Yukon Ombudsman

Yukon Information and Privacy Commissioner

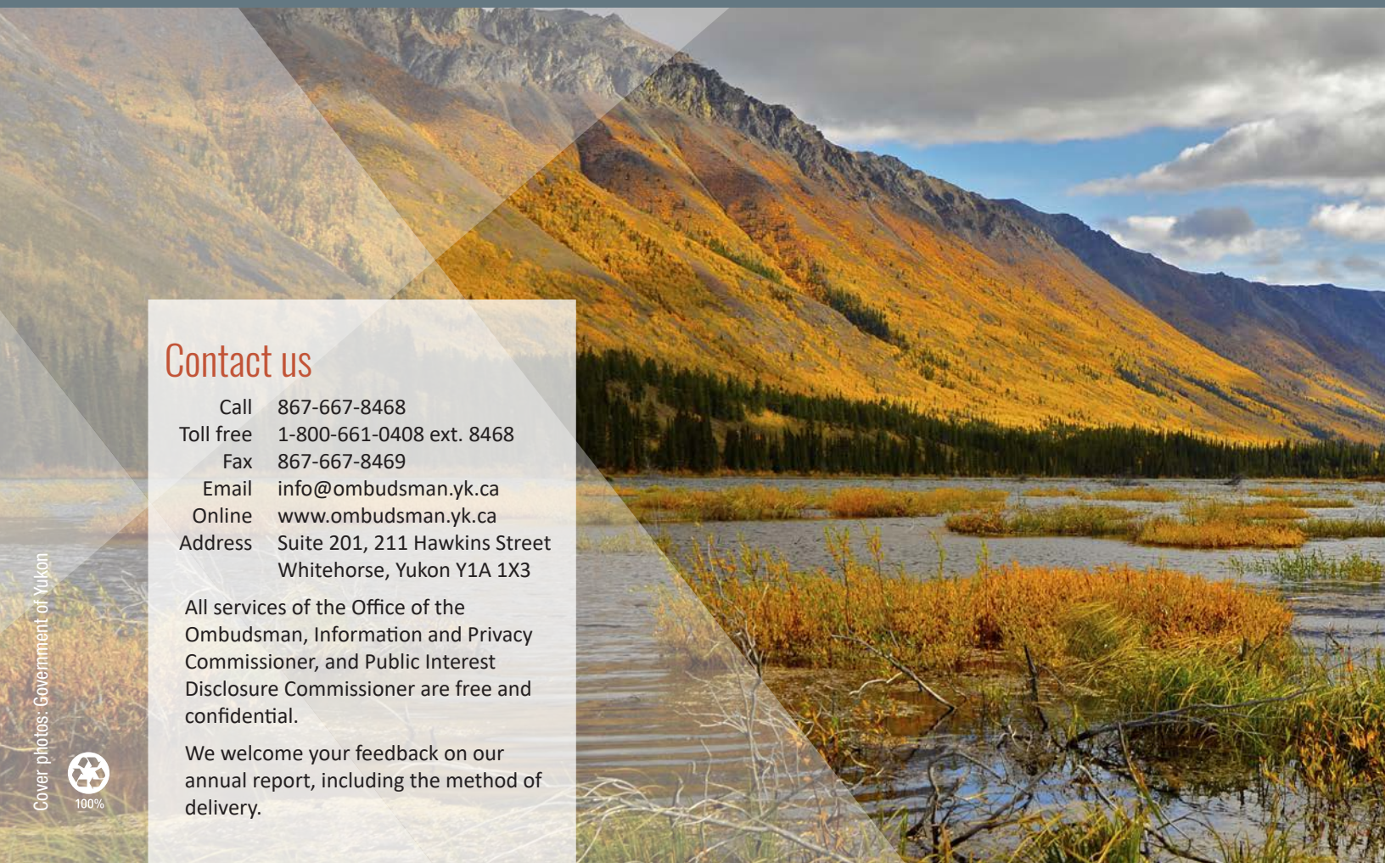
Yukon Public Interest Disclosure Commissioner

2018 ANNUAL REPORT

Working hard for Yukoners

Table of contents

Photo by Alistair Maitland Photography



Contact us

Call	867-667-8468
Toll free	1-800-661-0408 ext. 8468
Fax	867-667-8469
Email	info@ombudsman.yk.ca
Online	www.ombudsman.yk.ca
Address	Suite 201, 211 Hawkins Street Whitehorse, Yukon Y1A 1X3

All services of the Office of the Ombudsman, Information and Privacy Commissioner, and Public Interest Disclosure Commissioner are free and confidential.

We welcome your feedback on our annual report, including the method of delivery.

Cover photos: Government of Yukon

100%

Diane McLeod-McKay

Yukon Ombudsman, Information and Privacy Commissioner, and Public Interest Disclosure Commissioner

2018 was an incredibly busy and challenging year for my office. We experienced a significant change in staffing and had to manage double the workload as compared to 2017. In addition, the complexity of the work we did increased as well. In 2018, we received numerous disclosures and complaints under the *Public Interest Disclosure of Wrongdoing Act* (PIDWA), which led to large and complex investigations. We were also extensively involved in the redraft of the *Access to Information and Protection of Privacy Act* (ATIPP Act) by the Government of Yukon.

New staff

In 2018, I recruited to fill three positions in my five-person office. Losing seasoned staff with highly technical skills was difficult. However, I am very pleased that I was able to hire three professionals with exceptional qualifications. Two came with extensive mediation and conflict resolution skills. Both had previously worked in the ombuds field. The third came with a solid background in information security and technology. Being able to fill my vacant positions with such highly-skilled individuals will contribute to my ability to achieve one of the goals identified in my 2017 Annual Report, i.e. to ensure my office staff are skilled enough to manage the challenges that come with delivering on our multiple mandates.

Workload doubled

Not only did I recruit and train three new staff members in 2018, but I had to do so in the course of managing double the workload from the previous year. In 2018, we opened 180 files, compared to 90 in 2017. The majority of these (141) were managed through our informal resolution process. It is interesting to note that 41.8% of the 141 files were requests for review of decisions made by public bodies under the ATIPP Act. As well, the time-driven informal case resolutions under the ATIPP Act and the *Health Information Privacy and Management Act* (HIPMA) increased 164.5% from 2017. My new staff members had to work very hard and learn quickly, so that we could keep up with the volume of work. We are in the process of examining the numbers of requests for review that we receive, to ensure public bodies are effectively managing access to information requests.

A spike in PIDWA files

In 2018, we saw a sudden and significant increase in files opened under PIDWA. We opened 14 files in 2018, compared to only two in 2017. Of those 14, eight were investigations (five disclosures and three complaints of reprisal). PIDWA investigations have proven to be extremely complex and resource-intensive. I have only 1.5 FTEs (FTE stands for 'equivalent of a fulltime employee') to manage these investigations along with all other formal investigation files opened. In 2018, we also saw a dramatic rise in our overall investigative work. In 2017, we had two of these files whereas in 2018, my office opened 12 in total. As mentioned, eight of those were PIDWA investigations.

When PIDWA was proclaimed in force, my office received no funding increase and no additional FTEs. Consistent with other jurisdictions, the work generated by PIDWA was slow to come but has now arrived. Given the amount of work this law is generating for my office and the significance of the investigations that serve the public interest, increased resources to meet this mandate are now necessary. I requested and was granted one additional FTE in my 2019/20 budget for this and other investigation work conducted by my office.

ATIPP Act redraft

During 2018, my office was extensively involved in reviewing the revised ATIPP Act, which was passed in the Yukon Legislative Assembly in December 2018. Not only did I spend 15 hours in face-to-face meetings with the drafters, I and my team spent countless hours throughout the summer and fall reviewing the more than 100 pages of legislation and amended drafts to ensure the privacy and access to information rights of Yukoners would be preserved and, where possible, strengthened. We will spend 2019 reviewing the regulations, once developed, and begin planning for implementation. The new ATIPP Act grants the Information and Privacy Commissioner (IPC) additional authority that we will need to prepare for and be properly resourced to deliver on. In my 2020/21 budget, I intend to request another FTE to ensure we are able to carry out this work.

2018 Annual Reports

Specific information about the year 2018 for each of my mandates can be found in my 2018 Annual Reports for the Ombudsman, Information and Privacy Commissioner, and Public Interest Disclosure Commissioner, which are included within this document. I hope you find the information within the reports informative and useful.

Kind regards,

Diane McLeod-McKay, B.A., J.D.,
Yukon Ombudsman, Information and Privacy Commissioner, and Public Interest Disclosure Commissioner

Goals update

In my 2017 Annual Report, I indicated there are eight goals that I will focus on during my current five-year term, which began in June 2018. They are:

1. to establish an oversight office sufficiently skilled to address new challenges and deliver on our multiple mandates;
2. to support the development of privacy management programs for public bodies and custodians;
3. to improve access to information by working with public bodies to make increased information accessible without an access request and by improving the knowledge of those responsible for processing formal access to information requests;
4. to assist public bodies in implementing the new ATIPP Act;
5. to enhance fairness in authorities, through the use of proactive measures;
6. to increase the understanding by public entities and employees about what a disclosure is, how to make one, and reprisal protection;
7. to deliver on my outreach strategy to increase knowledge amongst the public and within the health sector on the mandates of the office and to inform the public about their rights thereunder; and
8. to participate in the review of HIPMA (to be initiated by August 2020) and PIDWA (to be initiated by June 2020).

Updates on these goals are in the Ombudsman, Information and Privacy Commissioner, and Public Interest Disclosure Commissioner messages, with the exception of goals one and eight, which I have addressed in my general message.

Yukon
Ombudsman

2018 ANNUAL REPORT OF THE YUKON OMBUDSMAN

The Honourable Nils Clarke
Speaker, Yukon Legislative Assembly

Dear Mr. Speaker:
As required by section 31 of the *Ombudsman Act*, I am pleased to submit the Annual Report of the Ombudsman for the calendar year 2018.

I am also pleased to share this with the Yukon public.

Kind regards,

Diane McLeod-McKay,
Yukon Ombudsman

Photo: Government of Yukon

A YEAR IN REVIEW

I am pleased to present my 2018 Annual Report under the *Ombudsman Act.*

This year we saw a marginal increase in complaints to the Yukon Ombudsman. In 2017, we received 25 complaints compared to 30 in 2018. The complaints received this year were about 12 different authorities. These authorities are listed in the "Accountability" section of this annual report.

Of the 30 complaints, eight were made about the Department of Health and Social Services (HSS), five about the Department of Justice (Justice), and another five about the Department of Energy, Mines and Resources (EMR).

The complaints made about HSS centre around social assistance benefits received by Yukoners. Those about EMR relate primarily to mining activity, and those about Justice are related to the Whitehorse Correctional Centre, the Coroner, and the Maintenance Enforcement Program. Detail about some of these complaints can be found in the "Samples of our work in 2018" section of this annual report.

In most of the stories we've included, our office found that the authority acted fairly. However, in some cases we made observations about the need to increase transparency, so that individuals can access information more readily about those services. The authorities agreed with our observations and committed to making improvements to increase transparency.

In our discussions with individuals who made complaints under the *Ombudsman Act,* it was apparent that these individuals were frustrated with the lack of information available about policy and procedures and the lack of other information to tell them about services provided by the authorities. As such, we examined access to this kind of information during our investigations, which led to our observations made in this regard.

In the new *Access to Information and Protection of Privacy Act* (not yet proclaimed into force), public bodies who are also authorities under the *Ombudsman Act* will be required to make information publicly accessible about the structure under which they deliver services, including responsibilities and functions, as well as the policies used to deliver services. My hope is that these requirements will facilitate transparency and alleviate this frustration.

Update on goals

In my 2017 Annual Report, I indicated that during my second term as Ombudsman, which began in June 2018, I would enhance fairness in public service delivery through proactive means.

My office, together with other ombuds offices in Canada, has been working to develop a fairness evaluation tool and this work is now complete. We plan to pilot the tool in 2019 with a few authorities in Canada, including in Yukon, to test its effectiveness. Once we move from pilot to implementation, we will work with authorities to implement the tool. Its purpose is to help authorities evaluate fairness in service delivery and make improvements as necessary. In Yukon, we intend to use the fairness standards identified in the tool, together with the *Ombudsman Act*, to measure the fairness of authorities that we investigate.

