Establishing New Categories of Records for Disclosure

British Columbia is a leader in transparency and openness. A robust system is in place to support the proactive disclosure of information.

In 2016/2017, government introduced a new proactive disclosure initiative to publish records of interest to the public without the need for formal FOI requests. To support this initiative, the Minister of Finance issued a series of Ministerial Directives, which established new categories of information for mandatory, regular release that had previously been the subject of public interest and/or access requests. This includes:

- Ministers' receipted travel expenses;
- Calendars of Ministers, Deputy Ministers and Associate Deputy Ministers;
- Summaries of directly-awarded contracts, contracts with values or amendments of \$10,000 or more and alternative service delivery contracts administered by the Strategic Partnerships Office;
- Summaries of community gaming grants awarded; and
- Summaries of open and closed FOI requests.

Since May 2016, over 2,500 proactive disclosures have been made under these directives. Among these, over 1,000 calendars, summaries of directly-awarded contracts, summaries of community gaming grants awarded, travel expense summaries, and summaries of open and closed FOI requests and over 1,500 response packages for general FOI requests have been proactively disclosed.

Efforts to expand this initiative continue, with new reporting on summaries of some types of contracts to commence in the 2017/2018 fiscal year. CIRMO continues to engage with ministries to identify new categories of information for disclosure.

For the first time since the legislative authority was introduced in 2011, the Minister responsible for the Act issued eight Ministerial Directives in 2016 requiring the regular, online disclosure of several categories of government information.

12

Enhancing the Open Information Website

To improve public access to these and other records, in May 2016 government also launched an enhanced [Open Information](#) website, offering enhanced search functionality and improved accessibility, for mobile devices and people with disabilities.

Expanding the Disclosure of FOI Response Packages

In the past, when an FOI request response package contained material subject to copyright, in order to protect the copyright material in accordance with federal copyright law, the entire package was not proactively posted to the Open Information website (though most other general request response packages are posted). In 2016/2017, government implemented a secondary severing procedure to enable FOI response packages that contain copyrighted material to be published to the Open Information website without the copyrighted material⁵. This change in process is expected to result in a 10% increase in the number of FOI response packages published to the Open Information website annually.

⁵ Packages containing the copyrighted information remain available upon request.

Enhanced Data Assets at DataBC

The [BC Data Catalogue](#) attracts more than 11,500 visitors per month, who download more than 150,000 datasets annually. To improve public access to data, in the 2015/2016 fiscal year 70 new datasets were published in the BC Data Catalogue, of which 30 were released under the Open Government Licence. In the 2016/2017 fiscal year, 193 new datasets were published in the BC Data Catalogue, of which 63 were released under the Open Government License.

These releases included data related to compensation, property transfer tax and Consolidated Revenue fund payments. Other important data releases included:

- Land Ownership ParcelMap BC data;
- Geographic datasets that support resource development and exploration;
- Data to support emergency response; and
- Data related to accurate location of government services, including aboriginal business listings and Francophone services.

DataBC continues to make significant improvements to its online web presence and now offers an enhanced BC Data Catalogue where users can discover and access government data assets. The catalogue has added capabilities to showcase data visualizations. In 2016, DataBC launched the new BC Map Hub service as another way for citizens to leverage government geographic datasets for application development.

DataBC now provides access to government Application Programming Interface (API) services. APIs provide web accessible methods and tools for building software applications. Users who discover APIs in the BC Data Catalogue can now explore and experiment with them through the Open API Console.

Improving Productivity and Reducing the Backlog

Undertaking Business Process Reviews and Continuous Improvements

CIRMO processed more than 1.8 million pages of records in response to FOI requests in the 2016/2017 fiscal year.

This equates to roughly 7,100 pages every working day.

This is in addition to proactive disclosures of such things as calendars, travel expenses and contract information.

A key strategic focus for CIRMO and its ministry partners is on improving overall productivity in the information access system. This includes both FOI requests and proactive disclosures of information administered through CIRMO.

Over both the 2015/2016 and the 2016/2017 fiscal years, business process reviews, including formal “Lean” projects and other staff-led continuous improvements, have streamlined administrative workloads.

