Office of the Information and Privacy Commissioner for Nova Scotia

---

INVESTIGATION REPORT IR19-01

Department of Internal Services
Freedom of Information Access (FOIA) Website

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

TABLE OF CONTENTS

Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner
Catherine Tully

INVESTIGATION REPORT

January 15, 2019

Department of Internal Services

Commissioner's Message

Can privacy and progress co-exist? It seems that there is an endless barrage of stories of privacy breaches. Some may argue that in this age of innovation, we've simply reached the point that privacy cannot be meaningfully protected. But, must we abandon our right to privacy in order to achieve progress?

This investigation goes to the heart of this question because it reveals that these breaches involving a new and innovative system were easily preventable.

What standard should we hold government to? We've entrusted government with our personal information, do we simply have to accept that mistakes will happen or should we expect more? The narrative that privacy and innovation are incompatible is untrue, at best, and damaging to our democratic institutions, at worst. A failure to protect the privacy rights of Nova Scotians contributes to the erosion of citizens' trust in the government.

Ultimately, this series of privacy breaches was caused by a serious failure of due diligence in the selection and deployment of a new technology tool. The need for independent and knowledgeable technical assessment and security testing of a tool being considered for deployment cannot be overstated in the age where applications, software and web enabled technology tools of all sizes and descriptions are being developed by vendors and regularly marketed to governments. Taking the time to diligently assess a tool at all stages of a project is fundamental to ensuring that personal information held by government is respected and protected.

One significant and troubling factor is that the technology under investigation was implemented by the group responsible to lead privacy across all government departments. This investigation has highlighted that significant work is required to mature the government's privacy program to ensure that privacy is built into projects from the ground up. This will require training and a renewed commitment to completing privacy impact assessments before money is spent and

systems are built. In essence, it will require that government departments ensure that all new projects involving personal information are subjected to critical privacy analysis, security verification and a willingness to delay or abort projects where risks cannot be fully defined or adequately mitigated in time to provide effective protection. Leadership in this area requires the creativity and courage to innovate in a way that will not only make Nova Scotia a leader in data and technology, but also in privacy rights and citizen trust.

Is progress without the protection of privacy really progress at all? This investigation has demonstrated that we can have it both ways. Innovation that protects privacy rights is not only possible, it is essential to maintaining the public's trust in government and to ensuring that innovation benefits citizens.

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

Executive Summary

[1] Over the course of a one-month period in early 2018, two individuals accessed almost 7000 documents containing personal information on the Department of Internal Services' (Department) public Freedom of Information Access website (FOIA website). The first incident (breach #1) resulted in police involvement. Eleven additional unauthorized accesses (breaches #2 - #12) identified by the Department were committed by one other individual. In total, 740 individual access to information applicants were notified of the breaches.

[2] The immediate cause of the privacy breaches was a design flaw in the FOIA website. This flaw created a well-known and foreseeable vulnerability that was not detected by the Department prior to launching the FOIA website. Ultimately, this series of privacy breaches was preventable and was caused by a serious failure of due diligence in the deployment of a new technology tool.

[3] As part of responding to this series of privacy breaches, an independent security firm conducted a full security assessment. That assessment revealed more than two dozen other vulnerabilities in the FOIA website system that the Department was unaware of.

[4] This investigation identified shortcomings in the project management, security review and privacy impact assessment (PIA) process that resulted in the implementation of the FOIA website with these vulnerabilities. Those shortcomings included:

- The Department incorrectly rated the risks as low based at least in part on the trusted relationship with the vendors. This relationship inspired a sense that the projects were low risk which permeated all aspects of the project development and deployment.
- The project management process and user testing did not incorporate any technical testing and failed to recognize the risk associated with the storage database design – specifically the storage of public and private documents in the same database.
- The short time frames created a stressful environment and compromised the quality of system testing.
- The Department failed to act on information that there were risks associated with the lack of website vulnerability scanning.
- The Department failed to complete a timely and specific security threat and risk assessment after the clear recommendation to do so from Department Cyber Security staff and the Information and Privacy Commissioner.
- The privacy impact assessment process was neither diligent nor rigorous.
- The Department relied on one vendor for technical security measures included in the PIA instead of conducting its own analysis.
- The Department failed to incorporate risks and mitigations identified during the project into the PIA.

[5] In summary, the processes lacked due diligence. Risk assessments lacked rigor, at times not going beyond passive acceptance of untested conclusions or unverified claims nor beyond blind trust in vendor claims. The *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) requires that public bodies make reasonable security arrangements to protect personal information. The Department failed to make reasonable security arrangements for the FOIA website as required by s. 24(3) of *FOIPOP*.

[6] Following discovery of the privacy breaches, the Department undertook a process to manage the privacy breaches. This process must also satisfy the reasonable security requirements of *FOIPOP*. With respect to the privacy breach management undertaken by the Department, the key findings in this report include:

- The Department's initial containment action of shutting down the website was reasonable but the breaches are not contained. More than 600 documents containing personal information were downloaded onto an unknown computer and have not yet been recovered or secured.
- The Department's initial notification efforts were reasonable and timely. However, there are an unknown number of third parties affected by the download of the 600 plus documents who have not been notified.
- The Department lacks a comprehensive, methodical plan to prevent a similar occurrence in the future.

[7] I make six recommendations to the Department of Internal Services:

1. Strengthen privacy leadership in government and due diligence in the privacy impact assessment process.
2. Take immediate steps to contain the breaches that resulted in the download of 618 documents containing personal information to a private computer that has not been secured by the Department (breaches #2 - #12).
3. Take all reasonable steps necessary to notify individuals affected by the download of the 618 documents containing personal information (breaches #2 - #12).
4. Conduct an internal post-incident review as an aid to ensuring that the Department fully understands the causes of these breaches and has identified all reasonable steps necessary to prevent future similar errors.
5. Conduct an inventory of technology solutions, devices and applications across government and rate their vulnerabilities. From there create a plan to mitigate cyber security vulnerabilities beginning with systems storing the most vulnerable personal information and/or having the highest risk.
6. Clarify and strengthen the role of the Architecture Review Board.

