

October 9, 2026

VIA EMAIL

Keri-Lynn Power, LLB (Hons), LLM, (Chair)
Access to Information and Protection of Privacy Statutory Review 2025
2nd Floor, Beothuck Building
20 Crosbie Place
St. John's, NL
A1B 3Y8

Dear Ms. Power,

Re: Submission for the Access to Information and Protection of Privacy Statutory Review Committee 2025

Thank you for the opportunity to provide input to the statutory review of the Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015).

NL Hydro is the people's Crown Corporation and we act on behalf of the people of Newfoundland and Labrador. We understand the importance of accountability and transparency to the people of this province and are committed to being open, transparent and accountable across all our operations. We fully support the Access to Information and Protection of Privacy Act (ATIPPA) in its role to ensure the accountability of public bodies.

As part of our continued commitment to transparency and accountability, we provide the people of Newfoundland and Labrador with access to information about completed requests made under the Access to Information and Protection of Privacy Act.

Please find enclosed our submissions.

If you have any further questions, please feel free to contact the undersigned by telephone at (709) 725 4859 or by e-mail at cassandrahearn@nlh.nl.ca

Sincerely,



Cassandra Hearn
Access and Privacy Officer

Submissions

Please note our submissions are identified by the section reference in ATIPPA, 2015.

Division I - the Request

1. **A limit on the number of concurrent ATIPP requests made by the same applicant**
Section 11 (Making a request)

We suggest a legislative mechanism that permits public bodies to limit the number of active ATIPP requests being processed concurrently for the same applicant where the requests are numerous, substantially related, or place an unreasonable administrative burden on the public body. Such a provision would not restrict an individual's right of access. Rather, it would provide a framework to manage high-volume requests in a fair and efficient manner, ensuring that public bodies can continue to meet their obligations to all applicants within legislated timelines.

Comparable provisions already exist within the access to information oversight framework in Newfoundland and Labrador. Under subsection 44(7) of the ATIPPA, 2015, where the Information and Privacy Commissioner has five active complaints from the same applicant dealing with similar or related records, the Commissioner may hold additional complaints in abeyance until one of the existing matters has been resolved. This recognizes the practical need to balance access rights with administrative capacity. Similarly, the Office of the Information and Privacy Commissioner for British Columbia limits the number of open files a complainant may have before the Office at one time, citing the need to ensure equitable and timely access to its services. When an applicant exceeds the threshold of open files, additional matters may be deferred until existing files are concluded.

2. **Preclude applicants from submitting requests for records that can be obtained through other processes**
Section 5 (Application)

We suggest amending the Act to preclude applicants from submitting ATIPP requests for records that are reasonably available through another established legislative, administrative, or operational process. The access to information regime is intended to provide a right of access to records that are not otherwise publicly available or obtainable through existing channels. In some circumstances, applicants use the ATIPP process to seek records that can readily be obtained through alternative mechanisms, such as routine disclosure processes, customer service channels, established application processes, regulatory proceedings, litigation disclosure, employment-related processes, or publicly accessible sources.

Processing these requests through the ATIPP regime can result in unnecessary duplication of effort, increased administrative burden, and the diversion of limited access to information resources away from requests that genuinely require the application of the Act. A legislative provision that directs applicants to established alternative processes where records are otherwise available would promote administrative efficiency, reduce duplication, and support the timely processing of ATIPP requests overall.

This approach would provide an important safeguard by ensuring independent oversight before a request is disregarded, while recognizing that the ATIPP process may not be the most appropriate mechanism where a suitable alternative avenue for obtaining the records already exists.

Compared to the current approach (Section 22 Published material)

The focus is (generally) on records that are publicly available, available for purchase by the public, or accessible through a public source. Examples of this would include a published annual report, publicly available regulatory filing, information available on a website, or documents available in a public library or registry. In these situations, the applicant can already access the information without engaging the ATIPP process. The proposed amendment is a broader approach. This will apply where records are not publicly available, but are available through another established process. For example: an employee seeking employment-related records through a labour relations, grievance, or human resources process. A customer seeking records available through a customer account process. A complainant seeking records through court discovery. A regulatory participant seeking records through a regulatory proceeding. A property owner obtaining records through a statutory inspection or application process. These records are not publicly available, so section 22 may not apply. This way, there is already a dedicated mechanism for obtaining them.