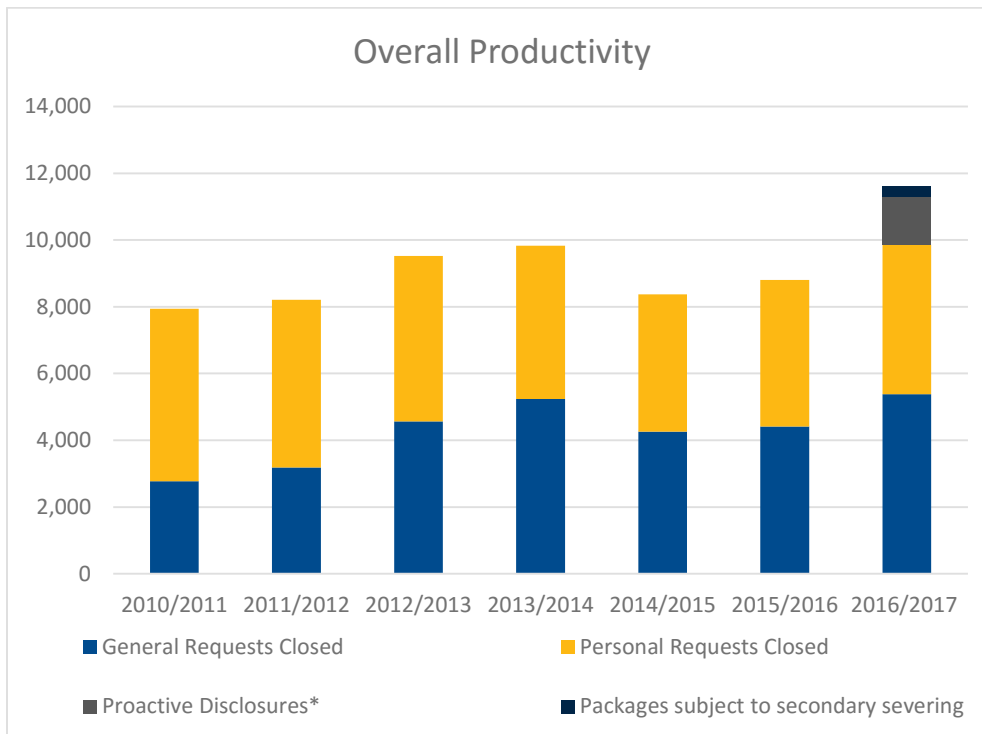
In 2015/2016, government implemented new, end-to-end, FOI software that is capable of creating efficiencies in case management, redactions and the secure release of records. Government is continuing to explore new technologies that assist with de-duplication and records organization, which could potentially provide significant benefits, particularly when used to process large-volume requests.

Improving Productivity

As part of a broader investment of \$3 million to enhance corporate information management services, government allocated CIRMO an additional \$1.5 million in funding in 2016/2017, dedicated to increasing front-line staffing capacity in access to information. This was in direct response to the continuing increases in the resources required to respond to increasingly large and complex FOI requests. A full staff complement and less turnover than in previous years, combined with an influx of new funding, provides the stability necessary to deliver high quality FOI services.

As a result of the targeted improvement strategies described above, by the end of the 2016/2017 fiscal year, overall FOI productivity increased by 12% compared to the prior year. There was a 22% improvement in productivity in processing general requests for this time period. In addition to administering the FOI request process, CIRMO also has a key role in coordinating proactive disclosures. Taking into account both FOI requests and proactive disclosures, productivity across both streams increased by 24% in the 2016/2017 fiscal year. As a result of the new secondary severing procedure to remove copyright material, IAO also processed about 300 FOI response packages proactively that would not previously have been disclosed publically⁶.

⁶ See the section of this report titled “Expanding the Disclosure of FOI Response Packages.”



*Proactive disclosures previously released and reported as FOI requests. This does not include FOI response packages disclosed under Directive 02-2016, which are included in General and Personal Requests Closed.

Reducing the Backlog

The significant change in the volume, size and complexity of requests over the past six years has led to an accumulation of overdue requests. This backlog results in additional workload and resource pressures, which in turn have a further impact on on-time performance for new requests.

Although 4,905 general requests were received in the 2016/2017 fiscal year, 5,380 were closed. This includes a number of requests that had been received in previous years and were overdue.

Understanding FOI Fees and Costs

The estimated cost to government of the FOI program is \$24 million annually. FOIPPA provides for the recovery of some fees for FOI services.

In 2015/2016, the Province recovered \$61,000 in fees from the 8,809 FOI requests processed. In 2016/2017, the Province recovered \$62,000 in fees from 9,857 FOI requests.

While the vast majority of responses to FOI requests are provided without payment, fees are one way that government can recover some of the costs associated with large or broadly worded requests. The prospect of fees also encourages requestors to clarify their requests in order to target records of importance to the subject they are interested in.

Only 0.3% of the approximately \$24M total costs dedicated to supporting the FOI process are recovered through fees from applicants.

