NUNAVUT INFORMATION AND PRIVACY COMMISSIONER
Review Report 20-164

Review File 18-179-5
January 13, 2020
Citation: 2020 NUIPC 2

BACKGROUND

On September 24th, 2018, an administration officer with the Nunavut Legal Services Board (“NLSB” or "Board") requested an information technology (IT) consultant to investigate an issue with access to the NLSB electronic application used to process business information. In the course of its exploration of the issue, the IT consultant "identified an active attempt by an unknown party to gain unauthorized access to the server" in October 2011, as well as "several critical security vulnerabilities which could have allowed these attempts to succeed" completely undetected. Other highly concerning "vulnerabilities" were also detected.

The October, 2011 event occurred on an older server that was still in operation but which no longer hosted the NLSB's databases. The NLSB's application and data base was moved to another server in 2013 by their server provider, and with the change in servers the Chief Executive Officer (CEO) and the Board reasonably expected that the new server featured updated security reflective of the current versions in use at that time. However, the new server mirrored the same configuration as the server that had been compromised, and so, in simple terms, was as insecure as the old server. Due to a lack of appropriate server management, including leaving passwords and settings in default factory modes, and an absence of applied standard security protocols, the same vulnerabilities that existed in the old server were found to exist on the new server, and so directly threatened the security of the data currently held. Given the critical failures and ongoing high risks to the data, the consultant took immediate steps to suspended operation of both servers, until further analysis of the situation could be made.

On October 10th, 2018 I received notification from the then CEO of the Board of a contravention of the *Access to Information and Protection of Privacy Act* (“ATIPPA” or "ATIPP Act"). In addition to this notice, and in corresponding with my office regarding the IT consultant's findings, the CEO revealed that this was not the first serious issue experienced with a data base by their office. Apparently, they had suffered a total loss of a data base and email service some years earlier as a result of a complete "crash" of the system in which all of that data was rendered unrecoverable.

The NLSB collects personal information in order to conduct its business of providing legal services for clients. For context, rather sensitive personal information may have been affected by these several incidents including the recently discovered "vulnerability" which, at the time the issue was discovered, the consultant estimated had been in existence for over five years. For greater specificity, the type of information that was or could have been affected by the breach, as reported by the CEO, included but was not limited to:

- name,
- address,
- social insurance number,
- date of birth,
- financial information or other evidence of income (to determine eligibility for legal services), as well as
- the area of law that the client was seeking help with.

Because the CEO mentioned “forms”, I suspect that the forms that were stored electronically on this server also contained original signatures in many cases. However, the CEO quite unequivocally stated that the data in the data base did not include "court-related information". Based on the information provided, the data base appears to have been used for administration of the office and processing applications from the public for legal services, but not case specific documents.

The business environment relevant to this case includes a number of stakeholders, including:

a. the NLSB which was responsible for user account management (on boarding and off boarding users) for their web application, and electronically processing client applications;
b. a third party website consultant located in Ontario, and responsible for "putting in place security" for their web application;
c. a third party server service provider located in Canada, the US, and internationally, responsible for hosting the database on a secure server and for updating software to ensure the information was both available and protected, and hosting NLSB data, in theory, in Toronto;
d. a local IT consultant brought in by the NLSB to address recent technical issues;
e. the Government of Nunavut (Department of Justice) which provides the funding for the work of the Board;
f. contracted service providers, including independent lawyers representing NLSB clients;
g. Nunavummiut served by the NLSB.

An IT consultant aiding the NLSB with this matter analyzed the issues inherent with the platform used to host the NLSB's database and concluded rather assuredly that "all data stored on [the server was] exposed to unknown parties for an unknown length of time, certainly some vulnerabilities had existed for over five years". The nature of the issues with the server rendered any access audit of the server moot because the server had been accessible to anyone with the knowledge of how to capitalize on the vulnerability for some time and such access would have been undetectable and apparently not traceable.

It was rather clear that the requirements to protect information and prevent such unauthorized access and loss of data, as identified by ATIPPA, had not been met, both in the case of the vulnerabilities discovered by the IT consultant and by the loss of an earlier version of the entire data base in 2007. Given the nature of the breaches, I determined that it was warranted to conduct an official review of this matter under the 49.1(2) of the ATIPP Act.

ISSUES

While several concerns came to light in exploring this case, in my opinion these are the main issues:

1) Is the Legal Services Board a public body subject to the *Access to Information and Protection of Privacy Act*?
2) Were reasonable security arrangements made against such risks as unauthorized access, collection, use, disclosure or disposal in compliance with s. 42 of ATIPP;
3) Did the Board provide appropriate notifications in relation to the data breach in compliance with s. 49.9, 49.10, 49.11?
4) Did the Board take steps to control and mitigate risks and to prevent future recurrence of this incident?