My other key goal is to increase awareness of the obligations of authorities subject to the *Ombudsman Act* and the rights of the general public under the legislation. In 2019, I intend to acquire communications support and I am optimistic that this support, together with the fairness evaluation tool, will enable us to deliver on this goal.

Own motion authority under the *Ombudsman Act*

In my 2017 Annual Report, I reported that Yukon's *Ombudsman Act* is the only ombuds law in Canada that does not grant authority to the Ombudsman to initiate investigations themselves, known as "on their own motion" investigations. In 2018, a number of individuals brought our attention to concerns that we could not investigate under the *Ombudsman Act*, because the individuals were not personally aggrieved, which is a requirement to make a complaint under the Act.

As an example, we determined that within our investigation of group home care under the *Public Interest Disclosure of Wrongdoing Act* (PIDWA), some of the issues would be better suited for an investigation under the *Ombudsman Act.* However, because I cannot initiate an investigation on my own motion under this Act, we were unable to investigate these issues. In this example, it would be up to the children in care to make a complaint, which they may be hesitant to do, given their reliance on HSS for their welfare. This may prevent children from raising concerns with the Ombudsman. Additionally, we spoke to a few individuals in 2018 who expressed fear about making a complaint under the *Ombudsman Act* given their reliance on services delivered by an authority. If the Ombudsman had authority to initiate an investigation on their own motion, these issues could have been examined.

For the sake of ensuring fairness in the delivery of publicly-funded services, the Ombudsman should have authority to initiate an investigation on their own motion, whether or not an individual is personally aggrieved. In 2019, I intend to address this issue with the Speaker of the Yukon Legislative Assembly, who is responsible for the *Ombudsman Act.*

In closing, I hope you find the information in this 2018 Annual Report informative and useful.

Diane McLeod-McKay
Ombudsman

SAMPLES OF OUR WORK IN 2018

Putting personal privacy first... even at work

BAILEY, AN OFFICE SUPERVISOR IN THE DEPARTMENT OF ENERGY, MINES AND RESOURCES (EMR), LEFT WALLACE, HIS DIRECT REPORT, IN CHARGE OF THE OFFICE WHILE BAILEY WAS AWAY FOR A WEEK. WHEN BAILEY RETURNED, HE BECAME SUSPICIOUS THAT WALLACE HAD USED THE OFFICE FOR NON-GOVERNMENT MEETINGS.

Bailey found personal emails to and from Wallace during work hours in the office general inbox. Bailey also found that Wallace had not completed tasks that Bailey wanted done before his return.

Bailey asked to meet with Wallace to discuss these issues. Before the meeting could occur, Wallace went on leave. After Wallace left, Bailey noticed that Wallace had not activated his out-of-office message on his voicemail. Bailey obtained a generic password to put the out-of-office message in place, but once Bailey had full access to Wallace's email account, Bailey decided to look through it. He then downloaded and printed some of Wallace's personal emails and documents, as well as work-related emails and documents, all of which Bailey considered to be strong evidence against Wallace.

Bailey contacted his boss to discuss Wallace. During the meeting, Bailey produced the emails and revealed how they were obtained. Afterward, Bailey attended a meeting with EMR Human Resources (HR) and was disciplined because of his actions. Bailey grieved the result. He then complained to the Ombudsman that EMR HR treated him unfairly when it took disciplinary action.

The Ombudsman conducted an investigation and found that Bailey had enough knowledge to perform his supervisory duties. As part of this knowledge, Bailey should have known

that Wallace had privacy rights regarding his personal email and that he did not have authority to access Wallace's email account, without first consulting Bailey's boss. Bailey had other less invasive options available. He could have first addressed his concerns directly with Wallace. We found no unfairness in the decision to take disciplinary action against Bailey.

We made two observations during this investigation. We observed that EMR may not have taken adequate steps to manage the potential privacy violation and encouraged the department to evaluate whether a privacy breach occurred and to inform the Office of the Information and Privacy Commissioner about its findings. We also observed that the procedure for accessing an employee's email may not have been followed and we encouraged EMR to evaluate whether this procedure is robust enough to prevent privacy and security breaches.

Following our investigation, EMR informed us that it "…found the work with the [Ombudsman] very helpful in driving continuous improvement".

Different treatment doesn't always equal unfair treatment

MARLEY IS A SINGLE SENIOR WHO RECEIVES A PIONEER UTILITY GRANT FROM THE DEPARTMENT OF HEALTH AND SOCIAL SERVICES (HSS) TO HELP PAY FOR HEATING HER HOME IN WINTER. WHEN SHE FIRST APPLIED FOR THE YEARLY GRANT, SHE GOT THE FULL AMOUNT. THAT CHANGED AFTER NEW LEGISLATION WAS PASSED, AND MARLEY FELT THE CHANGE LED TO UNFAIR TREATMENT, WHICH BROUGHT HER TO THE OMBUDSMAN.

For reasons of long-term program sustainability, HSS introduced income thresholds and testing at the time the new *Pioneer Utility Grant Act* was passed in 2014. The income thresholds were put in place to determine grant eligibility. Seniors were now divided into two groups, single and couples. Only single seniors who earned less than $117,000 annually and 'coupled' seniors who earned less than $165,000 annually were eligible to apply for a grant. The position of HSS is that all eligible seniors have limited funds to pay for heating but more so if two seniors are living together. That's because the amount they could put toward heating costs also depended on the amount they had to pay for other necessities of life. These necessities were presumed to be higher for two people. In other words, couples had less disposable income to pay for heating than a single senior.

The second measure, income testing, was to determine the size of a grant paid to an eligible applicant. Single seniors earning $40,000 or less annually would receive the full amount of the grant. The amount then diminished on a sliding scale to zero as income reached $117,000. Coupled seniors earning $56,000 or less annually would receive the full amount, diminishing to zero as their income reached $165,000.

Marley's income qualified her for the grant, so she applied and received it. She later learned that her friends, Jordan and Casey, had the same combined income as she did and that they had received a higher grant. Marley thought something was wrong, especially since they had similar houses and heating costs.

Marley made a complaint to the Ombudsman. She felt that HSS was discriminating against her by treating seniors differently when calculating grant amounts. She believed that she had been treated unfairly. The Ombudsman decided to investigate her issue.

We learned that the first *Pioneer Utility Grant Act* in 1978 provided financial assistance to seniors to assist or partially offset high home heating costs during the winter. It was a universal benefit available to all eligible seniors at a flat rate, regardless of income or location of principle residence in Yukon. In 2003, the flat rate was amended to allow for an annual rate increase. In 2014, HSS became concerned about the growing number of seniors and program costs. It wanted to assist low-income seniors, and this led to the new legislation that resulted

in Marley being treated differently than her friends, Jordan and Casey.

We found that this treatment, although different, was not unfair. The program is specifically designed to benefit seniors. It also recognizes that the cost of living is higher for coupled seniors than for single ones. As such, they are treated differently. But this does not amount to unfair discrimination under the *Ombudsman Act* because there are fair and rational reasons for this treatment. HSS is not precluded from providing a special program that sets priorities in providing heating cost assistance and draws distinctions that promote reasonable outcomes. Each eligible applicant, single or coupled, receives a grant that diminishes as their income increases. While Marley received a different amount than Jordan and Casey, it wasn't due to any unfairness.

Cancellation of a courtesy does not an unfairness make

JORDAN WAS THE HOLDER OF A QUARTZ (ALSO KNOWN AS HARD ROCK) MINERAL CLAIM FOR MORE THAN 10 YEARS. UNDER THE YUKON *QUARTZ MINING ACT*, CLAIMS ARE RENEWED ANNUALLY. IN ORDER TO RENEW THE CLAIM, THE CLAIM HOLDER MUST EITHER HAVE DONE WORK ON THE CLAIM WORTH MORE THAN $100 OVER THE YEAR OR PAY A FEE "IN LIEU" OF ANY WORK BEING DONE.

For more than a decade, Jordan received a courtesy notice from the Department of Energy, Mines and Resources (EMR) reminding him of the renewal, and each year he would make the necessary "in lieu" payment by the due date. This continued annually until recently, when EMR stopped sending courtesy notices.

Jordan filed a complaint with our office claiming that he was not notified about the cancellation of the courtesy notice process and that it was unfair because it caused him to miss the renewal date of his claim, which then lapsed.

The complaint was investigated by a member of my office's informal case resolution team. Our investigation confirmed that the practice of sending out the notices was started years ago by the federal government and this continued under the Yukon government upon devolution. We noted during our investigation that the practice was inconsistent with what was done with placer claims, which had never had courtesy notices sent.

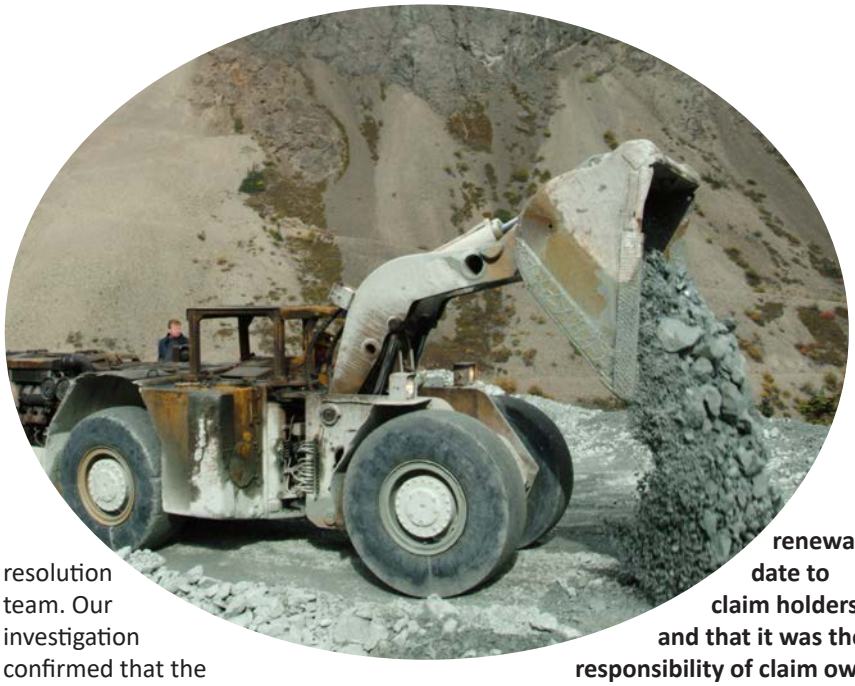


Photo: Government of Yukon

In our discussions with EMR, staff explained that with the growing number of quartz mineral claims in Yukon (more than 200,000), it had become administratively difficult to support the continuation of the courtesy notices.

In determining whether this change in process might be considered unfair, we investigated what steps EMR took in cancelling the process. Through our investigation we learned that EMR had informed quartz claim holders of the change in the renewal information mailed to them the previous year. EMR also provided information about the cancellation of these notices on its websites and in the offices of mining recorders across Yukon.

In reviewing documents during our investigation, we confirmed that the information about the cancellation of courtesy notices had been received by the complainant. We also confirmed that the *Quartz Mining Act* did not require EMR to give notice of the renewal date to claim holders and that it was the responsibility of claim owners to ensure they renewed on a timely basis. For those unsure of their claim status, EMR provides a search tool on its website allowing claim owners to check the status of their claim(s).

Our office determined that no unfairness occurred in the cancellation of the courtesy notice process or in the way EMR informed claim owners.

Taking notice of the need for notice

JAIME, AN APPLICANT FOR SOCIAL ASSISTANCE, CONTACTED OUR OFFICE WITH TWO CONCERNS. FIRST, JAIME DID NOT AGREE WITH A DEPARTMENT OF HEALTH AND SOCIAL SERVICES (HSS) DECISION TO CONSIDER A BANK DEPOSIT AS MONTHLY "INCOME," THEREBY RESTRICTING HIS SOCIAL ASSISTANCE AMOUNT FOR THAT MONTH. HE WAS ALSO UNHAPPY WITH THE WAY THE DEPARTMENT COMMUNICATED WITH HIM.

Jaime's position was that the money was a reimbursement of funds previously loaned to a friend in need and should not be counted as income. Jaime took the complaint to the Social Assistance Review Committee (SARC), which is tasked with hearing disputes of this nature from social assistance applicants. The SARC ruled in favour of upholding the decision to limit Jaime's social assistance amount.