3. Extend disregard to 15 days

Section 21 (Disregarding a request)

We suggest amending section 21 to extend the timeframe within which a public body may apply to the Information and Privacy Commissioner for authorization to disregard a request from five (5) business days to fifteen (15) business days after receipt of the request. The current five-day period can be insufficient for public bodies to adequately assess complex requests, consult internally with subject matter experts, estimate the scope of responsive records, and determine whether the circumstances warrant an application under section 21. In large and operationally diverse organizations, such as Hydro, identifying the nature and impact of a request often requires consultation with multiple business units and record custodians before a well-supported determination

can be made. As a result, public bodies may be required to make decisions regarding a potential disregard application before they have sufficient information to properly assess the request. Conversely, concerns that only become apparent after initial review may not be addressed because the statutory timeframe has expired.

This amendment would not alter the Commissioner's authority to approve or deny a disregard application and would not reduce an applicant's substantive right of access. Rather, it would improve the quality of disregard applications, support informed decision-making, and promote a more efficient administration of the Act. A longer application period may also reduce the number of premature or unnecessary applications submitted to the Commissioner by allowing public bodies additional time to clarify requests with applicants, assess record volumes, and determine whether concerns can be resolved without pursuing a disregard application.

4. Extend transfer to 15 day
Section 14 (Transferring a request)

We suggest amending section 14 of ATIPPA, 2015 to extend the timeframe for transferring an access request to another public body from five (5) business days to fifteen (15) business days after receipt of the request. The current five-day transfer period does not provide sufficient time for public bodies to determine whether another public body has greater custody or control of the requested records, particularly where requests involve multiple organizations, shared responsibilities, historical records, complex operational matters, or subject matter spanning several public bodies. In many cases, a public body must conduct a preliminary assessment of the request, consult with the subject matter experts, and engage with other public bodies before it can make an informed determination regarding custody or control. This assessment often cannot be completed within five business days, particularly where key employees are unavailable, records are decentralized, or the request concerns a matter involving multiple jurisdictions or organizations. As a result, public bodies may transfer requests prematurely without sufficient information, retain requests that would be more appropriately processed by another public body, or miss the opportunity to transfer altogether because the statutory deadline expires before adequate review can be completed.

5. Add disregard option for personal information correction requests
Section 21 (Disregarding a request)

We suggest amending section 21 of ATIPPA, 2015 to permit a public body, with the approval of the Information and Privacy Commissioner, to disregard a request for correction of personal information in circumstances that would otherwise meet the

criteria for a disregard application. Currently, the Act provides a mechanism for public bodies to apply to the Commissioner to disregard certain access requests; however, there is no comparable mechanism for requests seeking the correction of personal information. As a result, public bodies may be required to continue processing repetitive, vexatious, frivolous, or otherwise problematic correction requests, regardless of whether the underlying issue has already been considered and resolved. This can be particularly challenging where an applicant repeatedly seeks to correct information that does not constitute their personal information under the Act, but is instead properly characterized as a professional opinion, work product, evaluation, or other record that is not subject to correction rights. In these circumstances, public bodies may be required to repeatedly review and respond to substantially similar correction requests despite having previously determined that no correction is warranted. Providing access to a disregard mechanism for correction requests would create consistency within the Act by ensuring that comparable remedies are available for both access requests and correction requests where an applicant engages in repetitive or abusive processes.

NL Hydro has experienced instances where multiple correction requests were submitted regarding information that had previously been assessed and determined not to constitute the applicant's personal information, but rather represented work product. Despite these determinations, there was no mechanism available to seek authorization to discontinue the processing of repetitive correction requests. As a result, significant administrative resources were required to repeatedly review and respond to substantially similar matters. A disregard mechanism for correction requests would provide public bodies with an appropriate tool to manage these situations while maintaining the Commissioner's oversight role and protecting legitimate correction rights.

6. A limit on the number of concurrent correction of personal information requests made by the same applicant

Section 10 (Right to Request Correction of Personal Information)

We suggest amending the Act to establish a mechanism that limits the number of active requests for correction of personal information that may be processed concurrently for the same applicant. While ATIPPA provides individuals with the right to request correction of their personal information, there is currently no mechanism to manage situations where an applicant submits a large volume of concurrent correction requests. In these circumstances, public bodies may be required to process numerous overlapping requests simultaneously, placing significant demands on limited administrative resources and impacting the timely processing of other access and privacy matters.