[8] This investigation, along with other recent privacy breach investigations, have made it clear that our privacy laws are woefully lacking. As a result, I have again written to the Premier to recommend that the changes I recommended almost two years ago be implemented. My letter focuses in particular on amendments to improve privacy breach management, notification and the powers of my office to conduct investigations.

1.0 Purpose and Scope

1.1 Introduction

[9] This privacy breach investigation report arose out of the Province of Nova Scotia's largest known data breach. On April 9, 2018, the Department of Internal Services (Department) notified my office of the unauthorized access to and download of thousands of records from its Freedom of Information Access website (FOIA website) by an unknown actor associated with one Internet Protocol (IP) address. This first identified privacy breach appeared to have involved an automated program to download every document stored in the database behind the website.

[10] The FOIA website went live on January 6, 2017 and provided twofold functionality - one private and one public. The account portal portion of the website was intended to be private and allowed individuals to create an account for making access to information requests under the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*), pay fees and receive disclosure packages in response to requests. Access to information requests and response packages included, in some cases, highly sensitive personal information particularly where individuals requested access to their own personal information held by government. The public disclosure log portion of the website provided public access to disclosure packages requested by other individuals which contained general information and were approved for release to the public without the need to make an access to information request. Documents on the public disclosure log could be accessed by anyone with an internet connection.

[11] The Department disabled its FOIA website at 8:26 a.m. on April 5, 2018, following receipt of information from a government employee that documents containing personal information could be obtained by changing the web address (URL) of documents on the public disclosure log.[1] By investigating this initial report, the Department eventually identified a total of 12 privacy breaches.

[12] Privacy breach #1 was discovered after an initial review of the website's activity logs. The Department's further review of the activity logs subsequently identified an additional 11 instances of unauthorized download activity. The identity of the individuals involved in the 12 instances of unauthorized access is known only by the IP address of the computer used in the activity. Privacy breaches #2 through #10 are IP addresses assigned to the Atlantic School of Theology. Privacy breaches #11 and #12 are two different and private IP addresses hosted by the Bell Aliant network. These IP addresses were later determined to also be associated with the Atlantic School of Theology (AST). The IP addresses are assigned to visitors when AST grants guest access to its wifi. The evidence also suggests that breaches #2 through #12 all involved just one individual.

[13] While the Department was able to identify activity in 12 instances that appeared to be unauthorized, the full extent of the potential breach of personal information will never be known. There may have been other incidents where individuals inadvertently or purposefully accessed

[1] The Department acknowledged that the employee's access to these records was also a privacy breach. The Department properly followed up with this individual to ensure that the records were appropriately and fully deleted. Given the circumstances and the full containment by this employee, this breach is not included in my investigation report.

third party personal information on the FOIA website that have not been identified. It was only where individuals repeatedly accessed numerous documents that the pattern of inappropriate access could be identified through the review of the website activity logs. There is no practical way of identifying one-off or limited unauthorized accesses. In addition, there are no activity logs available for the first four months that the FOIA website was in operation.

[14] The Department reported breach #1 to the Halifax Regional Police (HRP) on or about April 7, 2018 as a possible crime. The HRP obtained a production order to require the internet service provider to disclose the physical address associated with the identified IP address. After obtaining a search warrant, the HRP then searched the location and on April 10, 2018, seized equipment containing the documents downloaded by an individual. On May 7, 2018, the HRP announced the conclusion of its investigation of the FOIA website download activity, resulting in no criminal charges.

[15] In total, 740 individual access to information applicants were notified of the breaches and almost 7000 documents containing personal information were accessed.

[16] Based on the information provided to this office on April 9, 2018, I notified the Department that I was initiating an investigation. This report describes our investigation into the FOIA website privacy breaches and the Department's response to those breaches. The Auditor General initiated a performance audit related to the FOIA website. Our staff collaborated where it made sense, while maintaining the independence of the two offices.

1.2 Jurisdiction

[17] The Department of Internal Services is a public body within the meaning of the *Freedom of Information and Protection of Privacy Act*. Under the Act, public bodies have a responsibility to "protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."[2]

[18] Pursuant to the *Privacy Review Officer Act* (*PRO*), Nova Scotia's Privacy Commissioner has the authority to "initiate an investigation of privacy compliance if there are reasonable grounds to believe that a person has contravened or is about to contravene the privacy provisions and the subject-matter of the review relates to the contravention."[3]

[19] The information provided by the Department on April 9, 2018 provided reasonable grounds to investigate the Department's compliance with *FOIPOP*'s privacy provisions.

[20] My office also received two privacy complaints from individuals affected by these breaches. We investigated these individual complaints simultaneously under the provisions of section 6(1) of the *Privacy Review Officer Act* and this report serves as an outcome to those complaints as well.

[2] *FOIPOP*, s. 24(3).
[3] *PRO*, s.5(1)(b).

1.3 Investigative process

[21] For this investigation, my team gathered a total of more than 100 documents from the Department including:

- policy documents
- service provider contracts
- privacy impact assessments
- security threat and risk assessment and security audits
- security incident response plan
- monthly third party website status reports
- management committee meeting minutes
- a chronology of privacy breach response activity
- inventory of records and affected individuals
- website activity logs
- internal and external communications about the FOIA website and incident response
- project charters
- project meeting minutes
- project closeout report
- project business requirements
- email communications

[22] My investigation staff interviewed 20 government employees representing all aspects of the development, procurement, implementation and operation of the FOIA website as well as members of the Department's executive team responsible for the privacy program and FOIA website project. This included employees from the Department's Project Management, Business Relations, Information Access and Privacy, and Enterprise Architecture units. My investigators also interviewed representatives of the Halifax Regional Police, the government employee who alerted the Department to the issue, staff from Saint Mary's University and the Atlantic School of Theology, and four different website users individually affected by the breaches.