The second issue Jaime brought to our attention was that he received inadequate and delayed communication from HSS throughout the hearing process. Specifically, Jaime indicated having only received notice of the SARC hearing date on the morning of, leaving him insufficient time to prepare. Jaime also indicated having not been provided with a copy of the SARC decision until a little over a month had passed, by which time the deadline for appealing the decision to the Yukon Supreme Court had lapsed.

While HSS stood by the SARC ruling, our investigation revealed that the department had not met its requirement under the legislation to provide Jaime with a copy of the SARC decision within the time frame for appealing it, resulting in unfairness. To remedy the situation, HSS agreed to reimburse the disputed amount in full.

While satisfied with the outcome, our office made some additional observations in regard to this case. We suggested that HSS consider creating a policy guideline or practice note to help department employees and SARC interpret the Social Assistance Regulations related to income determination. In the interest of transparency, we suggested these guidelines be made readily available to applicants for social assistance.

While HSS provided evidence to support that Jaime was given at least seven days' notice of the review hearing, as prescribed in the legislation, it was not explicitly clear from the evidence whether this in fact occurred. As the point was now moot, we took the opportunity to remind HSS that the onus is on them to ensure that applicants who request a review are duly notified within the prescribed timeframe.

The importance of setting a date

SIDNEY WAS REQUIRED TO PAY CHILD SUPPORT BY AN ORDER OF THE COURT, WHICH WAS REGISTERED WITH THE MAINTENANCE ENFORCEMENT PROGRAM (MEP). SIDNEY CAME TO OUR OFFICE EXPRESSING CONCERN THAT THE MEP WAS TELLING HIM THAT HE HAD TO PAY THE CHILD SUPPORT ON A SPECIFIC DAY EACH MONTH. THE COURT ORDER DID NOT SPECIFY THE DAY OF THE MONTH TO MAKE PAYMENT, SO SIDNEY MADE A COMPLAINT ABOUT THE ISSUE TO OUR OFFICE AND IT WAS INVESTIGATED BY A MEMBER OF OUR INFORMAL CASE RESOLUTION TEAM.

The responsibility of the MEP is to enforce child support payments according to the terms contained in a court order (or legal agreement). When a person registers a court order with MEP, either as the party who pays or receives support, the program works from those terms to collect and distribute ongoing support. MEP will do what it can to collect support payments as per the court order.

Sidney's court order required that he pay support in the amount of $300.00 per month but was silent on the date the payment had to be made. This is because the parties to the court order could not agree on a date for the monthly payment. The Maintenance Enforcement Program had adopted a practice that when a date was not specified in a court order and the parties could not agree with MEP on a payment date, then MEP would require it be paid on the first of every month. Sidney objected to the requirement to pay on the first of the month, believing the date for payment should be a later date.

During the work with our informal case resolution team member, MEP agreed that it did not have authority under the *Maintenance Enforcement Act* or otherwise to impose a payment date and agreed that its authority is to follow the terms set out in the court order. In addition, we discovered that Section 4 of the *Maintenance Enforcement Act* authorizes MEP to refuse to file an order where there is doubt or ambiguity about its meaning, legal effect or enforceability, and an order that does not specify a date for payment will not be accepted for registration as there is doubt about the enforceability of the court order. Where no date is specified, before it can be registered with MEP, the parties must agree to amend the order or return to court to ask the court to set a date.

MEP agreed to develop a policy to guide staff on how to deal with a court order that does not specify a date for payment of support.

HOW WE MEASURED UP IN 2018

Accountability

Facilitating fairness

The Director of Intake and Informal Case Resolution in the Yukon Ombudsman office is working with our colleagues in several ombuds offices in Canada to finalize a new fairness evaluation tool. We intend to pilot this tool early in 2019 and hope to have it ready for use by authorities later in the year.

Skills development

Yukon's Ombudsman attended the meeting of the Canadian Council of Parliamentary Ombudsman, hosted by Manitoba's Ombudsman in Winnipeg.

Complaints against the Ombudsman

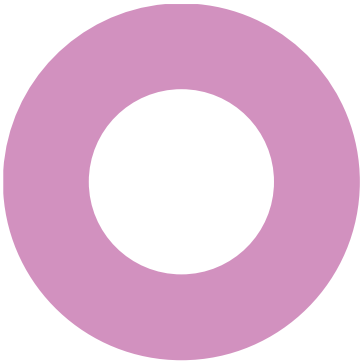
None

Ombudsman Act 2018 activity	
Resolved at intake - no file opened	
Request for information	60
Informal complaint resolution	6
No jurisdiction	5
Referred-back	20
Total	**91**
File opened by type	
Settlement files opened	29
Investigation files opened	1
Total	**30**
All files opened in 2018	30
Files carried over from previous years	9
Files closed in 2018	25
Files to be carried forward	**14**

Our performance on investigations

Ombudsman investigation - 1 year target

Closed (within 1 year)	0
Closed (over 1 year)	0
Still open (within 1 year)	1
Still open (over 1 year)	0



Ombudsman settlement - 90 day target

Closed (within 90 days)	13
Closed (over 90 days)	5
Still open (under 90 days)	2
Still open (over 90 days)	9

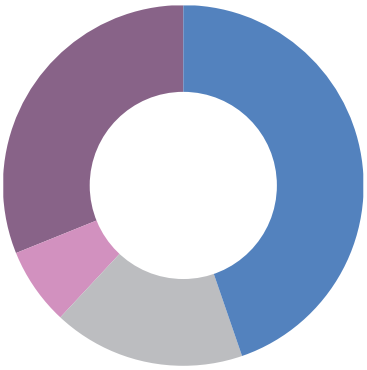


Photo: Government of Yukon

Files opened in 2018 by authority

Authority	Number of files			Recommendations		
	Informal case resolution	Investigation	Total	Formal*	Accepted	Not yet implemented (includes from prior years)
Department of Energy, Mines and Resources	5	0	5			
Department of Health and Social Services	7	1	8	1	1	
Department of Highways and Public Works	3	0	3			
Department of Justice	5	0	5	2	2	
Lotteries Yukon	1	0	1			
Public Service Commission	1	0	1			
Yukon Child Care Board	1	0	1			
Yukon College	1	0	1			
Yukon Hospital Corporation	1	0	1			
Yukon Human Rights Commission	2	0	2			
Yukon Teachers' Association	1	0	1			
Yukon Workers' Compensation Health and Safety Board	1	0	1			

*Formal recommendations are those made by the Ombudsman in a formal Investigation Report issued in 2018.

Photo: Government of Yukon

Yukon Information and Privacy Commissioner

2018 ANNUAL REPORT OF THE YUKON INFORMATION AND PRIVACY COMMISSIONER

The Honourable Nils Clarke
Speaker, Yukon Legislative Assembly

Dear Mr. Speaker:
As required by section 47 of the *Access to Information and Protection of Privacy Act* and Section 97 of the *Health Information Privacy and Management Act*, I am pleased to submit the Annual Report of the Information and Privacy Commissioner for the calendar year 2018.

I am also pleased to share this with the Yukon public.

Kind regards,

Diane McLeod-McKay,
Yukon Information and Privacy Commissioner

Photo: Government of Yukon

A YEAR IN REVIEW

I am pleased to submit my 2018 Annual Report under the *Access to Information and Protection of Privacy Act* (ATIPP Act) and the *Health Information Privacy and Management Act* (HIPMA).

This year we saw a significant increase in files opened under these two Acts. In 2018, we opened 136 files, compared to 2017, when we opened 64. This represents a 112.5% increase in files opened.

Sixty-one of the 103 ATIPP Act files opened are review files. In 2017, we opened just 17 review files.

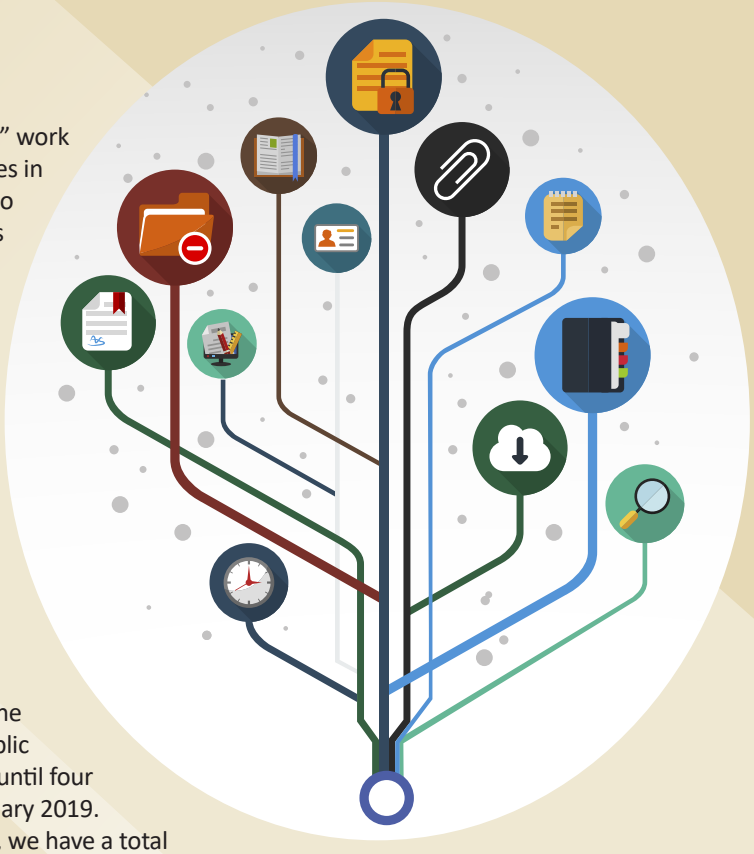
ATIPP Act - Access to information

The majority of our review files under the ATIPP Act (59 out of 61) are reviews of decisions made by employees of Government of Yukon public bodies that are responsible to process access requests. Our reviews suggest that the access to information program operated by these public bodies needs evaluation to ensure they are operating in accordance with the ATIPP Act.

As in prior years, we are not receiving adequate evidence from public bodies to support their decisions to refuse access to records or information. Our experience has shown that employees responsible for determining whether exceptions apply often do not understand these exceptions, including that thresholds for applying an exception must be met. On occasion, when we ask for the records to review, it is evident that the public body did not complete an adequate review of the records, prior to refusing access. In these cases, there is always a delay before we receive the records for review.

In addition, most of the exceptions to the right of access to information are discretionary. Public bodies that rely on discretionary exceptions do not properly, or at all in some cases, exercise their discretion before refusing access. The exercise of discretion must occur.

The lack of "up front" work by these public bodies in dealing with access to information requests is contributing to delays in our ability to meet our timelines under the ATIPP Act. It also contributes to our inability to settle matters before the time allowed under the ATIPP Act runs out. In one case, we received a request for review in September 2018. We did not receive the records from the public body for our review until four months later, in January 2019. Under the ATIPP Act, we have a total of 150 days (approximately five months) to complete the review, including the inquiry stage. In another case opened in 2017, we were still receiving records for our review toward the end of 2018. These lengthy delays in processing access to information requests are unfair to applicants who have a right to access to information held by public bodies in a timely manner.



Another area of concern is the way public bodies search for records. Much of the information held by public bodies is now within electronic information systems, including email records. A number of investigation files opened under the ATIPP Act allege inadequate search. During our investigation of these allegations, we learned that searches are not being conducted properly and depend largely on the knowledge the employee responsible to process the request may have about the location of information, rather than a systematic approach. This problem has led us to develop search methodology to help public bodies perform adequate searches for records contained in electronic information systems. In 2019, we intend to offer a workshop on this topic.

Given the state of access to information as described, I am of the view that the only real way to resolve these issues is for the Government of Yukon to conduct an evaluation of access to information programs operating within its public bodies together with the records manager program.

The Government of Yukon ATIPP Office issues an annual report on the access to information activity of the public bodies. The report includes the number of requests received by the public bodies from year to year and the time taken to process them. These records show that the number of access to information requests received by public bodies over the past four years has been relatively stable. There was a modest increase of 35% in requests between 2016/17 and 2017/18. The report does not identify the amount of records requested in each instance or any challenges in searching for large amounts of records. It also does not identify the amount of resources dedicated by each

public body to processing access to information requests and the training received by access to information coordinators (ATI coordinators). This information would be useful in evaluating the quality of the program. It would also be helpful to know how ATI coordinators are processing access to information requests.

The current government has indicated its commitment to improving access to information held by Yukon government public bodies. The fact that the new ATIPP Act was designed to increase the ability to access information, both within and outside the formal process, reflects this commitment. While this is good news, access to information will not improve under any access to information law, if public bodies are not positioned to meet their obligations.