ANALYSIS

1) Is the Legal Services Board a public body subject to the *Access to Information and Protection of Privacy Act*?

In my correspondence with the Board regarding a separate matter concurrently being addressed by my office (2019 NUIPC 10) the then CEO (Executive Director) of the

NLSB proposed that the "LSB is independent and not part of the GN" (Government of Nunavut), and rather is a "distinct public entity separate from the GN". While the CEO apparently appreciated the Board's responsibilities under ATIPP in this case, as demonstrated by notifying me of this breach, I thought it prudent to first establish if the NLSB is a "public body" under the Act and to confirm my jurisdiction in this matter given the relationship of the Board to the GN is somewhat unique.

The Nunavut Legal Services Board is established under the *Legal Services Act* of Nunavut. Each of the Board's seven members is appointed by the Minister of Justice. According to the NLSB web site "the NLSB is responsible for providing legal services to financially eligible Nunavummiut in the areas of criminal, family, and civil law". With operations in all three regional centers, the NLSB self-describes itself as a publically funded agency that operates independently, or "arms-length", from the Government of Nunavut.

The NLSB is identified in Schedule A of the Nunavut Financial Administration Act, as a "public agency", as well as Schedule A of the ATIPP Act regulations, as a "public body". Pursuant to section 1(2) of the regulations and given the definition of a public body in section 2(b) of the Act, the "Legal Services Board of Nunavut established under the Legal Services Act" is, clearly subject to the ATIPP Act, and my office has jurisdiction in this case. Further, there is nothing in the Legal Services Act that overrides, contradicts, or conflicts with the *Access to Information and Protection of Privacy Act*. The Board is required to comply not only with its own Act, but the ATIPP Act as well.

2. Were reasonable security arrangements made against such risks as unauthorized access, collection, use, disclosure or disposal?

When reviewing another matter that had been brought to my attention about the NLSB information handling practices specific to use of g-mail accounts for business purposes,

(2019 NUPC 10) I became aware that previous to the recently discovered "vulnerabilities" the organization's "internal IT platform [had] crashed", which rendered the email service and information databases unusable. Apparently several thousands of dollars and many years were spent trying to retrieve the lost data unsuccessfully. It appears that limited technical resources over an extended period of time contributed to the historical loss of records (prior to breach notification provisions coming into effect) and has contributed to the environment that allowed the vulnerabilities more recently identified by the IT consultant to exists undetected for so long. Without question, there was a significant lack of rigor by many parties in this case to protect the resources of this public body.

In this most recent case of the discovered vulnerability, personal information was most assuredly exposed to potential unauthorized access, and it is reasonably possible that information was also inappropriately disclosed (copied or removed from the data base).

Even one unauthorized access event is significantly troubling and it is possible that there may have been many and ongoing instances of unauthorized access. This also calls into question the integrity of the information itself as this may have been compromised by unknown actors.

It is reasonable to assume that the risks to the data in the database snowballed over time given the ongoing lack of security. The report prepared by the technical consultant who discovered the vulnerability in October 2018 identifies the numerous high risks that the data base was consistently and cumulatively subjected to. The consultant states that the software on the server used to host the NLSB data was well past its "end of life", this being "the officially announced date after which the software developer no longer maintains or updates the product", when the vendor ceases to not only patch and repair vulnerabilities but ceases to investigate if there are any vulnerabilities and the vendor then "recommends ceasing using the product".

Of significance, the consultant states that "these products were identified as having already been announced end of life prior to the commissioning of the server". I interpret this to mean that the measures in place to protect data were already well past their "best before" date at the time NLSB's data was hosted in that electronic environment. This is, of course, very concerning. The consultant also found that the version of software previously in use had not been updated prior to its end of life, and so security was not maintained despite newer releases being available - "thousands of security vulnerabilities... remained present and available for exploit on the … server".

Section 7 of the *Legal Services Act* provides that the objects of the Board are:

(a) to ensure the provision of legal services to all eligible persons;
(b) to ensure that the legal services provided and the various systems for providing those services are the best that circumstances permit; …

Section 8 of that Act requires the Board to

(a) administer the Act and the regulations;
(b) make every endeavour to attain the objects of the Board; …
(d) co-ordinate the provision of legal services; …

Section 11 gives the Board the power to

(a) make policies and rules for administering the Act and the regulations, and
(b) establish the offices and agencies and maintain the facilities that are necessary; and
(c) do the things that are necessary, incidental or conducive to the attainment of its objects or the fulfilment of its duties.