Although an average request costs \$2,410 to process, only about \$6 in fees is passed on to an applicant, on average.

FOI Requests	2012/2013	2013/2014	2014/2015	2015/2016	2016/2017
Total Number of Requests	9,534	9,832	8,377	8,809	9,857
Number with Fees Paid	144	177	158	176	188
Percentage with Fees Paid	2%	2%	2%	2%	2%
Total Fees Paid	\$58,000	\$78,000	\$50,000	\$61,000	\$62,000
Fees Averaged Across All Requests	\$6	\$8	\$6	\$7	\$6
Average Cost of Processing an FOI Request	\$2,075	\$2,010	\$2,358	\$2,243	\$2,410

Report on Performance: Protection of Privacy

A Continuing Commitment to a Culture of Privacy Protection

Implementing the Privacy Management and Accountability Policy and Establishing a Ministry Privacy Officer for Every Ministry

The Privacy Management and Accountability Policy (PMAP), implemented in 2015/2016, is government's corporate policy for privacy management. The PMAP strengthens government's ability to protect personal information by clearly articulating key privacy policies and accountabilities for privacy management in government. The policy sets the framework under which ministries must operate in order to ensure their compliance with the privacy requirements of FOIPPA.

The policy sets out clear roles and responsibilities, identifies the mandatory assessment tools and agreements that ministries must use, the policies and procedures that must be followed, and requirements for reporting and audit.

The policy requires each Deputy Minister to designate a "Ministry Privacy Officer" responsible for privacy and the implementation of the policy within their ministry. The Ministry Privacy Officer has a number of specific accountabilities under the policy, including acting as a resource for employees in their ministry and, where necessary, developing and issuing ministry-specific privacy policies, in collaboration with CIRMO, to augment the PMAP.

17

Enhancing Privacy Awareness and Education

Under the new Privacy Management and Accountability Policy, all government employees are required to complete role-based training appropriate to their jobs and the personal information they handle. This includes completion of a mandatory online module for all staff and, depending on an individual's role, may include other courses.

New, comprehensive information management training was launched in early 2017. This new training program takes a holistic approach to information management education that encompasses privacy, access, records management and elements of information security. Training is mandatory and employees are required to refresh their knowledge every two years.

Over 39,500 staff and contractors have completed new, comprehensive and tailored privacy training programs.

This course was completed by 25,117 employees between February 1 and March 31, 2017. This represents a 94% completion rate among active members of the BC Public Service. Ongoing expansion of the training initiative, including onboarding of new staff, will continue in 2017/2018.

In addition to the mandatory module, a variety of other privacy training is available from CIRMO, including on topics such as how to complete privacy impact assessments, the basics of information sharing agreements, and how to manage Freedom of Information requests. CIRMO also provides targeted training to address issues arising from privacy incidents.

In addition, a new, tailored privacy training module for service providers was rolled out in 2016. To date, 14,398 service providers have taken this training.

Providing Expert Advice

CIRMO's [Privacy and Access Helpline](#) is an important resource for ministry and other public sector employees as well as members of the public.

During the 2015/2016 fiscal year, the helpline received 1,173 inquiries via phone or email from public sector staff or members of the public. In the 2016/2017 fiscal year, the helpline received 1,375 inquiries. In addition to these calls, CIRMO received approximately 200 calls from Ministry Privacy Officers.

Fiscal Year	Number of Inquiries Received
2011/2012	1,250
2012/2013	1,400
2013/2014	1,250
2014/2015	1,333
2015/2016	1,173
2016/2017	1,375

CIRMO also regularly provides support and guidance with respect to complex and high-profile government initiatives, ministry policies, data releases, technological advances, and contracts impacting the management of personal information, to ensure compliance with privacy legislation.

Conducting Privacy Impact Assessments

A Privacy Impact Assessment (PIA) evaluates how a current or proposed enactment, system, project, program or activity will impact the personal privacy of the individuals whose information is collected, used, or disclosed. It is just one of the ways that government ensures that new ways of doing business are compliant with the provisions of FOIPPA and that any risks to personal information are identified and mitigated.

There has been a marked increase in the number of Privacy Impact Assessments conducted by ministries over the past five years. The number of PIAs reviewed by CIRMO in 2015/2016 was 687 (an increase of 28% compared to 2014/2015). In 2016/2017, the number of PIAs reviewed by CIRMO increased slightly to 719.

Because a PIA is only conducted when there is a new program or a change to an existing one, workload volumes can vary year-over-year. However, the generally steady upward trend in PIAs conducted reflects an improved understanding across government regarding the requirements for, and benefits of, these assessments. Over the past two fiscal years, CIRMO has undertaken efforts to streamline and increase efficiency in the PIA process. For example, conducting overarching PIAs for an entire project, rather than multiple PIAs for specific project components or phases of the larger project, results in fewer overall PIAs.

