Access to Information and Protection of Privacy Act (ATIPPA)
Statutory Review 2020
Office of the Chief Information Officer's Response

The Office of the Chief Information Officer (OCIO) has reviewed the Terms of Reference provided by the Review Committee and have divided the response in two sections; ATTIP Coordinator's Operational Processes and Considerations Specific to the OCIO. Operational responses are in relation to the ATIPP Coordinator's issues of processing requests while the latter is the OCIO's ability to effectively respond and provide responsive records.

SECTION 1: ATTIP Coordinator's Operational Processes:

The following areas relate to the OCIO's ATIPP Coordinator's experience in using and administering the *ATIPPA*, 2015.

1. ***An examination of the request for extensions/disregards process to the Office of the Information and Privacy Commissioner***

   a. Section 23 – Extension of time limit is the section ATIPP coordinators apply when they require an extension for responding to a request. In this scenario, the clock is still running while the coordinator is creating the time extension submission for the OIPC. The requirement of preparing an extension submission on an already limited timeframe is challenging for coordinators since obviously time is of the essence. With legislated ATIPP timelines for responding, the ATIPP Coordinator now has to put time toward preparing an extension request for the OIPC, which includes a rationale for the extension. To prepare an extension request to the OIPC would usually take 2-3 days of preparation, depending on the request. This time is now being taken away from working on the actual request. If an extension is not granted, the coordinator has lost an additional 2-3 days in preparation of the extension request.

      Recommendation: It is recommended that, once the coordinator has expressed to the OIPC that they are going to request an extension, the clock would not run for the few days it takes to prepare the extension request. Once a decision is made, time will resume.

   b. Section 21 – Disregarding a Request is the section ATIPP Coordinators apply when, within 5 business days after receiving the request, they apply for an approval to disregard an ATIPP request. The requirement of preparing a disregard request is challenging for coordinators already operating on a limited timeframe. With legislated ATIPP timelines for responding, the ATIPP Coordinator now has to put time toward preparing an application for disregard to the OIPC, which includes a rationale.

      Additionally, an expedited process should apply to applicants who make unduly repetitive requests or otherwise abuse the ATIPP request process. In particular, unduly

repetitive applicants should only require a short submission to the OIPC, which would include evidence of past requests for disclosure, to substantiate that their request has already been addressed.

Recommendation: It is recommended that, once the coordinator has expressed to the OIPC that they are going to request a disregard, the clock would not run for the few days it takes to prepare the disregard request. Once a decision is made, time will resume. Additionally, an expedited process should apply to requests from applicants who abuse the ATIPPA request process.

2. ***Public body response times for access requests and whether the current ATIPPA, 2015 requirements for response and administrative times are effective***

   a. Section 11 – Making a Request is the section that requires a request to be in sufficient detail so that an employee familiar with the records can identify and locate the records using reasonable efforts. In some situations, the ATIPP request is not clear and the ATIPP Coordinator requires additional information or clarification from the applicant before they can proceed with fulfilling the request. If the applicant does not respond to the request for clarification in a timely manner, valuable processing time is lost awaiting a response.

      Recommendation: It is recommended that, the clock would not run for the time that is required to clarify an ATIPP request from the applicant. Once clarification is provided, time for a response will resume.

3. ***Public and public body experience in using and administering the ATIPPA, 2015 to access information in the custody or control of public bodies in Newfoundland and Labrador and opportunities for improvement***

   Government periodically calls a commission of inquiry to address events of significant public interest. Throughout the inquiry process, ATIPP coordinators are heavily involved in the collection and assessment of relevant records. It would be unnecessarily repetitive for ATIPP requests to be completed on these records during the inquiry. All public ATIPP requests in relation to the subject matter of the inquiry should be temporarily put on hold until the final inquiry report is released.

   Recommendation: It is recommended that, an appropriate communication be prepared to confirm that ATIPP requests made in relation to the subject matter of an inquiry be temporarily put on hold until the final inquiry report is released.

SECTION 2: Considerations Specific to the OCIO

The following areas relate to issues and concerns raised by the OCIO in its ability to effectively respond and provide responsive records in accordance with *ATIPPA*, 2015, while maintaining effective working relationships with third parties.

1. ***Whether there are any categories or types of information (personal information or otherwise) that require greater protection than the ATIPPA, 2015 currently provides***

   a. Section 31(1)(l) – Disclosure harmful to information technology security the OCIO requires the strengthening and clarification of the language of section 31(1)(l) of the *Act* to ensure the security interests of government IT assets and government information are protected.

   Section 31(1)(l) of *ATIPPA*, 2015 states:

   > *31(1) "The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to*
   >
   > *(l) reveal the arrangements for the security of property or a system, including a building, a vehicle, a computer system or a communications system;"*

   There is minimal language within the *Act* that enables the OCIO to ensure information technology (IT) security related information is protected from unauthorized disclosure. Section 31(1)(l) is the only option to maintaining the confidentiality of IT security-related records. As such, the language in that section is essential to the ability to maintain the security of government IT assets and government information.