Generally interpreting the intent of the *Legal Services Act* as it pertains to the NLSB, it is clear that the Board's purpose includes ensuring required offices, agencies and "facilities" are established, and that the necessary policies and procedures are created conducive to good governance of the legal services provided by the Board. As a public body, the NLSB has, at all times, been required by the *Access to Information and Protection of Privacy Act* to protect personal information from unauthorized access and to ensure the accuracy and retention of information. Measures necessary to operate the NLSB, including policies and procedures, must also serve privacy and security of data collected by the Board, not just the nuts and bolts of legal services.

Of particular concern given the multiple "vulnerabilities" found by the IT consultant, is the apparent lack of an assessment conducted to identify and address privacy risks inherent in the systems put in place by the NLSB. Section 42.1 of the ATIPP Act now requires a public body to prepare a privacy impact assessment in conjunction with the redesign of existing programs or services. According to the GN's own Privacy Management Manual (P.68):

> 5.1.1. Project authorities must determine whether a PIA needs to be conducted in relation to each new initiative that falls under their responsibility. This is done by completing the Summary of Initiative Description to Determine the Need for a Privacy Impact Assessment form at Appendix 2 and the Risk Area Identification and Categorization Table at Appendix 3.

A privacy impact assessment (PIA), as defined in the ATIPP Act, is an assessment that is conducted by a public body to determine if a current or proposed program or service meets or will meet the requirements of Part 2 of the Act. These are best completed at an early stage of planning so as to address any privacy concerns that might be identified.

It is reasonable to assume that, in addition to the Board's legal responsibilities under the *Legal Services Act*, the Board's responsibilities clearly include "do[ing] the things that are necessary and conducive" to its business, including to protect the personal information collected in the course of their duties. In my opinion, the Board is required under the ATIPP Act to "determine if a current or proposed program or service meets or will meet the requirements of Part 2 [part 2 being PROTECTION OF PRIVACY] of this Act". There is no evidence that a PIA has ever been conducted in relation to the technology being used by the NLSB. This is not surprising because the hardware and software in use at the time of this breach notification appears to have been in place long before the Act was amended to require the preparation of PIAs and, as a result, this legacy system was not assessed in terms of either security or privacy protectiveness. This highlights the importance of the PIA requirements under the 2017 amendments to the *Access to Information and Protection of Privacy Act* which introduced the requirement that PIAs be conducted "during the development" of a new program or service or the "redesign" of an existing one. If a PIA had been conducted, and revisited, reviewed and updated on a regular basis, the Board may well have been aware of the privacy and security weakness of the systems it was using. It would also have been in a better position to understand the measures necessary to protect personal information and ensure policies and procedures and technological safeguards were established and maintained, and that regular staff training occurred. Data security seems to have been wholly delegated to the NLSB's distant and virtual service providers, with no follow up. A seemingly classic case of delegate and disappear, with concerning consequences not only for the privacy of those individuals using the services of the NLSB, but also for the integrity of the Board's informational assets.

In a recent review referred to earlier, 2019 NUIPC 10, a report that also focuses on the privacy and information security environment within the NLSB, I wrote that the GN's own Privacy Management Manual (PMM) sets out provisions regarding the public body's duty to adequately maintain records. The Introduction to this document provides that:

> The Privacy Management Manual (PMM) is a comprehensive set of tools and resources to be used by all employees of the Government of Nunavut to successfully implement the privacy provisions of the Access to Information and Protection of Privacy (ATIPP) Act.

It also provides that

> All employees are required to familiarize themselves with the PMM as the ATIPP Act holds each employee accountable for the privacy of personal information under the custody and control of the government.

In Review Report 2019 NUIPC 10, I found that the requirements set out in the PMM apply to the NLSB notwithstanding that there may be a level of independence from the GN. The PMM outlines expectations with respect to public records in relation to the ATIPP Act, including:

> Pg.10 - The Act also requires that public bodies implement reasonable security measures to protect the personal information under their control from unauthorized access (confidentiality), modification (integrity), use and destruction.
>
> Pg. 17 - The information that is collected and created while fulfilling our responsibilities must be documented and stored in a way that facilitates its retrieval for future operational and legal requirements, including responding to requests received under the ATIPP Act. Furthermore, it must be adequately safeguarded to protect its confidentiality, integrity, availability and value.

I find that the data held by the NLSB had not been maintained in a manner that met best practices nor the requirements of ATIPPA, the intent of the NLSB, nor the GN's policies. Records must be maintained in a way that both protects them and facilitates their retrieval for future operational and legal requirements, including the ability to respond to an access to information request under ATIPPA.