To do so, the government must have knowledge of the shortcomings in public bodies' access to information programs and must implement measures for improvement. To this end, the Yukon government may wish to consider auditing these programs to identify where improvements are needed. Information generated by an audit would assist the ATIPP Office and my office to prioritize areas to focus on for education and allow us to use our limited resources more effectively. This work would contribute to one of my eight goals set out in my 2017 Annual Report, which I intend to deliver on during my second term. The goal is to increase the knowledge of those responsible for processing formal access to information requests.

Fixing the problems with the access to information system now will enable a smoother transition from the existing ATIPP Act to the new ATIPP Act, which contains a number of new accountability measures. The new Act is expected to be proclaimed into force by 2020. Once it is in force, we will work with public bodies on meeting their access to information requirements. This work will enable me to meet another of my goals, to help public bodies implement the access to information provisions of the new ATIPP Act.

ATIPP Act - Privacy

During the summer and fall of 2018, my team and I worked extensively with Yukon government employees on the new ATIPP Act. During my review of the many drafts of the Act that I received, I compared the contents to my recommendations made in my 2015 ATIPP Act Review comments and found that most were incorporated into the new law. The majority of those comments were to amend the existing ATIPP Act to allow increased sharing of personal information within and among public bodies for the purposes of innovation, while ensuring proper controls are in place to adequately protect the privacy of individuals whose personal information is processed for these activities.

A key measure of control to ensure compliance with privacy laws is ensuring public bodies have a privacy management program that includes: policy and procedures; proactive privacy management tools such as privacy impact assessments; adequate security of personal information including the requirement to report breaches; proper resources for the privacy management program and reporting to senior management; and regular evaluation of the program to ensure it is effectively facilitating compliance. Another key measure of control is effective oversight.

The new ATIPP Act builds in most of these requirements and mandates public bodies to have privacy management programs in place, as described above. The new Act also expands the authority of the Information and Privacy Commissioner (IPC) to facilitate more effective oversight, including the ability to audit and to use own motion power, which is the authority to initiate an investigation into a potential issue on her own, without waiting for a complaint from an individual who has been affected.

The IPC's audit power under the new Act, once implemented, will be limited to auditing compliance with the privacy provisions. This power is the primary means by which the IPC will be able to evaluate compliance with these provisions. This was recognized during the passage of the new ATIPP Act in the Yukon Legislative Assembly. Conducting compliance audits is complex and resource-intensive work, which requires a specific skill set. With our current staffing levels, our ability to conduct these audits, together with the many new responsibilities we will have once the new ATIPP Act is proclaimed in force, will be limited. I have been informed that the Act is expected to be in effect by 2020. To ensure that we are able to perform our oversight function upon proclamation, I will be requesting an additional resource for my compliance review team. The responsibilities of this team are to: review privacy breaches and make recommendations on notification and to prevent recurrence; review all privacy impact assessments received and make recommendations for compliance; review all tools that promote compliance such as policy and procedure; promote and participate in educational opportunities to promote compliance; and evaluate information security risks. There is currently one person assigned to compliance review activities in my office, with the existing file load at 67.

Planning for the implementation of the new ATIPP Act has and will enable me to deliver on three of my eight goals. They are to support the development of effective privacy management programs in public bodies, ensure my office is sufficiently skilled to meet our new mandated obligations, and assist public bodies to implement the privacy provisions of the new ATIPP Act.

HIPMA

In 2018, we saw a slight increase in files opened under the *Health Information Privacy and Management Act* (HIPMA) over 2017. There were 33 files opened in 2018 as compared to 31 in 2017. The bulk of these files were complaints made against the Department of Health and Social Services (HSS) with a handful made against private sector custodians.

We found in our dealings with private sector custodians that some were not aware of their obligations under HIPMA, including our role. Much of our discussion with these custodians centered on educating them about HIPMA and supporting them to address any shortcomings identified through investigation. All were cooperative during the process and worked with us to evaluate how to achieve compliance. All complaints that we received in 2018 under HIPMA were settled by our informal case resolution team.

In 2018, I completed two consideration reports into complaints that were brought to us in prior years. The investigation of one of them demonstrated that the authority granted to Yukon's two largest custodians, HSS and the Yukon Hospital Corporation, to collect personal health information without consent bypasses the key measure of control in HIPMA which is consent. It was during this investigation that the impact of this provision became clear. This led me to research other health information privacy laws in Canada that are similar to HIPMA. I found that this is a unique authority not granted elsewhere. The consequences of this provision for individuals is that because consent is not required, an individual may not be informed that they have any choices regarding their personal health information. Unlike the ATIPP Act, there is no notice required in HIPMA to inform an individual about their rights, when information is collected.

The reason that notice is absent from HIPMA is that the laws on which HIPMA is modelled are consent-based, which means obtaining consent is the default for the collection, use or disclosure of personal health information. For obvious reasons, where consent is obtained, notice is not required. When HIPMA is reviewed, I will address this issue with those responsible for the review. A comprehensive review of HIPMA must be initiated by August 2020. One of my eight goals is to participate in the HIPMA review once it is initiated.

In 2018, my compliance review team began working closely with HSS on proactive privacy management. Establishment of Yukon's electronic health information infrastructure, plus its automation of activities within its many programs and services, generates a lot of proactive privacy work. The majority of the privacy impact assessments (PIAs) we reviewed this year came from HSS, which has done a significant amount of work to establish its privacy management program and is working effectively with our office on addressing privacy and security risks. Given the amount and sensitivity of personal health information processed by HSS, I am pleased about its willingness to work cooperatively with our office.

Also in 2018, I had an opportunity to meet with Yukon's Chief Medical Officer of Health. The Government of Yukon, like many other jurisdictions in Canada, needs access to information, which includes in some cases personal health information, to conduct research to improve health outcomes. The purpose of our meeting was to discuss how to design research databanks in a privacy-compliant way and how to conduct a privacy impact assessment on a system that is multi-layered. I was pleased to be consulted early on these matters, during the planning stages.

One of my goals is to support the development of effective privacy management programs by custodians. My focus for the coming years will be to provide resources that will assist private sector custodians to develop and implement these programs for small-scale operations. The communications support that I intend to acquire in 2019 will assist us to move this goal forward.

Information security concerns

Through our compliance review activities and investigations, we have evaluated the security of personal information processed in Yukon government electronic information systems.

In one investigation that we completed on Peoplesoft, which is used to process the personal information of all Yukon public servants (and others, including my office's employees), we found shortcomings that violated the security requirements of the ATIPP Act. As well, during consideration of a complaint made about the personal health information processed in an information management system operated by HSS, we found shortcomings that violated HIPMA's information security requirements. Ensuring information security is managed effectively is essential to protecting the privacy of personal information held by Yukon government public bodies and custodians.

Since I became Yukon's Information and Privacy Commissioner in 2013, I have recommended on numerous occasions the development of documented corporate-wide information security policies and procedures in the Yukon

government. According to the Yukon government's General Administration Manual (G.A.M.) 2.3 Information Technology Security Framework, the Information and Communications Technology (ICT) branch in the Department of Highways and Public Works is responsible for developing these policies and procedures.

The only documents that I am aware of created by the ICT branch in respect of information security are G.A.M. 2.3, two password protection policies, and the computer use guidelines.

G.A.M. 2.3 is not an information security policy. It is a framework designed to guide policy and procedure development. G.A.M. 2.3 states that it was developed in 2006 as a result of Auditor General of Canada reports, which had identified "on several occasions" the "lack of formal IT security policy or framework within the Government of Yukon…". The framework is based on ISO 17799 and is identified as "the government's standard reference and model for the development and implementation of this IT security framework." The ISO 17799 standards for information security were replaced in 2013 with ISO 27002.

In fiscal year 2014/15, the Yukon government's internal auditor audited the management of information security programs and the central leadership of the ICT branch. The conclusion reached by the auditor in respect of the framework in G.A.M. 2.3 was that "the Framework was designed according to a best practice standard that was current in 2006, although it had not been implemented as intended." The auditor recommended that the framework be updated and implemented. The report noted that "[t]he Yukon government continues to be exposed to risks as a result of shortfalls in the following areas: IT security governance, risk assessments, communications, network access, and measures to protect information and IT assets." ICT's response to the auditor's recommendation to update and implement the framework was to review G.A.M. 2.3 and to develop a process for the selection and approval of controls and their periodic review of relevance and performance. Information security controls generally include documented policies and procedures. The internal auditor's report was written four years ago and to my knowledge, the framework has not been updated, nor have any documented policies and procedures been developed. To its credit, the ICT branch did recently hire a chief information security officer (CISO).

Through our evaluation of these systems, we have identified other weaknesses that we have brought to the attention of chief information officers (CIOs) in departments, the CISO, and other employees within the ICT branch. Some of these weaknesses have been addressed and some not. We continue to be concerned that the Yukon government has not implemented the necessary information security controls to satisfactorily mitigate the risks to personal information.

I was informed during the development of the new ATIPP Act that its regulations would contain comprehensive information security requirements. I expect these will include a requirement for administrative controls that include documented policies and procedures as well as technical and physical controls to protect personal information. I am optimistic that these requirements, together with my ability to audit compliance with them, will allow me to examine more closely the nature of the information security risks and make recommendations for improvement.

Stories about some of our investigations and compliance review activities conducted under the ATIPP Act and HIPMA are contained in the section of this report entitled "Samples of our work in 2018". You will also find statistics about cases investigated in the section entitled "How we measured up in 2018". In closing, I hope you find the information in this annual report informative and useful.

Diane McLeod-McKay
Information and Privacy Commissioner

Ensuring Peoplesoft isn't soft on security

DAYNA, A PUBLIC SECTOR EMPLOYEE, CAME TO OUR OFFICE WITH CONCERNS ABOUT THE SECURITY OF AND ACCESS TO THE YUKON GOVERNMENT'S INFORMATION COMMUNICATIONS SYSTEM, WHICH IS CALLED PEOPLESOFT. DAYNA BELIEVED THAT PEOPLESOFT WAS BEING ACCESSED BY EMPLOYEES WHO SHOULD NOT BE VIEWING IT AND THAT THE SYSTEM'S SECURITY CLEARANCE WAS INADEQUATE. WE DECIDED TO CONDUCT A FORMAL INVESTIGATION.

The Information and Privacy Commissioner (IPC) assigned the case to two investigators, one with information technology and security expertise. The Public Service Commission (PSC), owner of Peoplesoft, asserted that it had authority to disclose employee personal information to Yukon government public bodies. In its view, it had a responsibility, which it was carrying out through Peoplesoft, to manage employees who work within these public bodies, or move between them during their government careers.

Our investigation revealed that employees, most of whom were responsible for human resources functions in all Yukon government departments and the Yukon Legislative Assembly, had access to the personal information of all employees, for management purposes. We found that the PSC had authority to disclose personal information about an employee to their home department. However, it had no authority to disclose this same information to other public bodies, or to the Legislative Assembly, because these entities had no responsibility for the employee.

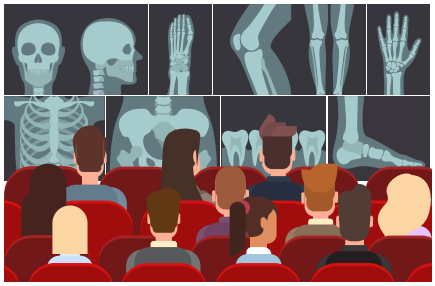
We recommended that the Public Service Commission limit public body access in Peoplesoft to only those employees for whom they have responsibility. Our investigation also revealed weaknesses in Peoplesoft that resulted in non-compliance with the security requirements of the *Access to Information and Protection of Privacy Act* (ATIPP Act). We recommended changes to address these weaknesses. The PSC accepted our recommendations and in early 2019, it started working with us to implement them. The Investigation Report about this complaint can be found on our website at www.ombudsman.yk.ca/reportATP16-22I.

This story demonstrates the importance of evaluating information communications systems for compliance with the ATIPP Act. Information communications systems store a considerable amount of personal information, including sensitive information. Mismanagement of this information can cause significant privacy breaches that can negatively impact large numbers of individuals. In providing their personal information to Yukon government public bodies, individuals expect that it will be managed in accordance with their rights under the ATIPP Act.