2.0 Background

[23] The Information Access and Privacy (IAP) Services group was formed April 1, 2015 by centralizing information access and privacy staff from across several government departments into one centralized service at the Department. The mandate for this group is to provide information access and privacy policy, practices, services and resources for government.[4] Upon its formation, the unit quickly identified that the software used to track and manage access to information requests was out of date and cumbersome to use. The IAP Services unit sought expertise from other units in the Department to identify a suitable replacement technology and this resulted in the deployment of a case management software solution, AccessPro, on April 5, 2016.

[24] The IAP Services group deployed the new FOIA website, an add-on module to the AccessPro solution, on January 6, 2017. This new website had a dual intention: (a) make it easier for citizens to request access to information and (b) increase government openness and transparency by making more information available without needing a formal access to information request. The new FOIA website was announced by the Department in news releases on September 27, 2016 and November 24, 2016.

[4] Information Access and Privacy Services, pamphlet prepared for the 2018 Reverse Trade Show.

[25] The FOIA website was an important step forward in facilitating and advancing access to information rights of Nova Scotians. It allowed citizens to make online access to information requests and to receive responses electronically. It also allowed citizens to receive copies of previously released records without the need for an access to information request. The FOIA website made a significant contribution to open government in Nova Scotia.

[26] There were two third party companies involved in the two projects associated with deploying this technology. CSDC, a technology company, was the vendor who developed the products and sold the product licenses for AccessPro and the FOIA website to the government which were deployed on its platform, Amanda 7. Unisys, a different technology company, provided project management and configuration services during the project development and implementation phases of both AccessPro and the FOIA website. Unisys servers provide cloud-based hosting and data storage for both AccessPro and the FOIA website in a private data centre located in Nova Scotia. Unisys also provided ongoing technology support and services for AccessPro and the FOIA website.

[27] The Province of Nova Scotia operates multiple technology solutions on multiple versions of the Amanda platform across numerous departments.[5] The relationship between the Province of Nova Scotia, CSDC and Unisys is long-standing. AccessPro and then the FOIA website were the first solutions to deploy live on the Amanda 7 version of the platform in a cloud environment hosted outside of the Province's own data centre.[6]

[28] The payment portion of the FOIA website was hosted separately by Unisys. Although a user could seamlessly make payments from the FOIA website, the user was actually redirected to the Province's online payments infrastructure when making a payment. Payment information and transactions were at all times separate from the FOIA website. The Province's online payment system is outside the scope of this investigation.

[29] When using AccessPro and the FOIA website, IAP staff uploaded documents as "attachments" onto a single database on the Unisys cloud server. The basic URL (website address) was common to all uploaded documents except for a unique file identification number (RSN) added to the URL for each document. RSN numbers were assigned to documents in sequence, in the order in which they were uploaded. Documents intended for individuals were intermingled with documents intended for the public disclosure log within the storage database.

[30] IAP staff set each attachment's status and details within AccessPro. Attachment status was assigned to designate that documents were either approved for the public disclosure log, approved for disclosure to an individual applicant only or were not approved. Unredacted

[5] Departments using solutions on a version of the Amanda platform include: Department of Agriculture, Food and Safety, Alcohol & Gaming, Service Nova Scotia, Department of Environment, Department of Labour and Advanced Education, Registry of Joint Stock Companies, Consumer Protection, Fuel Safety, Office of the Fire Marshall, Provincial Tax Commission, Driving Schools/Instructors, Tourism Culture & Heritage, Occupational Health and Safety, Office of Economic Development, Workers' Compensation Board, Department of Community Services and Department of Lands and Forestry.

[6] Other applications operating on the Amanda platform do not have public-facing web access, and/or store only publicly available information. Other technology solutions operating in a cloud-based environment were not using Amanda 7 or AccessPro.

documents that were being processed for access to information requests were not uploaded to the Unisys database. The document's status served as a display filter for the database. The FOIA website was a presentation layer sitting on top of the AccessPro case management software and storage database. The presentation layer used the status filters to determine which documents to display on the public disclosure log website. Documents not approved for the public disclosure log could be displayed internally with the AccessPro case management system.

[31] In the case of documents approved for display on the public disclosure log, the link was displayed in a document index. A keyword search bar was also used to display links to documents approved for public disclosure that contained the searched words. Clicking on a displayed link would take the user directly to the document specified in the link and input the URL in the browser's address bar where it was fully visible.

[32] In the case of files intended for an individual, a link was provided in a message delivered through the portal to the individual only. Clicking on the link would take the user directly to the document specified in the link and again display the full URL in the browser's address bar. A user seeing a few document URLs could easily detect that the web address was common across the documents except for the unique document identification number.

[33] This type of website serving as a landing page for a web-enabled database of documents which are not themselves accessible by web browser is very common. The technical community calls this the "deep web" – not to be confused with the "dark web".[7] The deep web refers to data which can only be accessed directly, not by typical browsing, and is material that won't be captured using regular search engines. This is because the landing website is indexed by the search engine but each document within the database is not. This type of database includes things like library collections databases and open access science databases, many of which are free to the public. It is commonly known that small changes to the URLs of these types of websites can result in access to other documents contained in the database.[8]

[34] A quick test of this using the Halifax Public Libraries database of collections demonstrates how it works. By browsing to the main page and following the links or by keyword searching using the catalogue search bar the user can find any item in the library's collections catalogue. Clicking on the item's link brings the user to the item's page and puts the URL for that item, including its unique identification number, in the browser's address bar. Changing just the number in the address bar takes the user to a different item directly (without any further browsing), although the user won't know what item he or she is moving to or if the new number inputted corresponds to an item in the database until after hitting "Enter". Different search

---

[7] https://www.wikihow.com/Search-the-Deep-Web; https://www.wikihow.tech/Download-a-Website; https://tech.co/what-is-the-deep-web-2018-05; https://darkwebnews.com/deep-web/10-deep-web-research-tools/; https://darkwebnews.com/deep-web/; https://www.youtube.com/watch?v=Pchg6F_koOw; https://en.wikipedia.org/wiki/Deep_web; accessed November 19, 2018.