That said, the CEO reported that they had taken steps to put some measures in place to appropriately manage internal use of information handled by the NLSB. The CEO reported that internal protections had been put into place, including that the data base was password protected, and that any employees who did have access to the data base had been trained in the use of the application and were made to sign a confidentiality agreement prior to being given a password for the system. Under the supervision of the CEO, the COO (Chief Operating Officer) appears to be responsible for managing IT resources for the NLSB. The COO is responsible for application administration, including creating new user accounts and setting rules for passwords so that they meet the privacy policy requirements of the application. When an individual leaves the organization, the COO ensures that their account is deleted from the system.
While I was not provided specific details of policies and procedures, it seems the Board does have some measures in place to manage access to the database to protect the data from unauthorized internal use. These practices may or may not have been committed to "writing". Certainly updating and committing these processes and procedures "to paper", in the form of prescribed policy and procedures so that they can be shared, would better meet the expectation of the Act in this regard.

I must also add that I see issues with the level of service provided by the third party service providers in this case, and further, given the information at hand, I have no certainty that the NLSB data was not hosted outside of Canada. The service provider for the database hosts the data virtually, and has servers in the United States. The CEO stated that the Board understood that the service provider hosted the data in Toronto. It

is not clear what assurances the Board has of this other than the vendor's word, and given the state of security on the server, it seems unreasonable to place much trust in this. Location is important, because the location that data is stored is important. More specifically, the jurisdiction and thus the laws applicable in that jurisdiction are relevant. Once the data is stored elsewhere, Canadian law has limited, if any, reach. Under United States law, data held in the States is subject to the *Patriot Act*. The *Patriot Act* serves US law enforcement, and makes information stored in the US subject to search and copy by that government. Awareness of what laws data is subjected to is an important consideration when determining what service providers to entrust personal information to. Given the information we were able to glean on-line and in the report of the IT consultant about the service provider, it seems at least possible that this information may not have been managed as described by the vendor. These issues would normally be brought to light by way of a Privacy Impact Assessment, and this further highlights the importance of conducting a PIA well before committing to any new use of information technology.

3. Did the Board meet its responsibility for appropriate notification in relation to the data breach?

Pursuant to sections 49.9 and 49.10 of the ATIPP Act, notice of a breach is required to be made to the Information and Privacy Commissioner where the breach is "material" (49.9) and to an individual affected by the breach where there is a real risk of "harm" (49.10). In certain circumstances, "others" may also be required to be notified under s. 49.11.

In determining materiality under s. 49.9, the public body is to consider the following factors:

(a) the sensitivity of the personal information;

(b) the number of individuals whose personal information is involved;

(c) the likelihood of harm to the individuals whose personal information is involved; and

(d) an assessment by the public body whether the cause of the breach is a ` systemic problem.

This is a non-inclusive list and other factors may be relevant to the determination. Certainly, given the circumstances, it has been demonstrated that this breach was material.

The CEO of the NLSB wrote to me on October 10th, 2018 to advise me of the vulnerabilities discovered by the IT consultant, and so fulfilled the NLSD's requirements under the Act to notify my office under s. 49.9 .

Under S. 49.10 of ATIPPA, the public body must notify individuals whose information is affected by a breach if the public body determines that there is a real risk of significant harm to the individual affected. "Harm", pursuant to S. 49.7 is defined as "bodily harm, humiliation, damage to reputation, damage to a relationship, loss of an employment, business or professional opportunity, a negative effect on the credit record, damage to or loss of property, financial loss and identity theft." To determine if there has been a "real risk of significant harm", the Act lists two factors must be considered:

(a) the sensitivity of the personal information; and

(b) the probability that the personal information has been, is being or will be misused".

Once again, however, this is a non-inclusive list. The personal information exposed to unauthorized access in this particular case is highly sensitive, and if exposed to malicious or even unauthorized actors, could or might be used to cause "harm". One or more data elements combined could be easily used for financial theft, or other harms. It

seems reasonable given the type of information, the circumstances and pursuant to definitions and requirements set out under ATIPPA, that the Board should notify individuals of this breach as soon as possible.

With regards to notification of affected individuals under 49.10, the CEO of the Board initially advised me that, "We estimate that approximately 5000 of our clients could have been affected by this vulnerability", and further "given the number of individuals who could have potentially been affected by this [being many], the NLSB has not yet taken steps to contact each individual". The CEO initially indicated that they intended to postpone action regarding notifying affected individuals until it reviewed the recommendations in my review report. The CEO also offered that, "the LSB does not have the capacity or resources to contact each and every one of these individuals directly, and many of them live in remote communities". While one of my roles is to make recommendations to public bodies, where, as here, the kind of information at risk is exactly the kind of information that might lead to identity theft, the earlier the notice is provided, the better and, as a review process can take many months, I would expect that a public body would not wait for the final report from this office before notifying clients so that they can take steps to monitor their financial information and mitigate damages. There is nothing under the Act that prevents a public body from notifying individuals once a breach has been identified and the harms test has been applied to that context. In fact the Act compels the public body to do so if the public body knows or has reason to believe that a breach of privacy has occurred with respect to personal information under its control, and there is a real risk of significant harm (Section 49.10 (3)).