A legislative mechanism permitting public bodies to place additional correction requests in abeyance once a specified threshold of active requests has been reached would

support a more efficient and orderly process while preserving the applicant's correction rights. Such a provision would not prevent an individual from pursuing a correction request; rather, it would provide a framework for sequencing requests where the volume of concurrent requests becomes unmanageable. Public bodies have experienced situations involving exceptionally high volumes of correction requests relating to similar records and issues. In those cases, the absence of a mechanism to manage concurrent requests created significant administrative burden and diverted resources from other access and privacy responsibilities.

A comparable approach already exists within the oversight framework of Newfoundland and Labrador. Under subsection 44(7) of ATIPPA, where the Information and Privacy Commissioner has five active complaints from the same applicant involving similar or related records, additional complaints may be held in abeyance until one of the existing matters has been resolved. This provision recognizes the need to balance individual rights with the effective administration of the Act.

7. **Authority to Charge Fees for Excessive Volumes of Access and Correction Requests**
Section 25 (Costs)

We suggest amending the Act to permit public bodies to charge a reasonable fee where an applicant submits access requests or requests for correction of personal information that exceed a set volume or threshold within a specified period. Public bodies have experienced situations involving exceptionally high volumes of concurrent requests that require significant administrative resources to process. In such circumstances, the cumulative burden of responding to numerous related or overlapping requests can impact a public body's capacity to meet its obligations under the Act and to effectively administer other access and privacy responsibilities. For example, Hydro received over 100 ATIPP requests and 11 requests for correction of personal information from one applicant. This volume of concurrent requests created a significant administrative burden and required the allocation of considerable public resources to process related matters. A reasonable fee structure for requests exceeding a prescribed threshold would assist in promoting the efficient administration of the Act while preserving applicants' statutory rights.

A fee mechanism could be structured to apply only where the volume of requests becomes excessive and would not prevent individuals from exercising their rights under the Act. Rather, it would encourage applicants to prioritize and consolidate requests, while allowing public bodies to recover a portion of the costs associated with processing unusually large numbers of requests. Appropriate safeguards could be included to ensure that fees are reasonable, subject to waiver where appropriate, and do not create an undue barrier to access or correction rights.

8. **Include all government holidays as ATIPPA holidays**

Section 16 (Time limit for final response)

We suggest amending the definition of "holiday" for the purposes of ATIPPA, 2015 so that all days recognized as government holidays are excluded from the calculation of statutory response timelines. Currently, certain government holidays and office closure days recognized by the provincial government are not treated as holidays for the purposes of calculating ATIPPA timelines. This creates an inconsistency between government operating schedules and legislated response requirements. This inconsistency increases the risk of miscalculating response timelines and creates unnecessary administrative complexity for public bodies. It may also require employees to attend otherwise vacant workplaces during government holiday periods in order to meet legislated deadlines, particularly where remote work is unavailable or operational requirements necessitate on-site attendance. Several government holidays that are not currently treated as holidays for ATIPPA calculations, include: St. Patrick's Day, St. George's Day, the June Holiday, and Orangeman's Day.

Division II - Exceptions to Access

9. **Change to 2/3 parts of the test are required to be met to align with the federal act or have the "supplied in confidence" removed/altered**

Section 39 (Disclosure harmful to business interests of a third party)

We suggest amending the third-party business information provisions of the ATIPPA to better balance transparency with the protection of commercially sensitive information. Specifically, modifying the existing three-part test so that only two of the three criteria are required to be met before information may be withheld; or removing or substantially revising the requirement that information be "supplied in confidence" in order to align more closely with the federal Access to Information Act. The current provisions require public bodies to demonstrate that information meets all elements of the applicable test before protection can be applied. In practice, the most challenging component is often the requirement that information be shown to have been "supplied in confidence."

Commercial relationships are significantly complex and information exchanged between public bodies and private-sector partners is often generated collaboratively through negotiation, project development, procurement processes, financing arrangements, and ongoing operational activities. Although such information may clearly be commercially sensitive and disclosure may reasonably be expected to cause harm, it may not technically qualify as having been "supplied in confidence."

This creates an unintended gap in protection. Information that is commercially valuable, non-public, and potentially harmful if disclosed may nevertheless become subject to disclosure because it cannot satisfy the strict "supplied in confidence" requirement. The federal Access to Information Act provides a useful comparator. Section 20(1) protects several categories of third-party information, including: trade secrets; confidential financial, commercial, scientific, or technical information supplied by a third party; and information whose disclosure could reasonably be expected to result in material financial loss, prejudice a third party's competitive position, or interfere with contractual or other negotiations. The federal legislation recognizes that demonstrable commercial harm alone can justify withholding information. Sections 20(1)(c) and 20(1)(d) focus on the consequences of disclosure rather than whether the information was originally "supplied in confidence." As a result, federal institutions possess greater flexibility to protect commercially sensitive records where disclosure would prejudice a third party's competitive position or interfere with negotiations, even where disputes may exist about whether the information was strictly "supplied" to government.