[8] The OWASP (Open Web Application Security Project) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate and maintain applications that can be trusted. All of the OWASP tools, documents, forums and chapters are free and open to anyone interested in improving application security. OWASP periodically publishes a Top 10 list of vulnerabilities in web applications as an awareness tool. The design flaw in the FOIA website, referred to as Insecure Direct Object References, was first included on the OWASP Top 10 list in 2010. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2010 accessed January 3, 2019.

engines and automation tools can be found online with a small amount of research to make the process of gathering up documents available from this type of web-enabled database faster. This process is referred to on Wikipedia as 'hoovering' (sucking up) large volumes of data quickly.[9]

[35] Web-enabled databases containing documents not intended to be publicly accessible require security features and/or architecture that prevents protected documents from being displayed if the document's URL is entered in the address bar by a user not authorized to view the document. Examples of this type of restricted access web-enabled database are also common, including personal banking and online email accounts that function in a similar way.

[36] Nova Scotia's FOIA website provided the landing page for a database that contained a mix of public and private documents. Documents intended for the public disclosure log did not contain personal information. They were always intended to be released publicly. Documents intended for individual recipients covered a range of document types and contained personal information with varying degrees of sensitivity. Documents intended for individual recipients included copies of access to information request forms, decision letters, notification of time extensions, fee estimates and disclosure packages. Disclosure packages that provided applicants with their own personal information requested from a government department contained the most detailed personal information which could include personal health information, financial information, unique identifiers, sensitive or intimate details of eligibility for and access to government services, and details of interactions with the Department of Community Services, the justice system.

[37] Two individuals filed separate privacy complaints with the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) in relation to these breaches. Their cases provide examples of the impact to individuals. One complainant's name and email address on correspondence related to a request for access to general government information was disclosed. This complainant expressed dissatisfaction with the quantity and quality of information provided to affected individuals, saying that it was too vague to give individuals assurance that the matter was being appropriately addressed.

[38] The second complainant applied for access to her own personal information held by the Department of Community Services. In this case, the application and decision letter contained sensitive personal identifiers such as dates of birth. The disclosure package contained detailed information about the applicant and several of the applicant's family members, including Social Insurance Number, details of government involvement with the family, as well as details of occurrences, vulnerabilities and challenges involving family members. The records also contained the community of residence, work and school locations, and detailed contact information. The complainant described a sense of extreme violation provoked by learning that this highly sensitive personal information was not protected and was breached by an unknown individual. Not knowing the status of who had the documents and what was done with them caused severe anxiety. In addition, this applicant informed our office that while she had received notification of the breach, other individuals mentioned in the documents did not.

[9] https://en.wikipedia.org/wiki/Web_scraping; accessed November 19, 2018.

3.0 Issues

[39] The issues arising from this investigation are:

1. Did the Department have reasonable security arrangements in place for its FOIA website in compliance with s. 24(3) of *FOIPOP*?
2. Did the Department take reasonable steps in response to the privacy breaches as required by s. 24(3) of *FOIPOP*?

4.0 Analysis and Findings

4.1 The meaning of "reasonable security"

[40] *FOIPOP* requires that public bodies protect personal information within their care and control "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."[10] Both issues articulated above evaluate the Department's actions against this statutory standard.

[41] I have discussed the meaning of "reasonable security" in Nova Scotia's privacy laws on several occasions.[11] Below, I have summarized 11 factors commonly considered when evaluating the reasonableness of a public body's security.

1. **Contextual:** Reasonable security is contextual. Overwhelmingly, what is clear in the case law is that reasonable security is intended to be an objective standard measured against the circumstances of each case.
2. **Sensitivity:** The more sensitive the information, the higher the security standard required.[12]
3. **Not technically prescriptive:** Reasonable security is not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect privacy vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.[13]
4. **Foreseeability:** Reasonable security must take into account the foreseeability of the breach and the harm that would result if the breach occurred. The higher the risk of a breach, the higher the security standard will be.[14]
5. **Trust:** For public bodies, particularly government departments, reasonable security also includes reasonable assurances to the public that the government is taking privacy protections seriously. Where government departments hold personal information, the public has an increased level of trust that their personal information is being protected.

---

[10] *FOIPOP* s. 24(3).
[11] NS Investigation Reports IR17-01 and IR16-02, for example. In both reports, I noted that the summary of considerations supplied above are consistent with every other jurisdiction in Canada.
[12] *Electronic Health System (Re),* 2010 BCIPC 13 (CanLII) at para 130.
[13] *Electronic Health System (Re),* 2010 BCIPC 13 (CanLII) at para 129.
[14] BC Investigation Report F06-01; Canada OPC, Alberta OIPC, "TJX / Winners"; Alberta Order H2005-IR-001.

This creates a high standard for government departments to ensure security measures are in place.

6. **Industry standards**: Industry standards, codes of practice or established user agreements can illuminate security requirements provided that following those practices reaches the contextual standards of reasonableness. If the industry standard is less than the contextual evidence demonstrates reasonable security requires, the industry standard is not sufficient. Simply accepting that a third party or contractor will follow industry standards or established user agreements does not demonstrate reasonable security.[15]
7. **Cost:** The cost of implementing a new security measure may be a factor but it is on an extreme scale – reasonable security does not require a public body to ensure against a minute risk at great cost. However, a public body cannot dilute security by insisting on a cost efficiency in one area and refusing to pay for reasonable security in another.[16]
8. **Life cycle:** Reasonable security applies to the entire life cycle of the records.
9. **Format:** The medium and format of the records will dictate the nature of the physical, technical and administrative safeguards.
10. **Timing:** Reasonableness requires a proactive and speedy response to known or likely risks.[17] Time is of the essence in any privacy breach. The safeguards must ensure that should a privacy breach occur, the public body and the individual will learn of the breach and have response measures in place quickly and efficiently.[18]
11. **Documentation:** Procedures for establishing reasonable security must be documented and public bodies must be prepared to respond to the idea that employees won't always follow the documented procedures.[19]

4.2 Did the Department have reasonable security arrangements in place for its FOIA website in compliance with s. 24(3) of *FOIPOP*?