In subsequent correspondence with my office, the CEO later stated that with regards to the public notice, the Board now "proposed that a public notice be posted in public spaces (community centers, post office, hamlet office, health centers) in all 25 Nunavut communities, written in [Inuktitut, French and English language], in order to advise the

public of the vulnerability" and to provide contact information in case anyone had questions. Having no indication that this step was taken, I requested verification that notice has been made, but have as yet not received confirmation.

As part of my investigation, I have taken into consideration the various rationale provided by the CEO (the high number of persons affected, remoteness of individual's locations, and limited capacity and resources of the NLSB) in determining the most appropriate form of the notice. In my opinion there are several factors that require consideration before deciding the right approach to notification in this case, none of which are the same as the Board has suggested.

In most cases, the fact that a large number of individuals have been affected by a breach would not, by itself, justify an approach that does not result in the contact of each individual that has been affected by a breach. Certainly in today's environment, sending breach notifications to 5000 people is not unheard of.

Nor is the fact that an individual lives in a remote community a valid argument to excuse direct notification of that individual by any public body. Individuals are contacted directly in all manner of environments and circumstances across the globe, privately and for public purposes; "remoteness" has no bearing upon the ability of the NLSB to contact each affected individual.

Furthermore, the fact that "the [Nunavut] LSB does not have the capacity or resources to contact each and every one of these individuals directly", is also not a valid rationale for avoiding direct contact. The fact that the NLSB is not normally tasked with or have specific expertise to pursue such an exercise is not, in my opinion, a relevant consideration. For context, the NLSB has, according to Board's 2016/17 Annual Report (the last report posted to its web site) an annual budget of approximatly12 million dollars ($11,818,000). While this is not an organization suffering the limitations of a shoe-string

budget, the Board in the same report indicates it is "underfunded" and may need to cut its service offering. So, we can take from this, they are also not flush with cash despite the many zeros. However, and while the costs of the services delivered by the Board are high, the costs that might be incurred to directly notify individuals cannot constitute "not having" resources to contact these individuals. One of the consequences of failing to comply with privacy legislation is having to address it - which costs money, as the Government of Nunavut, having recently experienced a serious cyber-attack, can attest to.

In considering factors to determine if notification of individuals directly should be pursued, the age of the information collected by the NLSB is a significant factor that, perhaps, was the most relevant concern the CEO identified. Given the passage of time since collected, I would question the current accuracy of the information that was presumably correct at the time of collection, but that has been at rest in the database for these many years. Residential addresses and names change over time, and there would therefore be a significant error rate in directing notifications to those locations and individuals who had been added to the database many years ago. To rely on their accuracy might amplify the risks to privacy, by sending personal information possibly to a recipient that is an unrelated third party, and in multiple cases. Each data set would need to be verified for contact information prior to notifying the client. While onerous, this task is not impossible and may be a reasonable expectation in some circumstances.

I further considered the accuracy of the records most recently opened by the LSB. The Board could have had confidence that directing a notification to each individual associated with most recently created records, especially for current clients, would likely result in the notice being directed to the correct address, and that the number of these records would not make the task onerous for the limited resources and capacity of the NLSB.

I also considered that not all of the records impacted may still exist. Given the length of time that these vulnerabilities have existed, it is reasonable to expect that the Board cannot identify all records affected, as some records may have been purged as part of a data retention policy. Just because a record was lawfully destroyed should not negate the Board's responsibility to notify those individuals of the risks that existed to their data, and this is where a very public notice would be both appropriate and practical, expecting those individuals possibly affected would self-identify.

While I would normally insist on individual notifications, in considering these factors, in my opinion the public interest would be best served by a combination of approaches in this case. It was, and still is, reasonable for the NLSB to

1) verify the accuracy of the contact information it has on file for the period that the vulnerability applied to, and
2) directly contact all persons within its data base who's information was active at the time the vulnerability was discovered, and,
3) also undertake a public notification about the vulnerability.

In addition to the locations already identified by the Board in its earlier discussions it would be appropriate for such a notice to appear in Nunavut newspapers, and via local radio and local TV feeds, as well as to post a notice on the NLSB web site and in its physical offices. As already identified by the Board, such a notice would include contact information for a NLSB representative who can aid in answering questions and addressing concerns. Further, and as part of this exercise, the NLSB should ensure that it can identify for any individual receiving notification what kinds of information that were or could have been held by the NLSB and that may have been exposed to the vulnerability.

I anticipate that a notice such as this may well result in a significant number of inquiries, and I would strongly suggest that the NLSB identify and train one individual within the organization to be dedicated to responding to these inquiries - someone who can knowledgeably answer questions and advise individuals.