For organizations such as Hydro, commercial information frequently arises through collaborative processes rather than simple one-way submissions. Major infrastructure projects, energy developments, procurement activities, and commercial negotiations often involve: jointly developed pricing models; negotiated contractual provisions; risk assessments; financing arrangements; strategic development plans; and technical evaluations prepared by multiple parties. The practical question should not be whether the information was supplied by a third party, but whether disclosure would cause genuine commercial harm. A test that focuses excessively on the origin of the information rather than the impact of disclosure can undermine legitimate commercial interests while providing little additional benefit to transparency.

10. Add an Explicit Critical Infrastructure Exception and Cybersecurity Exception

We suggest including a specific exception protecting critical infrastructure and cybersecurity information. At present, public bodies must generally rely on section 31(1)(l) and related harms-based provisions to protect records that could expose vulnerabilities in essential infrastructure. While these provisions provide some protection, they were not designed specifically to address the modern cyber and physical security threats facing critical infrastructure operators.

The electricity system is increasingly recognized as critical infrastructure whose disruption could have significant consequences for public safety, economic stability, emergency services, and provincial security. As cyber threats and physical security risks continue to evolve, utilities must maintain a robust ability to protect information that could reasonably be used to identify, exploit, or target vulnerabilities within the electrical system.

The existing ATIPPA framework generally requires a public body to establish a reasonable expectation of specific harm before information may be withheld. This approach can create challenges where the information itself is inherently sensitive due to its relationship to critical infrastructure. For example, a detailed electrical system diagram, network architecture document, or vulnerability assessment may not necessarily reveal an immediate and identifiable threat. However, disclosure of such information may contribute to a broader understanding of system weaknesses when combined with other publicly available information. The risk often arises from the aggregation of information rather than the disclosure of a single record in isolation. As a result, critical infrastructure operators may find themselves relying on exceptions that were developed before today's cybersecurity environment and that do not explicitly recognize the unique risks associated with the protection of essential infrastructure.

Parliament has recognized the need for enhanced protection of critical infrastructure information through amendments to the federal Access to Information Act. Section 20(1)(b.1) specifically protects information supplied in confidence relating to emergency management plans and information concerning the vulnerability of buildings, networks, systems, computer networks, communication systems, and the methods used to protect them. The provision recognizes that disclosure of such information could undermine the security and resilience of critical systems and therefore warrants specific statutory protection. This federal approach acknowledges that certain categories of infrastructure and security-related information require protection because of their inherent sensitivity, rather than solely because a public body can demonstrate a specific and immediate harm in each individual case

11. Issues regarding the disclosure of solicitor-client privilege information should be provided to Court opposed to the Commissioner

Section 30 (Legal advice) and 44 (Investigation)

Solicitor-client privilege has repeatedly been recognized by Canadian courts as a substantive rule of law and a principle of fundamental justice. Unlike many discretionary or mandatory exceptions under access legislation, solicitor-client privilege serves a broader public interest by protecting the confidential relationship between lawyer and client and promoting the administration of justice. The Supreme Court of Canada has emphasized that solicitor-client privilege must remain as close to absolute as possible and should only be interfered with where absolutely necessary. Given the elevated status afforded to solicitor-client privilege, disputes concerning its existence, scope, waiver, or application are particularly well suited for judicial determination by courts that possess inherent jurisdiction over privilege claims. In *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, 2008 SCC 44, the Supreme Court

held that clear and explicit statutory language is required before a tribunal or administrative decision-maker may compel production of privileged documents. The Court recognized the unique status of solicitor-client privilege and stressed that courts are generally the appropriate forum for resolving disputes where privileged information is at issue.

The Supreme Court has also described solicitor-client privilege as a "fundamental civil and legal right" that should not be set aside absent clear legislative authority. In *Lavallee, Rackel & Heintz v. Canada (Attorney General)*, 2002 SCC 61, the Court stated that solicitor-client privilege is essential to the effective operation of the legal system and must receive the highest level of protection.