Fiscal Year	Number of PIAs Reviewed
2010/2011	208
2011/2012	266
2012/2013	444
2013/2014	509
2014/2015	536
2015/2016	687
2016/2017	719

Personal Information Directory

The [Personal Information Directory](#) (PID) is a public registry that satisfies the legislated requirement in FOIPPA for the Minister responsible for the Act to establish and maintain a public-facing directory of the government's personal information holdings. The PID includes summaries of information sharing agreements, PIAs and personal information banks that are established within or across ministries. Located on the DataBC website, the PID provides greater transparency by listing these holdings in an easily accessible way.

Investigating Privacy Incidents and Complaints

Reporting Privacy Incidents to CIRMO

Government policy requires any employee who becomes aware of an actual or suspected information incident, including a privacy breach, to report the incident immediately.

A member of the public who suspects their privacy may have been impacted by government's actions can also report a privacy complaint. Privacy complaints are treated as suspected privacy incidents and, where a complaint is found to be substantiated, the breach is investigated using standard procedures and approaches.

CIRMO is responsible for the coordination, investigation and resolution of all actual or suspected privacy incidents.

Most privacy breaches have a low potential for harm and affect only a single person or small group of people.

In both 2015/2016 and 2016/2017, only 1% of all privacy incidents investigated were considered to pose a serious risk of harm.

Understanding the Risk of Harm Resulting from Privacy Incidents

The details and circumstances of a privacy breach can vary significantly. In both 2015/2016 and 2016/2017, a very small proportion — only 1% — of all confirmed incidents represented a serious risk of harm.

In assessing the seriousness of information incidents, professional staff consider a range of factors to evaluate the potential for harm and the severity of any potential harm. In assessing the potential for harm, they consider a number of factors, such as the risk of:

- Physical harm;
- Identity theft or fraud;
- Hurt, humiliation or damage to reputation; and
- Loss of business or employment opportunities.

In assessing the severity of those potential harms, they consider factors related to the informational risks — such as the sensitivity, context and volume of personal information exposed — as well as situational risk factors, such as the ability to quickly contain an incident or the potential likelihood of further dissemination of the information. These factors contribute to a determination of low to moderate risk of harm; moderate to high risk of harm; or significant risk of harm.

In the 2015/2016 fiscal year, 988 confirmed privacy incidents were reported. In 2016/2017, the number of confirmed privacy incidents reported was 1,313. Of the 1,313 confirmed privacy incidents or complaints investigated in the 2016/2017 fiscal year, 228 (17%) were classified as "received and closed." A file that is "received and closed" involves an incident where there is little to no risk of harm and all necessary steps have been completed at the time the incident is reported to CIRMO. Such incidents involve little to no risk of harm that would warrant notification to the impacted individual, and the business area that experienced the breach has identified reasonable prevention steps such as employee coaching and awareness activities.

CIRMO is currently reviewing and updating its data model and analytical framework to support enhanced future reporting capabilities, including reporting based on the risk of harm.

	2012/2013	2013/2014	2014/2015	2015/2016	2016/2017
Confirmed Privacy Incidents and Complaints Reported^{7,8}	798	958	956	988	1,313

Increases in the reporting of privacy incidents over time can be attributed, in part, to corresponding increases in awareness and training across government about what a privacy breach is and what steps government employees are required to take when they have reason to believe one has occurred.

Understanding the Causes of Privacy Incidents

Most privacy incidents occur as a result of administrative errors in the processing and mailing of correspondence or in other client interactions, such as through email and over the phone. This type of privacy breach is characterized by having a low potential for harm to a single or small number of individuals.

The response to incidents caused by administrative errors involves an emphasis on containing and recovering information that has been exposed (wherever possible), assessing harm, and preventing similar incidents from occurring in the future.

During the 2015/2016 fiscal year, 791 administrative errors resulted in confirmed privacy violations. These administrative errors constituted 80% of all privacy confirmed incidents reported during this period. In 2016/2017, 980 administrative errors resulted in confirmed privacy violations, which accounted for 75% of all confirmed privacy incidents during this period.

21

When responding to a breach of any severity, CIRMO examines the circumstances and identifies prevention measures that are specific to the incident. CIRMO identifies practical steps that can be taken to prevent similar incidents from occurring, which include measures such as technical improvements, coaching and awareness activities with employees, and improvements to policy and/or practices.