Collaboration is one way to ensure protection of personal health information

SULLY, WHO WORKED FOR AN EMPLOYEES' UNION, APPROACHED OUR OFFICE EXPRESSING CONCERNS ABOUT THE SHARING OF SENSITIVE PERSONAL INFORMATION OF YUKON GOVERNMENT EMPLOYEES BETWEEN YUKON GOVERNMENT DEPARTMENTS, FOR THE PURPOSES OF ACCOMMODATING EMPLOYEE HEALTH ISSUES. HAVING CONSIDERED THE NATURE OF THE COMPLAINT AND THAT IT HAD GOVERNMENT-WIDE IMPLICATIONS, WE DECIDED THAT THE BEST APPROACH TO EVALUATING COMPLIANCE WAS TO HAVE THESE DEPARTMENTS CONDUCT PRIVACY IMPACT ASSESSMENTS (PIAS) ON THE PROCESSES USED TO FACILITATE THIS ACCOMMODATION. TO DO SO, WE NEEDED THESE DEPARTMENTS TO AGREE TO THIS APPROACH, WHICH THEY DID.

Our office began working with the Public Service Commission (PSC) first. The PSC operates the government's disability management program. We met with a group of PSC employees on several occasions to learn their processes and evaluate where privacy management could be improved. We also evaluated any information security risks that arose to mitigate these risks. The PSC employees, including their senior management, worked extensively with us and the Yukon government's ATIPP Office on developing the PIA. As part of this, the PSC made a number of changes to how it conducted this program, including the forms used and access to information communications systems to operate the program. It also made commitments to improve access to information by employees involved in running the program. In addition, the PSC agreed to increase privacy training for these employees to ensure they have a clear understanding of their obligations under the *Access to Information and Protection of Privacy Act* (ATIPP Act). The PIA was completed in 2018 and accepted by our office.



The other Yukon government departments agreed to conduct a joint PIA and, through that process, to align their information management practices used for accommodation purposes. We are still working with them on their PIAs and have made significant progress. We anticipate that they will finalize their PIAs soon and that we will accept them.

This story demonstrates the importance of Yukon government departments that handle personal information to do so in accordance with the ATIPP Act. The unauthorized sharing of highly-sensitive personal health information can have devastating effects for individuals. I am pleased at the level of engagement from departments during the development of these PIAs, especially from the PSC.

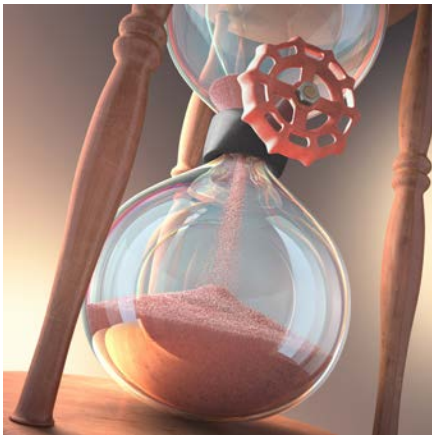
Requesting more time can be reasonable

RILEY CONTACTED OUR OFFICE TO REQUEST A REVIEW OF A DECISION BY THE GOVERNMENT OF YUKON RECORDS MANAGER TO GRANT AN EXTENSION OF TIME TO A PUBLIC BODY FOR RESPONDING TO AN ACCESS REQUEST. RILEY WAS CONCERNED THAT THE RECORDS MANAGER HAD EXTENDED THE TIME TO RESPOND WITHOUT THE AUTHORITY TO DO SO, AND WITHOUT PROVIDING REASONS FOR THE EXTENSION, CONTRARY TO THE *ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT* (ATIPP ACT).

In Riley's case, the public body had requested additional time citing that a large number of records needed to be searched and that meeting the time limit would unreasonably interfere with its operations.

The position of records manager is unique to the Yukon ATIPP Act legislation. Granting extensions of time for responding to a request is a discretionary power bestowed upon the records manager, who must demonstrate that discretion was exercised about whether to authorize the extension and also in respect of the length of the extension. If granting an extension, the records manager must tell the applicant the reason for extending the time and when a response can be expected.

After reviewing the evidence, our office agreed with the records manager's decision to extend the timeline for responding to Riley's access request. The records manager sufficiently established that a large number of records needed to be searched, and that due to unexpected technical challenges posed by the extraction and examination of the records, meeting the time limit would have unreasonably interfered with the operations of the public body.



Despite this determination, our office made some additional observations with regard to this case. We suggested that the records manager consider revising the letters sent to applicants notifying them of a time limit extension so that they include not only the provision of the ATIPP Act relied upon by the public body to request the extension, but also the detailed reason(s) for extending the time. We also suggested that the records manager consider taking tangible measures to ensure that all future responses provided to applicants are open, accurate and complete. This includes confirming that all relevant factors were considered and that they sufficiently exercised their discretion prior to granting the extension, and that this information is transparent to the applicant.

Lesson learned - taking action to avoid unnecessary delays

REESE FILED AN ACCESS REQUEST WITH THE DEPARTMENT OF JUSTICE (JUSTICE) AND WAS PROVIDED WITH THE RESPONSIVE RECORDS NINE DAYS PAST THE DEADLINE.

Reese reached out to our office to file a complaint regarding the administration of the *Access to Information and Protection of Privacy Act* (ATIPP Act), specifically, about Justice's unauthorized delay for responding to the access request.

During our investigation, Justice acknowledged the time lapse, explaining that an unexpectedly high volume of access requests combined with a staff shortage at the time, had caused a delay in responding to the access request, resulting in the missed deadline.

In response to our office's request for confirmation of what actions were being taken to avoid a recurrence of these circumstances, Justice committed to a number of measures, including hiring new staff; cross-training employees to ensure adequate coverage in the event of unforeseen leave; ensuring that open files are handed off to other employees in the case of scheduled leave; ensuring redundancy during absences; having the director provide back-up support during absences when necessary; ensuring that staff leave is managed in order to avoid gaps in coverage; and the authorization of overtime where required to ensure compliance with the ATIPP Act.

Upon review of the evidence, our office was satisfied that Justice had taken tangible action to reasonably avoid a recurrence.

When misunderstanding clouds perception about privacy

CAMERON CONTACTED OUR OFFICE EXPRESSING CONCERN THAT THE DEPARTMENT OF EDUCATION (EDUCATION) HAD ATTEMPTED TO IDENTIFY HIM (OR, COLLECT HIS PERSONAL INFORMATION) WITHOUT THE AUTHORITY TO DO SO UNDER THE *ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT* (ATIPP ACT).

Cameron had recently made an access request for information from Education. The information requested was not his own personal information and, as such, he had requested to remain anonymous throughout this process.

Cameron became concerned after two events involving employees from Education. First, during a visit to the Government of Yukon ATIPP Office to discuss his request, Cameron overheard a conversation between a worker at the ATIPP Office and an employee of Education. Cameron got the impression that an employee was attempting to ascertain his identity.

Later that same day, Cameron had a conversation with an outside party who reported they had received a call from someone at Education inquiring about a request for records. Cameron's assessment of this event was that Education was indirectly attempting to identify who had made his request for records.

Upon review of the evidence, our office discovered that Cameron's impressions were incorrect. Education established that one record was found to be responsive to Cameron's access request; however, this record contained personal information. Under the ATIPP Act, while individuals have a right of access to their own personal information, there are specified exceptions to the right of access to other individuals' personal information. In order to fulfill its duty to respond to the request "openly, accurately and completely" and within the required timelines, Education explained it had indeed reached out to the ATIPP Office to determine whether the personal information identified in the record belonged to the applicant (in this case, Cameron) or to a third party. Had the information been the applicant's own, Education could have released it immediately without needing additional time to consult or notify a third party. This situation is distinctly different than a department trying to ascertain someone's identity. As such, it was our office's determination that Education had acted in good faith by endeavoring to fulfill its duty to respond to the request as quickly as possible.

Regarding the second incident, our office confirmed that at no time during the conversation in question were any details regarding Cameron's access request discussed.

Upon review of the evidence, our office was satisfied that Cameron's personal information had not been collected by Education and that no violation of the ATIPP Act had occurred. Education accepted our recommendation to clarify with staff the processes for responding to access requests, in particular, that if an applicant asks to remain anonymous, under no circumstances should employees try to ascertain their identity, directly or indirectly.

The importance of accessing training on access

KELLY CAME TO OUR OFFICE AFTER RECEIVING A DECISION FROM THE DEPARTMENT OF TOURISM AND CULTURE (T&C) ABOUT HIS ACCESS REQUEST. KELLY WAS CONCERNED THAT HIS REQUEST WAS MISHANDLED BY T&C. SPECIFICALLY, HIS COMPLAINT WAS THAT THE SEARCH FOR RECORDS RESPONSIVE TO HIS REQUEST WAS NOT DONE CORRECTLY. THE INVESTIGATION OF THE COMPLAINT WAS ASSIGNED TO AN INVESTIGATOR IN OUR INFORMAL CASE RESOLUTION TEAM.

Our investigator found that the search conducted was not adequate; it was only done within a specific branch of T&C and it was not until much later that other branches or areas within T&C were identified as possibly having records responsive to the request. In addition, the investigator found several other deficiencies with the processing of the access request. The records manager failed to respond to the access request in the period required by the ATIPP Act; T&C failed to request an extension of time to respond, despite its ability to do so; the records manager failed to provide reasons for not fully responding to the access request; and T&C failed to identify third parties or other public bodies requiring consultation in a timely manner.

Sections 11 to 13 of the ATIPP Act require the records manager to respond to an access request openly, accurately and completely. Section 10 requires a public body, here T&C, to assist the records manager to respond as required by the Act. In this case, because T&C failed to manage the request properly, it meant the records manager also failed to meet obligations for responding.

- Failure to respond in time – In this case, the records manager had until August 4, 2017 to provide a response to Kelly. The first response was dated August 3, 2017, the second August 14, 2017, and the third October 27, 2017. All were marked "final", but the one that was in fact final was

the one dated October 27, 2017. In the records manager's first and second responses, they indicated what records were provided and the information redacted therefrom. T&C's first decision letter, which was appended to the first response letter, indicated that it was still reviewing records related to the access request that required third party consultation. The records manager was out of time as of August 4, 2017 because no extension was authorized to respond to Kelly's access request beyond that date. Despite this, the records manager continued delivering responses and records up to 2 ½ months past the deadline. As soon as time ran out for the records manager, any records not provided to Kelly by then are deemed refused by T&C. However, Kelly was never informed of this nor of his right to request a review by the Information and Privacy Commissioner (IPC) as a result of the deemed refusal.

- Failure to request an extension – If T&C could not meet the timelines for a response, which it could not in this case, it could have requested an extension from the records manager. The first decision letter provided to the records manager indicates T&C needed the extra time to conduct third party consultations. The records manager has authority to extend a deadline for response for this purpose. T&C did request one extension but did not request a second and was unable to provide the records manager with its decision on all the records responsive to Kelly's access request before the first extension expired. This left the records manager in contravention of obligations to provide a response within the specified period.
- Failure to provide reasons – The IPC made it clear in a Report issued in 2014 that the records manager is obligated to provide reasons for refusing access in their response. No reasons were provided in any of the responses given to Kelly by the records manager, nor are there any reasons for the information redacted from the records in T&C's decision letters appended to each response.
- Failure to identify third parties in a timely manner – The investigator determined that third parties were still being identified for consultation by T&C just days before the first deadline to respond, which led to the first request for extension that the records manager authorized. On this point, the investigator indicated that a public body must identify third parties at the earliest possible opportunity to allow for the necessary consultations to occur within the timelines.

T&C admitted that staffing issues and poor training contributed to the failures in processing Kelly's access request. The department acknowledged that protocol was not followed in this case and stated that "this appears to be the first time". It added that "the department practices the delivery of ATIPP requests on time, efficiently and giving the applicant the information that is requested."

To settle the investigation, two recommendations were made, which T&C accepted. The recommendations were to develop written policies and procedures on how to manage an access request and to ensure employees responsible for processing requests are adequately trained.

Voluntary breach reporting

In 2018, we received four breach reports under the ATIPP Act. All breaches reported to our office under this Act are voluntary. Three of the files we opened on breach reports stemmed from complaints by employees. Although this demonstrates that there is some knowledge amongst public body employees about what constitutes a breach, the lack of breach reporting to our office may be due to employees failing to recognize when a breach occurs. It may also mean that public bodies are simply choosing not to report them to us.