Similarly, in *Alberta (Information and Privacy Commissioner) v. University of Calgary*, 2016 SCC 53, the Supreme Court reaffirmed that solicitor-client privilege is no longer merely an evidentiary rule but a substantive right. The Court held that unless legislation contains explicit language authorizing disclosure of privileged records, decision-makers should not be interpreted as having authority to compel production of such records.

12. **Limit disclosure of records relating to a workplace investigation such that the right of access would commence after a workplace investigation has been completed**
Section 33 (Information from a workplace investigation)

Workplace investigations serve an important public and organizational function by enabling employers to investigate allegations of misconduct, harassment, discrimination, violence, conflicts of interest, and other workplace concerns in a fair, confidential, and effective manner. Permitting access requests for investigation records while an investigation remains active risks undermining these objectives. During an ongoing workplace investigation, records may consist of witness statements, investigator notes, draft findings, interview summaries, credibility assessments, and communications exchanged for the purpose of conducting the investigation. Disclosure of such records before the investigation has concluded may compromise the integrity of the process, discourage witness cooperation, create opportunities for collusion among participants, and impede the investigator's ability to collect reliable evidence.

A delayed right of access until the completion of the investigation would strike an appropriate balance between transparency and fairness. Such an approach would not permanently deny access to records; rather, it would recognize that disclosure during an active investigation may cause harm that cannot be remedied once the information has been released.

Other Considerations

13. Section 31 of the Hydro Corporation Act, 2024 be strengthened beyond Oil & Gas, particularly in light of the Churchill River developments

Historically, certain entities within the provincial energy sector benefited from additional statutory protections for commercially sensitive information through section 5.4 of the Energy Corporation Act. With the repeal of that legislation and the enactment of the Hydro Corporation Act, 2024, Hydro must now rely on the exceptions contained within the ATIPPA and the protections set out in section 31 of the Hydro Corporation Act. The latter are limited by the definition of “commercially sensitive information” which relates primary to the oil and gas sector.

Hydro respectfully submits that consideration should be given to strengthening section 31 of the Hydro Corporation Act, 2024 to ensure that it provides adequate protection for commercially sensitive information beyond the current focus on oil and gas related matters. Such consideration is particularly important in light of the significant commercial relationships associated with Churchill River developments and other major energy initiatives undertaken by the Corporation.

Hydro's operations involve complex commercial arrangements with contractors, consultants, Indigenous organizations, utility partners, financial institutions, equipment suppliers, and other private-sector entities. These relationships often require the exchange of highly sensitive commercial, financial, technical, and strategic information. Hydro's ability to attract, negotiate with, and maintain productive relationships with these partners depends in part upon their confidence that commercially sensitive information will receive appropriate protection from public disclosure.

The Churchill River developments represent some of the most significant energy assets in Newfoundland and Labrador and involve ongoing commercial activities of considerable scale and complexity. Existing operations, future developments, transmission initiatives, power purchase arrangements, financing structures, and commercial negotiations all depend upon Hydro's ability to manage sensitive information responsibly. In many circumstances, disclosure of commercially sensitive information could prejudice Hydro's negotiating position, impair the competitive interests of third parties, increase project costs, or adversely affect the province's economic interests.

While the ATIPPA contains important protections for third-party business information and information harmful to the financial or economic interests of a public body, these provisions may not always provide the degree of certainty required by commercial counterparties engaged in large-scale, long-term energy projects. The removal of the broader protections previously available under section 5.4 of the Energy Corporation Act has heightened the

importance of ensuring that section 31 of the Hydro Corporation Act, 2024 is sufficiently robust to address modern commercial realities.

Strengthening section 31 in this manner would provide greater certainty to existing and prospective business partners, reinforce confidence in the Corporation's ability to safeguard commercially sensitive information, and support the successful advancement of current and future Churchill River developments. It would also better align the legislative framework with the commercial environment in which Hydro operates and reduce the risk that concerns regarding confidentiality could negatively affect project costs, procurement outcomes, financing opportunities, or future investment.

Hydro recognizes the importance of transparency and public accountability and supports continued oversight through the existing access to information regime. However, the Hydro submits that consideration should be given to whether the balance between transparency and commercial confidentiality remains appropriate in light of the strategic importance of Newfoundland and Labrador's energy sector and the increasingly complex commercial arrangements required to develop and manage these assets. Ensuring that section 31 contains adequate protection for commercially sensitive information beyond the oil and gas context would help safeguard the province's long-term economic interests while allowing Hydro to continue fulfilling its public mandate.