Lastly in terms of notification, the Act requires "others", such as the Government of Nunavut to be notified in certain circumstances. It is not clear to me if the NLSB initially or has since reported this breach to the GN or the Department of Justice. It is possible as part of its business relationship with the GN, that the Board is responsible to notify the GN in such a case, although this is not clearly prescribed in the legislation. Such reporting would be reasonable. Similar reporting is required of researchers under the ATIPP regulations (s. 8(i)) if a contract condition has been breached pursuant to s. 49.11 of the Act, but not so clearly required of public bodies that are "arms length" from the GN. Given, in this case, the information that has been breached might expose individuals affected to identity theft and thus make them susceptible to harm from financial fraud or other harms, and while the NLSB does not by its own admission have the resources to address such risks, the GN may be able to offer further assistance, including resources to contact each individual.

4. Did the Board take steps to control and mitigate risks and to prevent future recurrence of this incident?

It is not only important to identify risk to privacy, but to take action to control the risk and prevent incidents from recurring. On September 27th, 2018, having confirmed the vulnerability with the aid of the IT consultant, the Board was advised of the vulnerability to their data. Though the CEO communicated to my office that they did not have enough evidence to confirm the data base had been accessed by any unauthorized individual, the Board was advised that the server had been compromised for at least 5 years and that, based on evidence obtained, that the Board should presume that the data had

been compromised. The Board "acted on the basis that there was a vulnerability and immediately took steps to shut down the access to the server altogether". The Board also requested the consultant to provide details so they could better understand the issues.

In addition to shutting down the server, the CEO reported that the NLSB took steps to "expedite" transfer its data to a secure server. The Board also reported the breach to my office within two weeks of discovering the vulnerability, which is within a reasonable time period. The Board took short term and long term steps to address the issue, and the CEO stated that they would continue working with the IT consultant to learn whether additional reasonable security measures would be necessary. However, and while the CEO at that time has been responsive and taken it upon themselves to provide a considerable level of detail to my office, I have not been apprised of what additional actions the board has taken since they proposed to notify the public. I would expect that a review of business processes and contracting has been pursued, and that conducting PIA's has been added as prerequisite to any new or significant changes to older information systems (including the system to which the database has been transferred) or to the development or implementation of new technologies. I expect the Board would have also ensured that policy and procedures in place are adequate to prevent this situation from recurring. If these steps have not been taken, more clearly needs to be done in terms of protecting the data collected by the Board. A complete review of all associated business processes and a gap analysis would be a good start, if this has not already been completed.

With regard to notifying clients, I was not advised if the Board sought legal advice on identifying or notifying clients impacted by the breach, but the CEO did state the Board eventually proposed to make a public notice to Nunavut's citizens. This public approach was determined by the Board to be the best approach for various reasons identified by the CEO in correspondence to my office, as discussed above. In terms of controlling

harms, however, the Board did not consider immediate notification in the same light as it considered immediately shutting off the servers. In taking this approach it addressed the risk to the data, but did not immediately consider the risks to the affected individuals. More immediate action could have been taken. In the end the Board and I have apparently come to not the same, but a similar conclusion, and that is that those impacted need to be notified of this vulnerability.

DISCUSSION:

This case emphasizes the dire need for governments to ensure that their departments, boards an agencies have contractual obligations clearly laid out regarding privacy and security requirements, and that such organizations are adequately financially resourced to meet their legislated obligations in this regard. Privacy and security of information, especially in an age where personal information is a prime target of malicious actors, needs to be made a high priority. The rights of individuals, including the right to be notified immediately of risks to their information, must also met.

There does not seem to be much emphasis on the responsibilities of public bodies for the protection of privacy apart from legislation. Mandate letters and strategic priorities rarely, if ever, mention, let alone highlight, the importance of active information management by these organizations. All too often they are given a broad mandate, a generally allocated budget lacking specific line items for security of records, and training in privacy and security is not made a collective requirement. Boards like the NLSB struggle to meet their administrative responsibility to properly maintain hardware and software, and the critical need to ensure that software is updated. They usually do not have the technical know how to do so, and can't hire IT staff without this clearly identified in their budgets. Information management costs money and requires not only an initial investment, but consistently funded operations and maintenance budget, and trusted business support services. Also, information systems cannot be simply

purchased and used. They need regular patching and upgrading and they have an end life and must be replaced every so often. Using an application that is no longer supported is to invite certain peril.

On a similar note, the GN should ensure, as part of funding agreements, that boards and agencies are required to conduct PIAs prior to establishing and/or making major changes to the manner in which personal information collected by them is handled. Privacy is protected under the Canadian Constitution, territorial legislation and GN policy. It is also protected under common law referencing recent cases of intrusion into seclusion being recognized as a cause of action in civil cases. The cases the NLSB takes on are sensitive in nature and individuals should not be concerned, when they approach the Board for assistance, that their sensitive information collected for administering the NLSB services is at risk. The NLSB owes a duty of care to the individuals it serves, and to the contractors it hires. More can be done by the NLSB and the GN to ensure individuals' rights to privacy is protected and respected.