Our office has extensive experience investigating breaches of privacy and is, therefore, a valuable resource available for public bodies to learn how to prevent breaches and, if they do occur, how to mitigate consequences and prevent recurrence. In order to encourage breach reporting, we do not report specifics about breaches voluntarily brought to our attention.

Under the new ATIPP Act, there are a number of breach management requirements. For example, public bodies must adequately secure personal information against a breach. As well, there are penalties in the legislation for failure to meet its information security requirements. The new ATIPP Act also includes mandatory breach reporting to the Information and Privacy Commissioner in certain circumstances. In order to prepare for this new obligation, public bodies may wish to work with our office to manage breaches of privacy, in order to gain expertise in this area and prevent breach recurrences, before the new Act takes effect.

Being aware of your rights makes all the difference

SALLY VISITED OUR OFFICE TO EXPRESS CONCERN THAT HER AND HER CHILD'S PERSONAL HEALTH INFORMATION WAS DISCLOSED BY THE YUKON HOSPITAL CORPORATION (YHC) TO A HEALTH CENTRE OPERATED BY THE DEPARTMENT OF HEALTH AND SOCIAL SERVICES (HSS). HER COMPLAINT WAS THAT SHE DID NOT KNOW THIS HAD OCCURRED AND LEARNED ABOUT THE DISCLOSURE AFTER RETURNING TO HER COMMUNITY, WHEN SHE WAS CONTACTED BY AN EMPLOYEE OF THE HEALTH CENTRE WHO HAD DETAILED KNOWLEDGE ABOUT THIS PERSONAL HEALTH INFORMATION.

Our office attempted to settle the complaint with YHC but was unsuccessful. The complaint moved to adjudication and the Information and Privacy Commissioner (IPC) found that YHC had disclosed more of Sally's and her child's personal health information to the health centre than was authorized by the *Health Information Privacy and Management Act* (HIPMA). The IPC also found that because of a mandated procedure by HSS, which obligated YHC to disclose the personal health information to the health centres for post-partum follow-up care, YHC failed to exercise its discretion for the disclosure.

The IPC made a number of recommendations to address these matters. YHC refused one but accepted the rest. One of the recommendations that was accepted by YHC was to take reasonable steps to destroy the records containing Sally's and her child's sensitive personal health information, which was disclosed to the health centre. YHC's response was that it tried but that HSS refused. The IPC met with a representative of HSS and worked with them on the destruction process. After some discussion with the complainant, HSS agreed to destroy the records and did so.

Sally was satisfied with the outcome. The Consideration Report about this complaint can be found on our website at www.ombudsman.yk.ca/considerationHIP17-08I.

This story identifies the importance of communication by custodians responsible for the management of personal health information with individuals whose personal health information is collected, used, and disclosed. In this case, had Sally been aware that YHC was going to disclose the personal health information about her and her child to the health centre, she could have refused. Because she was not informed, she could not exercise her right of refusal under HIPMA. The result was that the information was disclosed without her knowledge and against her wishes. Custodians responsible for sensitive personal health information should evaluate their procedures to ensure individuals know what is happening with their information so they can effectively exercise their right to control it.

Collect only what you need, and no more

KALE CAME TO US WITH A CONCERN THAT THE INSURED HEALTH AND HEARING SERVICES (IHHS) BRANCH IN THE DEPARTMENT OF HEALTH AND SOCIAL SERVICES (HSS) WAS TRYING TO COLLECT HIS SENSITIVE PERSONAL HEALTH INFORMATION FROM HIS PSYCHIATRIST, IN ITS ATTEMPTS TO VERIFY BILLING. KALE WAS VERY CONCERNED ABOUT THIS AND WAS ALSO WORRIED THAT IHHS DID NOT HAVE ADEQUATE SECURITY TO PROTECT THIS PERSONAL HEALTH INFORMATION, ONCE COLLECTED.

This complaint began prior to the enactment of the *Health Information Privacy and Management Act* (HIPMA) so we dealt with it at first under the *Access to Information and Protection of Privacy Act* (ATIPP Act). Our first approach was to work with HSS to try to settle it, which was unsuccessful. When HIPMA came into effect, we lost jurisdiction for the complaint under the ATIPP Act. We let Kale know about this, and his decision was to make a complaint under HIPMA. We again tried to settle the complaint to no avail. The matter then came before the Information and Privacy Commissioner (IPC) for adjudication.

During her adjudication, the IPC encountered challenges in obtaining the evidence needed to properly consider the complaint. After numerous attempts to obtain the evidence, which were met with denials of the existence of the evidence, she conducted an oral inquiry so that she could question employees working in IHHS under oath. Through this process, she was able to obtain the evidence she needed to complete the adjudication.

The IPC's findings were that HSS was trying to collect more of Kale's personal health information than was authorized by HIPMA. She also found that the information security at HSS was not up to the standards required by HIPMA. The IPC made two recommendations, which were both accepted by HSS.

The Consideration Report about this complaint can be found on the office's website at www.ombudsman.yk.ca/considerationHIP16-02I.

The compliance review team in our office is now working with HSS on the processes used for collection of personal health information for billing purposes and the development of a privacy impact assessment (PIA) to address the security issues. We are confident that through this work the collection of personal health information for IHHS billing purposes will be limited as required by HIPMA and will be properly secured.

Is using personal health information your first choice or last resort?

VAL, AN EMPLOYEE OF EMERGENCY MEDICAL SERVICES (EMS) IN THE DEPARTMENT OF COMMUNITY SERVICES, CAME TO US WITH CONCERNS THAT HER PERSONAL HEALTH INFORMATION WAS SHARED WITH OTHER EMPLOYEES IN EMS WITHOUT HER CONSENT. THIS OCCURRED AFTER STAFF UNDERWENT TESTING RELATED TO THE POSSIBLE CONTAMINATION OF AN AMBULANCE OR PIECE OF EQUIPMENT.

Prior to coming to us, Val had taken her concern to EMS, which had investigated. EMS concluded that the information shared was not personal health information but indicated that if it was, the *Health Information Privacy and Management Act* (HIPMA) authorized the use of it without consent. The reason for this conclusion was that the information was used to prevent or reduce the risk of serious harm that it reasonably believed existed to the health or safety of other EMS employees. Val was not satisfied with the conclusion reached by EMS.

We investigated Val's concern and determined that the information shared was indeed Val's personal health information because the information identified her and it was information about her health. Although the information did not contain Val's name, with the knowledge employees had about the incident which led to the testing, it could easily identify Val. We also determined that EMS's position (that the information sharing was necessary to protect the health and safety of other employees) was not reasonable. Instead, we determined that it was possible, using safety protocols already in place in the workplace, to ensure the safety of other employees without the need to share Val's personal health information. We also determined that EMS did not have a process for making privacy complaints, nor did the branch provide information about how to make a complaint. HIPMA requires custodians to have a procedure to manage complaints and to make information publicly available about its information management practices.

We were able to settle the complaint with EMS. The branch agreed to write Val to acknowledge the unauthorized use of her personal health information and advise her of the steps taken to address the cause of the breach. It agreed to develop a procedure for communicating with EMS employees about possible contamination of an ambulance or equipment, which does not include the sharing of personal health information about the ambulance crew. It also agreed to develop a privacy complaint policy that sets out the steps and procedures related to receiving, investigating, and reporting to a complainant about complaints regarding the collection, use or disclosure of their personal health information. In addition, it agreed to develop an education module for the Learning Management System to follow up with the new policy's implementation.

HIPMA prevents custodians from using personal health information if other information will suffice. This case demonstrates the need for custodians to ensure they do not collect, use or disclose personal health information unless it is necessary to do so for a specified purpose. This case also demonstrates how important it is for custodians to have policy and procedures in place to manage complaints and to communicate the policy and procedures to the public.

To Skype or not to Skype

TERRI, A CITIZEN OF DAWSON CITY, CONTACTED OUR OFFICE AFTER LEARNING THAT A DAWSON PHARMACY WAS USING SKYPE TO COMMUNICATE THE PERSONAL HEALTH INFORMATION OF ITS CUSTOMERS. WE CONTACTED THE CUSTODIAN RESPONSIBLE FOR THE PHARMACY TO RAISE THIS CONCERN.

The custodian acknowledged that transmission of any health information that may identify an individual via Skype video chats or Skype text does not meet the security measures required by the *Health Information Privacy and Management Act* (HIPMA) to ensure the privacy and integrity of personal health information. The custodian informed us that pharmacy staff would be directed not to use Skype or any other non-secure method of transmission of personal health information. It also developed a written policy to that effect which all staff were required to acknowledge and sign off on. We informed Terri of the outcome and she was satisfied.

This story demonstrates the importance of only using secure communication methods to ensure the adequate protection of sensitive personal health information.

Mandatory breach reporting

In 2018, we received reports of three breaches under the *Health Information Privacy and Management Act* (HIPMA). Two involved the loss of personal health information stored in travel cases. Custodians are responsible to protect personal health information in their possession and to have proper safeguards in place to prevent a breach. We urge custodians to have policies and procedures for secure transportation and storage of personal health information and to train their employees on them. Records cannot be left unattended during transport unless they are properly secured. Wherever they are stored, they must be protected from theft, loss and unauthorized access.

One of these breaches involved a health facility that offers counselling services (a custodian). An agent of the custodian left a locked suitcase in a locked car. The car was broken into and the suitcase stolen. The suitcase contained an intake book and the agent was obligated to reconstruct the personal health information contained in the book and notify the affected individuals. The custodian worked with our office to update its policy and practices regarding the transportation and storage of records. It also agreed to train staff in this regard.

Another briefcase was stolen when a physician custodian made a stop on the way home from work at a public place. While there, the briefcase was stolen. Records containing personal health information were in the briefcase and only some of the records were recovered. The custodian had to notify the affected individuals and report the breach to our office. The custodian agreed to modify its practices regarding traveling with personal health information and to consolidate this practice into a written policy.

Although these breaches have been limited in scope in that only a few individuals were affected, a similar breach that occurred in the Northwest Territories in 2018 should be a warning for Yukon's custodians who travel with personal health information. That breach involved a theft of a car containing a laptop. The laptop contained the personal health information of an estimated 80% of the Northwest Territories' population. Personal health information is a valuable asset and is often offered for sale on the 'dark web'[1]. Identity fraud or extortion are risks that are associated with these sales.

No breaches of digital records were reported to our office under HIPMA in 2018. This is not necessarily a good sign. Many of Yukon's custodians process vast amounts of digital records, and it would be common that mistakes and incidents happen. It is possible that breaches occur that go undetected or are not reported as required by the law. We urge custodians to have an audit strategy in place for digital records to improve the chances of detecting breaches.

[1] The dark web is a special part of the Internet only accessible with an anonymizing web browser. Websites on the dark web offer, amongst other things, illegal goods and services for sale.

Outreach activities in 2018

This year we were invited to meet with a number of groups to educate them on the requirements of the *Health Information Privacy and Management Act* (HIPMA). We learned that those responsible to comply with this law want to learn how best to do so.

In 2018, we again went out and presented to students in grade six in Whitehorse schools on how best to protect their privacy when engaging in online activities. Although we were there to teach them, we learned a lot from them during our discussions, which helped us strengthen our presentation. Way to go kids! These presentations are always fun and we have a lot of laughs with the kids. We plan to continue this work in 2019.

The Information and Privacy Commissioner (IPC) was invited by members of the Yukon Legislative Assembly to provide witness testimony this year to MLAs on the new *Access to Information and Protection of Privacy Act* (ATIPP Act). The IPC spent several hours providing information and answering questions about the new Act. She shared her extensive knowledge, gained over 20 years in the fields of access and privacy, about the importance of privacy and access to information rights in these laws and those contained within the new Act. Afterwards, some members told the IPC that the information provided was informative and useful in their decision-making about whether the new ATIPP Act has the right balance of authorities, controls, and oversight to ensure the protection of these important rights.

Also in 2018, the IPC invited Toby Mendel from the Centre for Law and Democracy to speak to Yukoners about the importance of access to information rights. The "standing room only" event brought together those in Yukon responsible to administer the ATIPP Act for a discussion of these rights. We were pleased with the turnout, which included representatives from municipal governments who are not yet subject to access to information laws in Yukon.

HOW WE MEASURED UP IN 2018

Skills development

Staff in our office attended a number of presentations on privacy and information security to improve our knowledge and skill in these fields.

One of our staff attended a meeting, along with our colleagues from all the privacy commissioners' offices in Canada, with Canada Health Infoway (CHI) to provide input on the development of e-services delivered by CHI. CHI intends to roll out these services within all provinces and territories. As such, hearing our input is important to ensuring Yukoners' privacy rights are protected when these services are delivered here.