⁷ This figure does not include suspected privacy breaches where it is determined that no actual loss or unauthorized collection, use, disclosure, access, disposal, or storage of personal information, whether accidental or deliberate, has occurred.

⁸ Statistics are generated at a point in time while investigations are ongoing. Therefore, there may be discrepancies between the figures reported in past reports and figures reported here. These discrepancies arise where, for example, continued investigation after the report is generated determines that the reported incident is not a privacy breach.

Understanding the Volume of Incidents and Complaints Reported

The number of reported incidents and privacy complaints was higher than the number of confirmed privacy incidents reported above in both fiscal years.

In 2015/2016, there were 1,109 suspected privacy incidents reported to CIRMO. Of these, 988 were substantiated by CIRMO as confirmed privacy incidents. More than half of the privacy complaints reported to CIRMO during this period were found to be unsubstantiated.

The fact that more privacy violations are reported than confirmed reflects a high level of awareness among employees of the important obligation to protect the personal information in their care.

In 2016/2017, there were 1,441 suspected privacy incidents reported. Of these, 1,313 were substantiated by CIRMO as confirmed privacy incidents. Of those which were substantiated, only 1% was ultimately determined to bear a significant risk of harm.

A privacy complaint may be found to be unsubstantiated in instances where, for example, a ministry or agency is determined to have had legislative authority to handle the individual's information under the circumstances, or where evidence confirms the situation a person has complained about did not occur as alleged. In these cases, CIRMO typically provides information to the individual to help them better understand the circumstances under which government is authorized to collect, use and disclose their personal information.

During the 2015/2016 fiscal year, government received 62 privacy complaints, a slight decrease from the previous fiscal year. Of these, a privacy breach was confirmed in 26 cases⁹. In the remaining 36 cases, the privacy complaint was determined after investigation to be unsubstantiated. During the 2016/2017 fiscal year, CIRMO received 80 privacy complaints. As of May 2017 when this report was produced, the investigation of 55 of these incidents was completed with 26 having been confirmed as substantiated, while in the remaining 29 cases, the privacy complaint was determined after investigation to be unsubstantiated. As of the same date, another 25 of these complaints remained under investigation.

⁹ All confirmed privacy breaches are included in the totals provided under the heading "Reporting Privacy Breaches to CIRMO."

Notifying Affected Individuals and Reporting Privacy Incidents to the Information and Privacy Commissioner

When there is a risk of significant harm, government notifies affected individuals as soon as possible. It is preferable to notify individuals directly, but if the incident involves a large number of individuals it may not be practical to notify each person individually in a timely manner. In order to reach the largest population of affected individuals in the least amount of time, other methods of notification, such as announcements in the media, may be used.

Government proactively reports all potentially serious privacy incidents to the OIPC as soon as possible. In addition, since January 2015, government has also provided a monthly report to the Office of the Information and Privacy Commissioner (OIPC), of all actual or suspected privacy incidents, regardless of severity.

In 2015/2016, government proactively notified the OIPC of 15 potentially serious privacy incidents, including an incident involving a missing hard drive which contained personal information for approximately 3.4 million individuals. In 2016/2017, government proactively notified the OIPC of 22 potentially serious privacy incidents. Several of these potentially serious privacy incidents were ultimately found not to represent a serious risk of harm.

After receiving the report, the OIPC may monitor a government investigation or open its own investigation. OIPC staff may also assess the methodology used in the government investigation and seek clarity on outstanding questions as they arise.

Looking Ahead: Continuing to Lead the Way in Access to Information and Protection of Privacy

As we move forward in 2017/2018, issues such as the rise in the use of wearables and the “Internet of Things,” the changing nature of information requests and new trans-border flows of data are just some considerations when providing access to information and protecting individuals’ privacy. Continuing to anticipate and address the unique and unprecedented challenges presented by these and other trends requires a robust and nimble privacy and access program.

With an increased focus on awareness and training, and fundamental enhancements and improvements to the way information is integrated and managed throughout government, the Province is well prepared to address these challenges. We are committed to building on our recent successes in the area of access to information and protection of privacy. This includes government’s continued commitment to streamlining the process for responding to FOI requests and increasing the proactive disclosure of information. It also includes a continued focus on robust awareness and education initiatives, and an enhanced and formal assessment of ministries’ compliance with legislative and policy requirements.

Opportunities and challenges will continue to arise. As a government, we are shifting to digital-only management of information. And as an innovator in such areas as evidence-based policy, program and service design, B.C. will need to develop solutions that strike the balance between protecting privacy and transforming the way we manage and use information.



Ministry of
Finance