   The unauthorized disclosure of operational IT security information has shown to result in cyberattacks that affect the confidentiality, integrity, or availability of government networks, systems, and data. The National CIO Subcommittee on Information Protection (NCSIP) has written a position paper titled "Protecting Sensitive Information throughout the Access to Information and Privacy (ATIP) Process", which states: "*...several types of cybersecurity information has been identified to be harmful in disclosing during an access to information request. These information disclosures includes: records containing details about IT infrastructure, network addressing or hostnames, and user identifiers (user ID's) that form half of the credentials needed to access systems.*"

   NCIP also states: "*Records containing details about IT infrastructure may include key information related to the location of critical infrastructure and the security controls in place to protect it. Records may include network addressing or hostnames, which, if disclosed, will result in additional unauthorized access attempts. Records may also include user identifiers (userids) that form half of the credentials needed to access systems. Once cybersecurity threat actors are in possession of this information, there is an increased probability of attack and increased likelihood the attack will be*

successful. Once attackers gain unauthorized access to one system they can use this access to gain access to additional systems holding sensitive information. Examples of sensitive information include credentials, IP addresses, hostnames, other system identifiers, vendor and technology names, versions, and network configurations and diagrams among others."

Additional information to withhold - network diagrams, file paths, directory structures, vulnerabilities, technology vendors and versions, and other system configuration information that aid attackers." NCIP

The OCIO contacted its independent 3rd Party Security Assessor (Electronic Warfare Associates Ltd. - EWA), who are experts in IT security. EWA notes that:

- once individuals are in possession of this information or a combination of such information, there is an increased probability of a cybersecurity attack and increased likelihood the attack would be successful
- once attackers gain unauthorized access to one system, they can use this access to gain access to additional systems holding sensitive information
- security and technical information should not be disclosed that would be subsequently used by cybercriminals to compromise the network and information assets.

Section 6 of the *Management of Information Act* requires a public body to protect government records. The disclosure of IT security related information would be contrary to the requirement to protect government records. The OCIO has made significant information management and protection investments and put controls in place to prevent unauthorized or inappropriate access or use of government's network and its information assets. These would include the Password Management Directive, Password Management Standard and Acceptable Use of the Government Network and/or Information Technology Assets Directive.

Cyberattacks occur all the time, to large, very well-protected organizations. If a cybercriminal were to access or manipulate personal and confidential government information, the harm to government's reputation would be significant. This has been experienced by other provincial jurisdictions who have fallen victim to social engineering attacks.

Recommendation: Based on the position and best practices of security professionals across the country, including the OCIO, it is recommended that stronger, more inclusive language be included in the ATIPP legislation to provide for the protection from disclosure of information respecting government's IT systems. This would be accomplished by having a separate section in ATIPP legislation dedicated to IT security protection.

2. *An examination of exceptions to access as set out in Part II, Division 2 of the Act*

The ability of ATIPP coordinators to efficiently and effectively review and assess third party information is dependent on the use of sections 19, 39 and 43. These sections limit the ability of a public body to consult with third parties as to the nature of their business or other proprietary information respecting its potential disclosure.

a. Section 19 – Third party notification is problematic since coordinators are not versed in what is and isn't proprietary information for other entities. Only the third party vendors are subject matter experts in their company records. Coordinators would need to engage the third party to determine sensitive areas of information that, if released, could be harmful and the reason why. Coordinators releasing third party information without consultations could not only cause harm to the third party, but cause harm to relationships between GNL and outside entities.

b. Section 39 – Disclosure harmful to business interests of a third party requires a three-parts harm test to be satisfied before this exemption can be applied to records. When third parties submit records to GNL, they usually have some indication of confidentiality on the submission, but not always in specific areas, more of a general idea of confidentiality. This becomes problematic during an ATIPP request since ATIPP coordinators are not familiar with what is considered proprietary confidential information. The third party would be the subject matter expert and would need to be consulted prior to a decision being made as to what information would be harmful if released. If the public body is unable to consult with the third party prior to the release decision, the public body is then in the difficult situation of deciding whether to release the information or to update the third party of the release.

   This situation is particularly problematic with respect to Requests for Proposals. The GNL is requesting vendors in RFP competitions to provide information on why they should be the successful proponent. This would require the vendor providing proprietary business information. Vendors could be reluctant to provide such information if they were not confident the information would be protected from disclosure should an ATIPP request be made. This has the potential to have a negative impact upon the information shared by vendors with GNL.

c. Section 43 – Burden of proof is the section that applies the burden on the head of a public body to justify its decision whether to grant a right of access to information. It is challenging for a public body to determine if it can satisfy the burden if it cannot consult with a third party on the nature of the information at issue. The burden of proof should not be on the head of the public body to prove that the disclosure of information is contrary to the *Act* when the information belongs to a third party.

Recommendation: It is recommended that the *Act* provide flexibility to public bodies to permit notification and the ability to consult with third parties, regardless of a three parts harm test, prior to the release of information or during an investigation under the *Act*.

CONCLUDING COMMENTS

As a general concluding comment, IM officials, who are often assigned *ATIPPA* duties, are challenged to maintain and advance their department/organization's IM program while ATIPP responses have to be developed within strict timelines. The IM officials are essential in providing support to the development of *ATIPPA* responses, as effective performance of IM duties is necessary to generate the responsive records required to address *ATIPPA* requests. The department has generally seen a larger than average increase in the volume and complexity of *ATIPPA* requests it has to handle, which has generally led to an imbalance in time devoted to IM. A rebalancing of resources may be necessary to ensure IM programs continue to evolve to enable and improve overall access to information. Good information management supports successful *ATIPPA* compliance.