Notification needs to happen and I fully trust the Board will do so as soon as possible if it has not already done so. In my opinion, this notice should include the notification of some of the individuals directly, in addition to a public communication. While the Board's proposal notifying individuals was based on, among other things, the reported dearth of resources available to the LSB, it is a requirement to notify these individuals directly unless it is not reasonably possible to do so. Furthermore, pursuant to s. 49.12, where the Information and Privacy Commissioner's opinion may be other than the Board's and where the Information and Privacy Commissioner sees that notification was not sufficient, the Information and Privacy Commissioner may recommend the Board take alternate or additional steps. To be clear this does not mean the public body should defer notification pending an opinion by the Information and Privacy Commissioner before acting in the near term, and the Board is ultimately responsible for their actions. The Board did conclude that a public notice was warranted, however, in my opinion,

there was no reason why the most recent and therefore reasonably accurate information in its data base could not been relied on to also contact those specific individuals directly, and then rely on the public notice to address the balance of those to be notified.

I am not clear how it is that the Board came to be engaged with the businesses that hosted and provided web services. How were they procured? Were they vetted? Is there no local service provider that can meet the Board's needs (why use a host service in Ottawa?)? Were second opinions on the service quality obtained? Were security and privacy assessment for these platforms and services reviewed before entrusting the personal information to these businesses and their technical offerings? Were references and reviews referred to? I would estimate, given the rudimentary information publically available about the server hosting, a considerable degree of it being rather negative, that it is not the level and quality necessary for the purposes of the Board, and the rather damning review by the IT consultant certainly reflects this.

Further, the service provider that was "responsible for creating the web site and ensuring security measures were in place for the software", and that "recommended" the above questionable and demonstrably unreliable server hosting service, appears to have let the Board down. The Board has a duty to the individuals whose information they collect, be that a client an employee or contractor, to ensure it is adequately protected, and should take steps to ensure there is some confidence in the products and services they entrust this information to. Again, it seems that appropriate business processes and governance were not in place to ensure high quality services were used, or what was in place failed to identify the risks attributable to the services and technology that the Board was entrusting its data to.

My final comment is to the Board and like organizations and equally to their funders. We are now in an age where electronic information, the internet, software, "cyberspace" in

fact have overtaken the tangible landscape of previous generations, those of bricks and mortar, paper and pen, manila envelopes, "in" boxes, and physical filing cabinets with metal keys. It is imperative that such organizations review their approach to information management in today's digital landscape, and on a regular basis rather than waiting for troubles to arise.

Organizations also need to educate themselves in the new ways of doing business using current electronic technology, so that they are not entirely reliant on "experts" but have some frame of reference that would allow them to reconcile the advice given by "experts" with their own knowledge, business needs, and expectations.

Finally, while I see many failures by the Board in this case, I also see a Board put into a position by the GN that they were likely to fail. A solution needs to be found in relation to this issue of dedicated IT funding for such organizations so as to ensure that the mandate of such organizations includes clear emphasis on the protection and best handling of the information in their custody and control.

FINDINGS

1. I find that ATIPP fully applies to the Legal Services Board, in that it is clearly listed as a "public body" in the regulations for the ATIPP Act, and further, as a "public agency" in the Financial Administration Act.

2. I find that the Board did not ensure reasonable security arrangements had been made against such risks as unauthorized access, collection, use, disclosure or disposal of personal information in its custody and/or control. The Board very well may have felt they had made such arrangements, but it placed all of its reliance on the word of a third party, and did not recognize it also needed to make efforts in this regard. The Board failed to ensure in the integrity of the services they

entrusted the information to, and did not review the security of their information on a regular basis. The Board breached both the Act and the requirements of the NU Privacy Management Manual to analyze risks and address those risk prior to disclosing information to these electronic systems.

3. The Board has yet to confirm that it has provided notification to the affected individuals. The NLSB did notify my office as required. It is uncertain if the NLSB immediately notified the GN, or that such notification is a clear requirement of any contractual agreement between the two, but it is possible the GN may have been able to assist with mitigating risk to those affected by supporting the notification process, and as the NLSB did not have resources to do so, the GN in my opinion should have been notified and asked to assist. If the NLSB is still struggling to notify individuals because of a lack of resources and the GN has not already been directly made aware of the details of his breach, the NLSB should notify the GN directly.

4. The Board did take immediate steps to address short terms risk once the vulnerability was detected, but has not identified how it intends to prevent long term risks to the data that it currently holds or collects. I do find that the Board took its responsibility seriously and took immediate steps to address the breach, recognizing their lack of expertise and quickly hiring a subject matter expert to inform them about these technical risks, but additional long term measures, such as staff and Board training, completing PIA's, and updating policies and procedures, should be completed.