4.2.1 *The cause of the breaches*

[42] In order to assess whether or not the Department made reasonable security arrangements for its FOIA website it was first important to understand the technical cause of the breaches.

[43] As noted above, the Department confirmed early on that the means by which individuals were able to access private records was that they were able to change the document identification number in the URL and that those changes led, in many cases, to documents that were intended to remain private being disclosed. The database did not apply the document filters when the document was navigated to directly by the URL. That meant that a user could access any document held in the database by changing the RSN number contained in the URL. Documents could be accessed randomly or in sequence.

[44] The activity of the users who accessed documents by modifying the URL from the FOIA website demonstrated different approaches. The user behind breach #1 for example started with

---

[15] Ontario Order MC09-9; BC Investigation Report F06-01.
[16] BC Investigation Report F06-01.
[17] BC Investigation Report F06-01; Alberta Order P2013-04; BC Investigation Report F12-02.
[18] Alberta Order H2005-IR-001.
[19] Alberta Order H2005-IR-0010; Ontario Order HO-001; BC Investigation Report F06-01; Alberta Order P2010-008.

downloading five different documents, not in sequence, from the public disclosure log. The user then attempted different RSN numbers, not in sequence, several of which did not correspond to documents in the database, then moved to starting at a random RSN number and downloaded a smaller series in sequence. Finally, the user downloaded every document (public and private) starting at RSN=0 to RSN=40,000.

[45] As noted earlier, the evidence suggests that breaches #2 - #12 all involved the same individual.[20] This individual began his[21] search with a public document. From there he began accessing records by manually changing the URL in sequence, with some exceptions, jumping over some document numbers, revisiting some document numbers, or entering typos in document numbers. This suggests an individual and manual approach.

[46] The evidence of Department witnesses confirmed that the website allowed for this type of searching because of its construction; that is, it functioned this way because the program coding from the product vendor CSDC set it to function this way. If all of the data within the database was intended to be public, this functionality would not be problematic. For a database intending to restrict access to some documents, Department witnesses acknowledged that this functionality posed a vulnerability.

[47] In summary, AccessPro and the FOIA website were constructed such that documents uploaded by IAP staff were stored in one file storage location. The status marker placed on the document by IAP staff operated as a display filter and that was the only thing distinguishing private and public documents within the storage database. The database did not use the display filters to distinguish authority to view a document if a user navigated directly to the document using the direct document URL. The FOIA website, through both the public disclosure log and the individual account portal, provided a clearly visible complete URL and RSN patterned structure every time a user clicked on a document link that he or she was authorized to view.

Finding #1: FOIA website design was the immediate cause of the privacy breaches.

[48] The design of the Department's FOIA website is common for websites that enable access to databases storing public information but it contains a significant security vulnerability if used for information intended to be private. Deploying a website and storage database with this design for storing and disclosing Nova Scotians' personal information without any mitigating security features was the immediate cause of these privacy breaches.

---

[20] Two facts have lead us to the conclusion that breaches #2 through #12 were committed by the same individual. First, our review of the patterns of documents accessed in breaches #2 - #12 revealed that the individual followed a sequence of documents through multiple sessions. For example, on Friday March 9th, one IP address at AST started at RSN=8540, a disclosure package intended for an individual, and accessed documents in sequence ending with RSN=8575. On Monday March 12th, another IP address at AST started at RSN=8576 and accessed documents in sequence ending with RSN=8595. On Tuesday March 13th, another IP address at AST started at RSN=8596 and accessed documents in sequence. Second, officials at the Atlantic School of Theology confirmed that when an individual signs onto the public website, the Saint Mary's University system logs a device identifier number. The device identifier for each of the accesses to the FOIA website at AST was the same meaning that the same device was used.

[21] The identity and gender of the individual is unknown.

4.2.2 *Contributing factors*

[49] How did the Department come to implement the FOIA website with this unmitigated vulnerability? What factors contributed to failing to identify and mitigate this risk? These are questions that must be addressed in order to evaluate whether or not the Department made reasonable security arrangements to protect personal information held on the FOIA website against the risk of unauthorized access as required by s. 24(3) of *FOIPOP*.

[50] As a result of this investigation, we identified shortcomings in three core processes that resulted in the implementation of the FOIA website with this vulnerability:

i. project management process,
ii. security review process, and
iii. privacy impact assessment process.

i. The project management process

[51] Following the Department's preferred methodology,[22] when IAP Services began searching for a new case management technology solution, the Department considered first solutions using platforms already in use. The Amanda platform is widely used across the Nova Scotia Government. The AccessPro solution was being used as an access to information case management software by other public bodies across the country and could be configured on the Amanda 7 platform. The solution could be configured and supported by Unisys under the umbrella of its existing, long-standing contract and this provided the unit with access to additional supports to bring the project forward. These factors are reflected in the Project Charter for the AccessPro deployment and were referred to by Department witnesses as creating a sense of low risk in relation to this technology solution.

[52] The government's relationship with Unisys was described by several witnesses as a trusted partnership that was comfortable after years of service. This factor was referred to by several Department witnesses as also contributing to a sense that the project was low risk. Department witnesses confirmed that the decision to use the AccessPro technology solution on the Amanda 7 platform hosted in the Unisys cloud environment was made following presentations from the vendors sometime in 2015 and the creation of a rudimentary test of business requirements compared to product capabilities called a "swim lane exercise".

[53] Department witnesses acknowledged that the AccessPro technology was not reviewed in depth prior to making the decision to use it. Department witnesses also acknowledged that the contract contained some security and technology provisions, but they were not reviewed by those who signed for the Department because operational responsibility for deploying the solutions had transferred to others under the departmental reorganization by that time. Department witnesses also acknowledged that the contract provisions were not reviewed by those conducting the privacy impact assessment prior to the contract being signed by the Department, even though contract provisions were called for as a risk mitigation strategy within the PIA for AccessPro.