The Information and Privacy Commissioner (IPC) was invited to participate in several conferences and meetings in 2018. One meeting was about how to increase the ability of researchers to access personal health information for research purposes while also ensuring compliance with privacy laws. This meeting, held in Toronto, brought together specialists in a number of fields from across Canada for a discussion. This work is still underway.

The IPC also met with her counterparts in smaller jurisdictions in Canada and internationally to collaborate on how to best deliver on their respective mandates in small jurisdictions. Participants from Bermuda, Cayman Islands and Barbados joined the meeting and brought important and interesting perspectives to this work.

ATIPP Act - 2018 activity

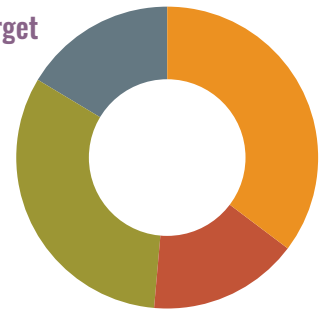
Resolved at intake - no file opened	
Requests for information	48
Informal complaint resolution	8
Non-jurisdiction	3
Referred-back	6
Total	**65**
Files opened by type	
Requests for review	62
Requests for comment	8
Complaint investigation	31
Requests for decision	2
Total	**103**
All files opened in 2018	103
Files carried over from previous years	53
Files closed in 2018	70
Files to be carried forward	**86**

ATIPP Act investigation (formal)- 1 year target

Closed (within 1 year)	2
Closed (over 1 year)	1
Still open (within 1 year)	0
Still open (over 1 year)	0

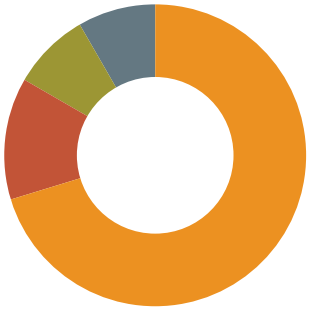
ATIPP Act investigation (settlement) - 90 day target

Closed (within 90 days)	11
Closed (over 90 days)	5
Still open (under 90 days)	10
Still open (over 90 days)	5



ATIPP Act review - 90 day target

Settled (within 90 days)	43
Still open (within 90 days)	8
Closed (over 90 days)	5
Not settled (formal hearing)	5



Files opened in 2018 by public body

Recommendations

Public body	Number of files							Formal*	Accepted	Not yet implemented (includes from prior years) or Failed to comply
	Complaints		Decision	Comments	Review	Inquiry	Total			
	Informal resolution	Investigation								
Department of Community Services	2	0	0	0	1	1	4			
Department of Economic Development	0	0	0	0	1	0	1			
Department of Education	3	1	0	1 - Privacy Breach	6	0	11			
Department of Energy, Mines and Resources	1	0	1	0	2	0	4			
Department of Environment	2	0	1	0	12	3	18			
Department of Health and Social Services	2	0	0	0	1	0	3			
Department of Highways and Public Works	1	0	0	1 - General	19	0	21			
Department of Justice	6	0	0	1 - PIA	7	0	14			1
Department of Tourism and Culture	1	0	0	0	0	0	1			
Executive Council Office	2	0	0	0	0	0	2			
Public Service Commission	4	0	1	0	1	0	6	17	17	15
Yukon Hospital Corporation	0	0	0	0	2	0	2			
Yukon Housing Corporation	1	0	0	0	1	0	2			
Yukon Liquor Corporation	2	0	0	5 - PIA	3	0	10			
Yukon Workers' Compensation Health and Safety Board	3	0	0	0	1	0	4			

*Formal recommendations are those made by the IPC in an Inquiry or Investigation Report issued in 2018.

Photo: Government of Yukon

ATIPP Act compliance review activities

Public body	PIA submitted, year submitted	Status A - Accepted NYA - Not Yet Accepted NR - No Review
Department of Community Services	Building Safety, 2015	NYA
	Personal Property Security Registry, 2015	A
	Yukon Corporate Online Registry (YCOR), 2015	NYA
Department of Education	ASPEN, 2015	NYA
	Challenge Day Program, 2015	NYA
	Google Apps, 2015	NR
	Education Employment Assistance Database, 2012	NR
Department of Environment	Electronic and Online Licensing System, 2015	NYA
Department of Finance	Online Accounts Receivable Payments, 2016	NYA
Department of Health and Social Services	Pioneer Utility Grant Program, 2015	NYA
	Electronic Incident Management Report Program, 2014	NYA
	Panorama, 2013	NYA
Department of Highways and Public Works	Simple Accommodation Cases, 2017	NYA
	Online Vehicle Registration Renewal, 2016	NYA
	Access to Information Program, 2015	NYA
	Government Services Account, 2015	NYA
	Motor Vehicles IDRIV system, 2014	NR
Department of Justice	Forum for Operational Collaborative and United Services Table (FOCUS project), 2018	NR
	Land Titles Registration, 2016	NYA
	Video Surveillance System, 2016	NYA
Public Service Commission	Disability Management and Accommodation, 2017	A
Yukon Hospital Corporation	HIS Connect – Lab Information System PIA, 2014	NYA
Yukon Liquor Corporation	BARS-C, 2018	NYA
	BARS-L, 2018	NYA
	Cannabis e-Commerce, 2018	NYA
	Cannabis Video Surveillance, 2018	NYA

HIPMA compliance review activities

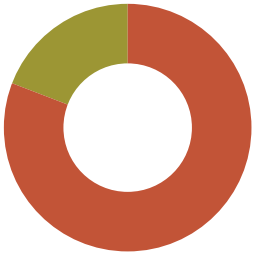
Custodian	PIA submitted, year submitted	Status A - Accepted NYA - Not Yet Accepted O - Other, PIA not yet provided, retracted or project on hold or being replaced
Department of Community Services	Electronic Patient Care Records (ePCR), 2018	NYA
Department of Health and Social Services	Aladtech Scheduling Software, 2018	NYA
	Community Nursing Logbook, 2018	NYA
	Chronic Disease Management Toolkit, 2017	NYA
	GENIE, 2017	NYA
	Medigent - claims processing, 2017	NYA
	Virtual Home Visits Pilot Project, 2017	NYA
	Vitalware, 2017	NYA
	e-health client registry with Plexia addendum, 2016	NYA
	Medigent - Drug Information System, 2016	NYA
	Yukon Home Health Monitoring Pilot Project (COPD), 2016	NYA
	Yukon Take-Home Naloxone Program, 2016	NYA
	Lab Information System (LIS) Connect Phase 1, 2015	NYA
Yukon Hospital Corporation	Meditech, 2017	NYA
	eHealth Client Registry, 2016	NYA
	Lab Information System (LIS) Connect Phase 2, 2016	NYA

HIPMA - 2018 activity

Resolved at intake - no file opened	
Request for information	9
Informal complaint resolution	2
Non-jurisdiction	1
Referred-back	3
Total	**15**
Files opened by type	
Consideration files opened	21
Request for comment	8
Request for advice	4
Total	**33**
All files opened in 2018	33
Files carried over from previous years	22
Files closed in 2018	22
Files to be carried forward	**33**

Consideration informal – 90 day target

Settled (within 90 days)	17
Still open (within 90 days)	4
Not settled (formal hearing)	0



Files opened in 2018 by custodian

Custodian	Number of files					Recommendations		
	Complaints		Comments	Request for advice	Total	Formal*	Accepted	Not yet implemented (includes from prior year) or failed to comply
	Informal resolution	Consideration						
Department of Community Services – Emergency Medical Services	1	0	2 - Privacy breach 1 - PIA	0	4			
Department of Health and Social Services	15	0	3 - PIA 1 - Privacy breach	1	20	2	2	
Health Facility – Counselling	1	0	0	0	1			
Health Facility – Optometry	0	0	0	1	1			
Health Facility - Other	0	0	0	1	1			
Pharmacy	1	0	0	0	1			
Physician	3	0	1 - Privacy breach	1	5			
Yukon Hospital Corporation	0	0	0	0	0	4	3	

*Formal recommendations are those made by the IPC in a Consideration Report issued in 2018.

Yukon
Public Interest
Disclosure
Commissioner

2018 ANNUAL REPORT OF THE YUKON PUBLIC INTEREST DISCLOSURE COMMISSIONER

The Honourable Nils Clarke
Speaker, Yukon Legislative Assembly

Dear Mr. Speaker:
As required by section 43 of the *Public Interest Disclosure of Wrongdoing Act*, I am pleased to submit the Annual Report of the Public Interest Disclosure Commissioner for the calendar year 2018.

I am also pleased to share this with the Yukon public.

Kind regards,

Diane McLeod-McKay,
Yukon Public Interest Disclosure Commissioner

Photo: Government of Yukon

A YEAR IN REVIEW

I am pleased to submit my 2018 Annual Report under the *Public Interest Disclosure of Wrongdoing Act* (PIDWA).

This year we saw a significant increase in PIDWA cases. In 2018, we opened 14 cases whereas in 2017 there were just two. This amounts to a 600% increase in cases. The cases we opened involved four different public entities. The statistical information about these cases can be found in the "Accountability" section of this annual report.

Cases received under PIDWA have proven to be large and complex; they take a significant amount of resources to investigate. These cases have significantly taxed the resources in my office and our ability to deliver on all our mandates. In one of the investigations, which involved two disclosures, I had to retain the assistance of an expert on the United Nations Convention on the Rights of the Child. This was an extremely challenging investigation and required the evaluation of thousands of documents and interviews with a number of witnesses. I intend to table my Special Report on this investigation in the Yukon Legislative Assembly in 2019.

During this investigation, it became apparent that there is a significant difference of opinion between the Department of Justice and our office about the authority of the Public Interest Disclosure Commissioner (PIDC) to obtain evidence. Our requests for evidence were met with numerous legal challenges, which served only to increase the complexity and length of the investigation. In my Special Report about this investigation, I made an observation about this issue.

Two of this year's disclosures were made about the Department of Health and Social Services (HSS). We received these disclosures in April 2018. The investigation of these disclosures was ongoing at the end of 2018 and will be complete in 2019. We had hoped to complete the investigation sooner given the seriousness of the allegations. However, this was prevented by the challenges we experienced obtaining evidence.

The other three disclosures were made against the Yukon Hospital Corporation. These investigations are underway.

Two of the three complaints of reprisal were made against HSS. These investigations are also underway.

Communicating PIDWA's disclosure procedures and reprisal protection

In my 2017 Annual Report, I highlighted the need for public entities to ensure that employees are aware of the disclosure requirements and reprisal protection in PIDWA. In 2018, when stories about the care of children in group homes was reported in the media, it was evident, based on the activity that followed, that the procedures to disclose a wrongdoing under PIDWA are not clearly understood. To ensure that the disclosure requirements that are directly linked to reprisal protection were followed, I issued a news release explaining the process to be followed when making a disclosure of wrongdoing.

As a result of the confusion that continues to exist around these procedures, I am again reminding chief executives of public entities of their obligation under section 7 of PIDWA to widely communicate disclosure procedures to their employees. Employees who fail to follow the procedures for making a disclosure under PIDWA are at risk of losing the reprisal protection afforded them under this Act. In my view, this is serious. I am pleased to report that I was informed by the Public Service Commissioner that the Public Service Commission (PSC) is creating a guidance document for use by chief executives of public entities to meet their section 7 requirements. This should serve to mitigate these risks.

To assist in raising awareness about PIDWA, I have included information in this annual report about what a disclosure is, disclosure procedures, and the role of my office.

PIDWA's impact on office resources

When PIDWA was brought into effect, I received no increases in funding or resources. In my office, I have three employees dedicated to intake and informal case resolution. This team fielded over 200 contacts and resolved 141 cases in 2018. I have just one employee dedicated to investigations, of which there were 12 this year. Eight of those investigations are under PIDWA, and are, as previously indicated, extremely complex and time-consuming. My one other employee is dedicated to compliance review activities. This individual carries over 70 open files. In my combined roles of PIDC, Information and Privacy Commissioner, and Ombudsman, I support investigations and compliance review activities in addition to my other work, which includes all adjudications under the *Access to Information and Protection of Privacy Act* and the *Health Information Privacy and Management Act*, and my operational duties.