RECOMMENDATIONS:

I make the following recommendations:

1. If not already done, I recommend that the NLSB identify individuals who have potentially been impacted by the breach, and directly contact those who were, at the time of the discovery of the breach, active clients whose contact information can be verified, to notify them of the breach.

2. In addition, I recommend that the NLSB notify the public of the breach, including:
    a) written notice in the three official languages, to be posted in public spaces in each community affected;
    b) notice by way of public service announcements (local radio and television channels) and on the NLSB web site.

    The notices should outline the nature of the breach, the kinds of information at risk, the time period during which the information was vulnerable, the kinds of risk that individuals need to be aware of and the name of the person within the NLSB who can be contacted for further information.

3. I recommend that the NLSB identify an employee within the organization who has the requisite knowledge and understanding of the breach to field any queries received as a result of the publication of the notices outlined above, and that this individual receive the support, training and time necessary to address questions from the public.

4. I recommend that in the event of a future privacy incident, when the Board knows or has reason to believe that a breach of privacy has occurred with respect to an individual's personal information under the public body's custody and control, and there is a real risk of significant harm, that it take reasonable steps to notify the individual or individuals of the breach of privacy directly and without delay.

5. I recommend that the NLSB consider officially notifying the GN and determine if the GN may offer support to the NLSB in relation to the notification of affected

individuals and other supports the GN may be able to offer in mitigating related risks.

6. I recommend that a Privacy Impact Assessment and a Threat Risk Assessment be conducted as soon as possible on the records management systems currently used by the NLSB, and that appropriate safeguards be implemented as necessary to protect and secure personal information held in the custody and control of the NLSB. When contracting out services related to records storage and application hosting I recommend that PIAs be done to ensure the information security products and services received meet or exceed industry standards, and accountability is built into service contracts. Within this I recommend the Board ensure, to the extent possible, that all information is stored within Canada.

7. I recommend that the NLSB immediately designate one individual as the designated privacy officer for the organization. The COO is clearly responsible for account management of electronic systems, and the CEO is responsible for the overall management and direction of the LSB, but there does not appear to be a person clearly designated and tasked specifically to oversee access to information and protection of privacy on a broader scale, including ensuring that the NLSB meets its legislated requirements under the Act and that privacy and security best practices are incorporated into its governance and day to day operations. Overtly assigned tasks in this regard, for example, ensuring all staff meet a certain level of privacy awareness training, would assist in ensuring this area of responsibly does not become submerged beneath other priorities of the NLSB, and would help to prevent privacy and information security from falling through the cracks in future.

8. I recommend that the NLSB ensure it has a privacy and security framework that reflects the ten internationally recognized principles of privacy and security of

personal information, and includes the necessary completion of PIAs, staff training, robust roles-based access and auditing for system applications, and having a breach management plan in place, as well as a critical incident action plan to aid in swift, strategic, and legislatively compliant responses to privacy events.

9. All things considered, I recommend the NLSB engage in a positive "reboot" on privacy and security to establish a high level of excellence and affirm its operational culture of privacy, to more adequately support the Board and staff members in making privacy protective decisions, and to provide the basic knowledge and tools necessary to be successful in protecting privacy and maintaining information security. To achieve this end, I recommend that the Board take steps to host a privacy and cyber awareness day annually, and its members, the administration, and contracted staff of the NLSB partake in related training led by a subject matter expert(s). This approach will positively infuse privacy and security awareness, and ensure all have a similar basic level of understanding of how to protect privacy and security of personal information held in the custody and control of the NLSB.

10. Because these recommendations are directed to the Minister of Justice as the designated "head" of the NLSB, I also recommend that the Minister of Justice ensure that funding provided to the Board includes adequate resources to appropriately manage end-of-life systems, replace legacy hardware and software with current, up to date and secure hardware and software, and to ensure systems are maintained with an appropriate level of functionality and security. Funding necessary to maintain electronic records and systems should be a regular line-item in funding agreements between the GN and the NLSB if this is not already the case.

11. I recommend that the NLSB develop a robust and tangible privacy and security framework that reflects internationally recognized principles of privacy and security of personal information, and includes the necessary completion of PIAs, staff training, robust roles based access and auditing for system applications, as well as having a breach management plan in place and a critical incident action plan to aid in swift, strategic, and legislatively compliant responses to high risk privacy events.

12. I recommend that after any major privacy breach event, all staff and Board engage in privacy training to raise awareness of the root causes of a breach and how to prevent similar errors in the future.

13. I highly recommend that staff be encouraged to report circumstances or incidents where data or personal information handled by the NSLB is or may be at risk.

Elaine Keenan Bengts
Information and Privacy Commissioner