[22] Platform over Best-of-Breed Standard PRI-13-002, November 7, 2013. Confirmed by CIO, Sandra Cascadden.

[54] Having made the decision to deploy this technology before any review of the product or services placed significant pressure on the processes that followed to catch any vulnerabilities and mitigate them before deployment. The documentation of processes that followed the decision to use the AccessPro technology solution include business requirements documents, Project Charter, Architecture Review Board decisions, Project Closeout Report and privacy impact assessments.

Process Documentation	AccessPro	FOIA Website
Business Requirements	Start: Nov. 20, 2015 Complete: March 7, 2016	Start: Aug. 10, 2016 Complete: Oct. 25, 2016
Product Purchase and Contract Signed[23]	March 31, 2016	n/a
Project Charter	Start: June 24, 2015 Complete: Feb. 19, 2016	Start: May 18, 2016 Complete: June 14, 2016
Project Meetings & User Testing	Start: Feb. 10, 2016 Complete: April 6, 2016	Start: July 25, 2016 Complete: Dec. 2016
Architecture Review Board[24]	March 22, 2016	Sept. 30, 2016
Product Launched Live	April 5, 2016	Jan. 6, 2017
Privacy Impact Assessment	Start: Jan. 26, 2016 Complete: Aug. 10, 2016	Start: Aug. 15, 2016 Complete: Jan. 3, 2017
Project Closeout Report	n/a	Feb. 23, 2017

[55] The Architecture Review Board (ARB) reviewed one component of the AccessPro technology deployment.[25] On March 22, 2016, this component review was given approval as a pilot status for six months, based on cyber security concerns raised at the ARB meeting. Department witnesses responsible for the project stated that they were unaware the project had been given a pilot status. Although the ARB minutes identify individuals responsible for follow-up, the project's pilot status was never reviewed.

[56] Following shortly after the deployment of AccessPro, IAP Services pursued the add-on FOIA website module. The module was described as a "presentation layer" that sits overtop of the AccessPro software. The Project Charter for the FOIA website positioned the project as being based on the "recent implementation of the AccessPro case management system."[26] The Project Charter describes the new FOIA website as presenting "a low risk option that is beneficial to both government and the public, provides an easy baseline to work from and improves the unit services to both government and public."[27] The Department viewed the add-on module as a next step process and embarked on it.

[23] The contract took the form of a Change Request under the umbrella of the Master Strategic Alliance Agreement between the Governments of New Brunswick, Newfoundland, Nova Scotia, PEI and Unisys Canada Inc. This Change Request added services and ongoing support for the FOIA system within the Amanda Cloud Managed Services. The 'purchase' of the products from CSDC took the form of activating product licensing fees which corresponded with user testing and/or deployment dates.
[24] The role of the Architecture Review Board is discussed below on pages 20, 21, 42 and 43.
[25] The ARB reviewed the simultaneous use of desktop applications and Java for the old case management system and the proposed new system.
[26] FOIA website Project Charter, p.4.
[27] FOIA website Project Charter, p.4.

[57] Unisys drafted the AccessPro Project Charter and provided project management services. The Department drafted the FOIA website Project Charter and led the project in collaboration with the Unisys team. The prior decision to use this solution and the implementation of AccessPro added to the sense of trust and low risk in relation to the FOIA website.[28]

[58] The FOIA website Project Charter identifies the project as having ambitious time frames. It lists as a project constraint "very tight timelines as the project needs to be approved, executed and implemented in 2.5 months."[29] The plan was to deploy the FOIA website August 29, 2016. Ultimately, the project was deployed five months later than originally planned. Despite this delay, the Project Closeout Report still documents that the deadlines specified by the client unit (i.e. IAP Services) were too short. That document states, "In trying to meet client deadlines, the agreed to schedule was very tight. This led to a stressful environment and compromised the quality of system testing." The Project Closeout Report recommends, "Allow more time in the schedule for unforeseen and thorough system testing."[30]

[59] The testing referred to here is user testing and the Project Closeout Report documents that issues with AccessPro continued to plague the project. Department witnesses identified that there were aspects of AccessPro that did not work well and there was internal frustration with CSDC's responsiveness to fixing issues as they arose. This contributed to the Project Closeout Report's overall recommendation that "Project should not get initiated to add new functionalities to a non-stable system. First fix all outstanding issues on the existing system before embarking on a new project to add any functionality."

[60] The project documentation confirms that the project management and user testing were focused primarily on functionality from the user's perspective.[31] There was no feedback from this part of the process to the risk assessment exercises that were moving forward in tandem. User testing of AccessPro and the FOIA website would have made it clear that all documents were stored in the same location and that document status was merely a display filter. Maintaining privacy and restricted access to personal information and attachments intended for individual recipients separate from documents approved for public release was a fundamental assumption of the project. Witnesses gave evidence that this core requirement was communicated to the vendor. However, as the FOIA website project progressed, no one in project management or within the user group unit (IAP Services) questioned whether the technology solution could deliver what was intended. This occurred despite the mounting concerns within the user group about the quality of the product from CSDC.[32]

---

[28] FOIA website Project Charter, p.4. The Charter states that the unit's implementation of the new AccessPro software for *FOIPOP* tracking opened up new opportunities to manage and disclose information. Those opportunities were identified as the configuration and setup of a new portal "presents a low risk option that is beneficial to both government and the public, provides an easy baseline to work from and improves the unit services to both government and public."

[29] FOIA website Project Charter, p. 6.

[30] FOIA website Project Closeout Report pp. 4-5.

[31] During testing the Department also recognized the risk to privacy from the inadvertent publication of personal information on the public disclosure log. IAP Services developed criteria as well as a review and approval process as controls to prevent privacy breaches from staff posting in error on the website.

[32] FOIA website Project Meeting Minutes, December 1, 2016.