My ability to perform the obligations under my four mandates is being significantly impacted by our lack of resources. I brought this matter to the attention of the Yukon Legislative Assembly's Member Services Board (MSB) as part of my 2019/20 budget submission, where I also described my inability to deliver on my mandates under each law to raise awareness about the Acts. In my budget submission, I requested an additional

resource and additional budget dollars. I am pleased to report that my request was approved. The new resource that I will recruit in the spring of 2019 will be dedicated to investigations, which will increase my ability to complete investigations in a timely manner. I will use the additional budget dollars that I receive to help meet my other mandated duties, including raising awareness.

Update on goals

In my 2017 Annual Report, I established eight goals for my second term, which began in June 2018. Three of these goals relate to PIDWA.

My first goal is to increase understanding of PIDWA's disclosure procedures and reprisal protection. Once the guidelines are developed by PSC as discussed above, we will work with the PSC to ensure the guidelines align with the disclosure procedures set out in PIDWA, and as necessary, assist with their implementation. We will also reach out to employees of public entities through their unions and other associations to inform them about disclosure procedures and reprisal protection. This work will also contribute to meeting my second goal relating to PIDWA, which is to increase awareness of the obligations of entities subject to PIDWA and inform employees about how to make disclosures and ensure reprisal protection. Along with this work, we will create additional resources as necessary.

My third goal is to participate in the review of PIDWA, which, according to the legislation, must occur before June 2020. We will add this work to our strategic plan to ensure our comments are received as part of the review. There are some areas of this law that, in my view, need to be amended to ensure its purposes are achieved.

I hope you find the information in this 2018 Annual Report informative and useful.

Diane McLeod-McKay
Public Interest Disclosure Commissioner

What employees need to know to make a disclosure under PIDWA

The primary purpose of PIDWA is to provide a tool that employees of Yukon public entities can use to disclose wrongdoings without reprisal repercussions. As long as you, the disclosing employee, follow the disclosure rules, you will be protected from reprisal. If you don't follow PIDWA rules when making a disclosure of wrongdoing, you run the risk of not receiving this protection. It's important for you to know that even if you just need advice in deciding whether to make a disclosure or not, PIDWA protects you.

So what are the rules? I've summarized them below, although I also encourage every employee to review the legislation. It's relatively short and not overly complicated. A link to PIDWA can be found on our website at www.ombudsman.yk.ca/pidwa-act.

Disclosure rules

1. You must be an employee of a public entity to report a wrongdoing. You can also be a former employee who suffered a reprisal and was terminated by a public entity. In addition, you can be a contract employee but not a 'fee-for-service' contractor. The 24 public entities covered by PIDWA in Yukon are shown in a table on page 31.
2. You must have a reasonable belief that a wrongdoing is being or may be committed.
3. Your disclosure must be made in good faith.
4. You must ***only*** disclose a wrongdoing to:
   - a supervisor (i.e. your immediate supervisor or chief executive)
   - the designated officer, if one exists in your public entity, or
   - the Public Interest Disclosure Commissioner (PIDC).
5. You must make your disclosure in writing and it must include, if known, the following information:
   - a description of the wrongdoing
   - the name of the individual(s) alleged to have committed, or who may be about to commit, the wrongdoing
   - the date of the wrongdoing
   - whether the disclosure has been made to someone else (for example, if you disclosed to your immediate supervisor, did you also disclose to your chief executive or the PIDC) and what response was received
   - other information, if prescribed (there are currently no regulations prescribing additional specifics), and
   - any other information the person receiving the disclosure identifies as reasonably necessary to investigate the allegation.

When making a disclosure directly to your public entity, be sure to inform them that you are making a disclosure under PIDWA, so it is clear what your intentions are. I strongly recommend that you obtain advice prior to making any disclosure. This advice can be obtained from your immediate supervisor or chief executive, a designated officer, or the Public Interest Disclosure Commissioner.

Disclosing in urgent situations

If you believe there is an imminent risk of substantial and specific danger to the life, health or safety of individuals, or to the environment, and there is not enough time to make a disclosure using the above procedure, you may make a disclosure to the public ***only*** if:

- you make the disclosure to the appropriate law enforcement agency
- you follow any direction the law enforcement agency issues, and
- immediately following the disclosure, you notify your supervisor or, if one exists, your designated officer.

You are not allowed to disclose to the public any information that is subject to a restriction created by a Yukon or federal law.

Additional limits on information disclosure

When making any disclosure, you are not allowed to disclose the information described in subsection 15 (1) "Cabinet confidence" of the ATIPP Act unless the circumstances in subsection 15 (2) exist. You must also limit the amount of personal information disclosed to that which is necessary to make the disclosure. The ATIPP Act can be found at www.gov.yk.ca/legislation/acts/atipp_c.pdf.

How public entities can help ensure employees are protected by PIDWA

Chief executives of public entities are required by PIDWA to ensure information about the legislation is widely communicated to their employees.

For those public entities that have not adequately informed their employees about PIDWA, there is a risk that employees may inadvertently make disclosures contrary to the requirements of PIDWA. There is also a serious risk that staff are receiving disclosures but are not recognizing them as a disclosure under PIDWA. As a result, they may steer the disclosing employee down an incorrect path. In either case, the employee may pay the price for the failure of public entities to inform them adequately about the legislation.

It is very important that staff receiving a disclosure, or what may appear to be a disclosure, first apply it to PIDWA before making any other determination, such as a process under another piece of legislation, an employment agreement or an applicable policy. Given this, I strongly encourage chief executives to take proactive steps this year to ensure their employees are well informed about PIDWA.

For those public entities that are drafting disclosure procedures, I strongly recommend that these procedures be geared solely to employees, as they are defined in PIDWA, so that the rules employees must follow for PIDWA reprisal protection are clear. A public entity that creates disclosure procedures that apply to more than just PIDWA-defined employees, no matter how well-intentioned, runs the risk of failing to clarify exactly what rules employees must follow to be afforded PIDWA protection.

How reprisal protection works should be clarified in any policy or communication provided to staff to ensure that they know about these procedures and their rights.

Disclosure procedures in public entities and 'designated officers'

No public entity has developed disclosure procedures under PIDWA and therefore, a disclosure cannot be made to a 'designated officer' within a public entity. Instead, any disclosure made within a public entity, as opposed to the Public Interest Disclosure Commissioner (PIDC), must be made to an employee's supervisor. Under PIDWA, that is either the chief executive or the employee's immediate supervisor.

Accountability

Skills development

In 2018, the lead investigator for PIDWA investigations attended a national meeting held in Quebec with our counterparts from across Canada who are responsible for similar legislation. At these meetings, we share our collective experience in conducting investigations under these laws, including beneficial learnings to improve our performance.

PIDWA - 2018 activity	
Resolved at intake - no file opened	
Requests for information	8
Informal complaint resolution	0
Non-jurisdiction	3
Referred-back	0
Total	**11**
Advice files opened	6
Comment files opened	0
Disclosure files opened	5
Reprisal files opened	3
Totals	14
All files opened in 2018	14
Files carried over from previous years	2
Files closed in 2018	8
Files to be carried forward	8

Disclosure of wrongdoing – target 1 year

Closed (within 1 year)	0
Closed (over 1 year)	0
Still open (within 1 year)	5
Still open (over 1 year)	0

Reprisal complaint – target 1 year

Closed (within 1 year)	1
Closed (over 1 year)	0
Still open (within 1 year)	2
Still open (over 1 year)	0

2018 PIDWA reporting

Public entity	Letter sent by PIDC	Response received	Disclosures to report	Reprisals to report
Chief Electoral Officer	21-Dec-18	08-Jan-19	0	0
Child and Youth Advocate	21-Dec-18	24-Jan-19	0	0
Department of Community Services	21-Dec-18	03-Jan-19	0	0
Department of Economic Development	21-Dec-18	09-Jan-19	0	0
Department of Education	21-Dec-18	15-Jan-19	0	0
Department of Energy, Mines and Resources	N/A	05-Feb-19	0	0
Department of Environment	21-Dec-18	25-Jan-19	0	0
Department of Finance	21-Dec-18	14-Jan-19	0	0
Department of Health and Social Services	21-Dec-18	25-Jan-19	1*	0
Department of Highways and Public Works	21-Dec-18	25-Jan-19	0	0
Department of Justice	21-Dec-18	09-Jan-19	0	0
Department of Tourism and Culture	21-Dec-18	08-Jan-19	0	0
Executive Council Office	21-Dec-18	03-Jan-19	0	0
French Language Services Directorate	21-Dec-18	04-Feb-19	0	0
Public Service Commission	21-Dec-18	08-Jan-19	0	0
Women's Directorate	21-Dec-18	21-Dec-18	0	0
Yukon College	21-Dec-18	None		
Yukon Development Corporation	21-Dec-18	16-Jan-19	0	0
Yukon Energy Corporation	21-Dec-18	11-Jan-19	0	0
Yukon Hospital Corporation	21-Dec-18	None		
Yukon Housing Corporation	21-Dec-18	08-Jan-19	0	0
Yukon Legislative Assembly	21-Dec-18	08-Jan-19	0	0
Yukon Liquor Corporation	N/A	21-Dec-18	0	0
Yukon Workers' Compensation Health and Safety Board	21-Dec-18	11-Jan-19	0	0

*The Department of Health and Social Services provided the following information about the disclosure that it reported.
For the Department of Health and Social Services, there was one disclosure of six allegations of wrongdoing to a supervisor or designated officer. This was acted on through an investigation led by an external investigator (Pamela Costanzo).
The investigation determined that there was one allegation of mistreatment of a youth, in breach of law and department policy. The corrective actions included a public apology and further incident review.

Files opened in 2018 by public entity

Public entity	Disclosure	Reprisal	Advice	Total	Recommendations: Informal*	Recommendations: Formal
Department of Community Services			1	1		
Department of Health and Social Services	2	2	2	6		
Department of Highways and Public Works		1	1	2		
Yukon Hospital Corporation	3		2	5		

*Formal recommendations are those made by the Public Interest Disclosure Commissioner in a formal Investigation Report issued in 2018.

Recommendations made in prior years that are not yet implemented

Public entity	Number of recommendations	Date of recommendation	Timing of implementation	Overdue
Department of Highways and Public Works	11	August 3, 2017	Spring 2019 – Spring 2022	None

Yukon Ombudsman

Yukon Information and Privacy Commissioner

Yukon Public Interest Disclosure Commissioner

OFFICE OF THE OMBUDSMAN, INFORMATION AND PRIVACY COMMISSIONER, AND PUBLIC INTEREST DISCLOSURE COMMISSIONER

Financial report

The budget for the Office of the Ombudsman, Information and Privacy Commissioner (IPC), and Public Interest Disclosure Commissioner (PIDC) covers the period from April 1, 2018 to March 31, 2019.

Operations and maintenance (O&M) are expenditures for day-to-day activities. A capital expenditure is for items that last longer than a year and are relatively expensive, such as office furniture and computers.

Personnel costs comprise the largest part of our annual O&M budget and include salaries, wages, and employee benefits. Expenses described as "other" include such things as rent, contract services, supplies, travel, and advertising.

For accounting purposes, capital and personnel expenses are reported jointly for the office. The "other" budget is the operational costs required for the Ombudsman to carry out the mandated responsibilities under the *Ombudsman Act*, the IPC to carry out the mandated responsibilities for the *Access to Information and Protection of Privacy Act* and the *Health Information Privacy and Management Act*, and the PIDC to carry out the mandated responsibilities of the *Public Interest Disclosure of Wrongdoing Act*. These costs are required to be accounted for separately under the law and, therefore, are reported separately. The budget dollars for PIDC operations were reallocated from the operations budgets of the Ombudsman and IPC in 2017/18 and 2018/19.

Our personnel budget increased slightly in 2018/19 to provide staff with a small increase in line with public servants. Our capital budget increased slightly to replace and manage our information technology. The O&M costs increased for the Ombudsman and PIDC by $4,000 in total to account for additional hardware or software needs and for professional contracting.

2018/19 Budget			
Personnel	Joint	$	944,000
Capital	Joint	$	13,000
Other	Ombudsman	$	107,000
Other	IPC	$	131,000
Other	PIDC	$	69,000
Total		**$**	**1,264,000**

2017/18 Actual expenditures			
Personnel	Joint	$	836,303
Capital	Joint	$	3,783
Other	Ombudsman	$	62,310
Other	IPC	$	102,689
Other	PIDC	$	17,813
Total		**$**	**1,022,898**