[61] No testing of the FOIA website was done by technical staff. An enterprise architect is the only technical staff from the Department assigned to the project in the Project Charter. He stated that his assigned focus was solely on the one component that was reviewed by the Architecture Review Board.[33] The Project Closeout Report documents that testing was done only by the IAP unit staff and states they did not have enough time to really learn the product or test it well.[34] Although the Project Closeout Report states, "risks and issues are all identified quickly and addressed objectively as a team," the technical risks associated with the solution and the lack of technical review and testing were not identified or flagged during the project management process.

[62] User testing and the FOIA website requirements implicitly expose that the fundamental premise of the storage database is for all uploaded documents to be stored together and that document statuses were display filters. This fundamental architecture is evident in the business requirements documents and the function of the site which should have raised concerns to trigger closer analysis by technical staff or requesting further product documentation for review.

[63] The sense of low risk influenced how the projects moved through the various processes to deployment. The Department failed to recognize three key factors that made the project high risk, not low risk: it was the first implementation of AccessPro on the Amanda 7 platform, it was the first ever use of the FOIA website, and both were to be hosted in the cloud and serviced by a vendor.

[64] It is critical to ask what checks were in place that could have intervened at any stage along the way to elevate the sense of risk from one of trust, because of a comfortable vendor relationship, to one of seeking verification and due diligence because of the inherent risk in deploying technology solutions, particularly when the tight time frames were compromising the ability to properly test the technology.

[65] As the Department got closer to deploying the FOIA website, it discussed providing my office with a demonstration of the website. Minutes of a meeting attended by the deputy minister, the chief information officer and the chief information access and privacy officer (who was also the project sponsor), in short, the senior executive of the Department, state, "Briefing for the Information and Privacy Commissionaire (sic) (send her the document and invite her for a demo) as just FYI: there is no possibility to accommodate any change she may request."[35]

[66] During the demonstration, which took place at the end of December 2017, I immediately recommended that a security threat and risk assessment be performed and that the Department ensure there was no ability for users of the FOIA website to access each other's documents.

[33] Approval for the Unisys mail server to be a trusted sender on the government email system.
[34] FOIA website Project Closeout Report pp. 4-5.
[35] FOIA website Project Meeting Minutes, October 24, 2016.

[67] In summary, the evidence establishes that the following shortcomings in the project management process contributed to the implementation of the FOIA website with the storage database design vulnerability:

- The trusted relationship with the vendors inspired a sense that the projects were low risk which permeated all aspects of the project development and deployment.
- The decision to purchase the technology occurred before the solution had a technical review and before any privacy impact assessment was initiated.
- The project management process and user testing did not incorporate any technical testing and failed to recognize the risk associated with the storage database design – specifically the storage of public and private documents in the same database.
- The short time frames created a stressful environment and compromised the quality of system testing.

ii. The security review process

[68] The evidence establishes that there were two potential processes available to ensure that security risks associated with the FOIA website would be properly identified and mitigated: the Architectural Review Board process and a security threat and risk assessment (STRA). STRAs are a recommended step in the broader privacy impact assessment process discussed below.

[69] The government's Architecture Review Board was initiated in 2010 as the body to, among other things:

- review and approve technology-oriented standards,
- monitor compliance to technology and information standards within the province,
- review and approve architectures of critical projects and initiatives, and
- provide architecture guidance and governance at the ideation stage of potential projects.

[70] Despite its broad mandate, the ARB's operating practices only clearly trigger ARB review for specific types of technology projects, enterprise level architecture (i.e. the Amanda platform, not applications running on the platform) and changes to computer desktops. As a result, the ARB reviewed only limited aspects of the AccessPro and FOIA website projects.

[71] The ARB did not review the entire AcessPro project or FOIA website project. Instead it was tasked with reviewing two discrete issues.[36] Detailed architecture diagrams, software coding details and other features of the products were not available to the ARB for review. ARB Decision 94, which approved the trusted sender email status for Unisys, documents the decision and provides the status of the project as:

- Meets approved technology & information standards – unknown at this time
- Privacy impact assessment – yes, in development
- Website vulnerability scan – no[37]

[36] The ARB reviewed the configuration of the old case management desktop application to ensure it would not conflict with the new AccessPro being deployed because the two had to coexist on desktops for a transition period (ARB Decision 33). The ARB reviewed the approval for a Unisys mail server to be set up as a trusted sender within the NSGOV mail system so that automated email messages sent from the FOIA website could be processed and sent from the NSGOV mail system. (ARB Decision 94).

[37] ARB-94.

[72] The IAP Services unit has provided a privacy representative as a member of the ARB since 2015. The privacy representative sat on the ARB committee at the time that AccessPro and the FOIA website were discussed and thus was in position to know the limited extent of the technical review applied to the projects and the questions raised by the Cyber Security representative on the ARB. IAP Services authored the privacy impact assessments for AccessPro and the FOIA website. Therefore, IAP Services had all of the information necessary to recognize the serious lack of security testing.

[73] Internal email communications demonstrate that the Department considered the need for a STRA for the Amanda 7 platform as early as July 2016. There were multiple projects at the time moving to the Amanda 7 platform and email exchanges between Department Risk Management staff, Enterprise Architecture staff, Business Solutions staff, and Unisys project management staff considered whether one STRA could be done for all projects going to Amanda 7. On October 6, 2016, the enterprise architect provided an opinion to the project manager that another project was the driving project for the Amanda 7 portal "and they will most likely be doing a STRA for the portal technology." The project manager interpreted this to mean that the FOIA website was exempted from doing a STRA and forwarded this to the project sponsor.

[74] However, on October 14, 2016, a Business Solutions manager identified to a group of internal recipients, "We had been assuming only one TRA is required to cover off all Amanda 7 projects. However, that assumption may be incorrect. Perhaps we need three TRAs, as follows: 1. The public facing applications planned for the cloud: FOIPOP Disclosure Log/Requestor Portal and AMANDA portal for SNAP (I understand that a TRA was not done for FOIA). 2. The government facing applications planned for the cloud… 3. The government facing applications planned for on-premise.…" The executive director of Cyber Security and Risk Management immediately replied that "we can move forward with a single professional services resource, funded via the project(s) to perform a TRA covering off all aspects described.…"

[75] On December 7, 2016, the project manager for the FOIA website project sent an email to the executive director of Cyber Security and Risk Management and stated that the project was currently in user testing phase, planned to go live beginning January 2017. The email states, "…TRA was NOT done for the previous FOIA system that has been in use by the IAP team since April 2016…Do we need a TRA – for FOIA system and/or my project." On December 12, 2016, the response provided was, "Given the significant changes that occurred, I would recommend that a TRA be performed.…" The project manager followed up on the status of the procurement of professional services to perform the STRA on December 16, 2016. On January 3, 2017, a business relationship director followed up again on the status of procurement of professional services and documented that "It has been identified to the IAP team by the privacy commissioner that a TRA must be completed as soon as possible of the FOIPOP disclosure log."

[76] The firm KPMG was not contracted to conduct a security threat and risk assessment until November 2017. KPMG was contracted to conduct a STRA for the Amanda 7 platform which looked at the risks of migrating all provincial applications running on older versions of the Amanda platform to the new Amanda 7 platform. The report includes some mention of the FOIA website but is not specific to the AccessPro and FOIA website applications. The draft

report from KPMG was received by the Department on March 21, 2018 and was well past being able to assist the risk assessment for either AccessPro or the FOIA website projects.

[77] Had it been done before the projects deployed, the KPMG report could have assisted the Department to identify salient risks and mitigation strategies in this circumstance. Identified risks included the absence of security-related testing such as vulnerability assessment or penetration testing specific to AccessPro and the FOIA website applications.[38]

[78] Department witnesses acknowledged that vulnerability and penetration testing on applications separately from platforms and the government network environment has not been methodical or consistently required by the Department.

[79] There was sufficient internal discussion of the STRA prior to deployment of the FOIA website for the Department to have insisted on its completion earlier. Additionally, the Department itself flagged the lack of website vulnerability scanning during the Architecture Review Board's limited review and decision regarding the FOIA website.

[80] In summary, the evidence establishes that the following shortcomings in the security review process contributed to the implementation of the FOIA website with the storage database design vulnerability:

- The ARB's operating practices were too narrow and so the ARB only reviewed limited aspects of the AccessPro and FOIA website projects.
- The Department failed to consistently require vulnerability assessments and penetration testing on applications as separate from platforms.
- The Department failed to act on information from the ARB that there were risks associated with the lack of website vulnerability scanning.
- Initially, there was internal confusion over when a security threat and risk assessment should be completed and the Department failed to complete a timely and specific security threat and risk assessment after the clear recommendation to do so from Department Cyber Security staff and the Information and Privacy Commissioner.

iii. The privacy impact assessment process

[81] Privacy impact assessments are a common administrative safeguard utilized to identify risks to privacy of a given project or program. Modern privacy laws make the completion of PIAs in advance of implementing a new project or system mandatory. Even in jurisdictions without a mandatory statutory requirement, PIAs are often mandated by government policy and are always recommended by privacy commissioners.[39]

---

[38] Amanda 7 Threat and Risk Assessment Draft Report, KPMG, March 21, 2018, p. 26.

[39] For example: British Columbia: Accountable Privacy Management in BC's Public Sector, 2013 https://www.oipc.bc.ca/guidance-documents/1545 p. 12; Ontario: Privacy Risk Management: Building Privacy Protection into a Risk Management Framework to ensure that privacy risks are managed, by default, 2010 https://www.ipc.on.ca/wp-content/uploads/2010/04/Privacy-Risk-Management-Building-privacy-protection-into-a-Risk-Management-Framework-to-ensure-that-privacy-risks-are-managed.pdf; Newfoundland: Privacy Impact Assessments Expectations, 2015 https://www.oipc.nl.ca/pdfs/PIAExpectations.pdf.

[82] Best practice is to consider the PIA process as an evergreen process. This means that PIAs are completed in stages beginning with the conceptual stage of a new or changed program or system. This conceptual PIA is a red flag exercise that identifies potential issues very early in a proposed project or system. If the project proceeds, then the PIA is expanded to the design stage and the privacy risks are evaluated and mitigation strategies identified. Before implementation, the PIA must be reviewed to ensure that risks identified have indeed been mitigated and to identify any new risks that may have emerged. PIAs should also include a review schedule that requires privacy leads to revisit the project periodically to ensure that any new or emerging risks are properly identified and mitigated.

[83] The government's Privacy Policy, effective April 3, 2008, was applicable at the time of these projects. It defines a PIA as a "due diligence process that identifies and addresses potential privacy risks that may occur in the course of the operations of a government entity." This policy requires each government entity to complete a privacy impact assessment "for any new program or service, that involves the personal information." It also requires the privacy impact assessment to "contain a risk mitigation strategy, the implementation of which shall be monitored by the government entity."

[84] In addition to the Privacy Policy in effect at the time, government also had an Information Management Policy in place, effective October 1, 2008. Under this policy, information management is "a common thread that links disciplines such as information technology, records management, and the administration of access to information and privacy standards."[40] This policy directs departments to analyze information management requirements "at an early stage in the development of new or modified government projects" and requires that "specific risks, vulnerabilities, and other significant information management issues will be identified, documented, reported on, and mitigated as required."

[85] Both of these policies are clear and specific administrative safeguards. The privacy impact assessment process is a tool well placed to respond to the requirements of both policies.

[86] Our investigation identified three significant problems with the PIA process in this case:

(a) Failure to adequately identify risks, including lack of technical security risk identification.
(b) Failure to incorporate and mitigate risks identified elsewhere.
(c) Failure to take action on mitigation strategies identified in the PIAs.

(a) Failure to adequately identify risks

[87] A core element of any PIA is an evaluation of the security risks and protections for personal information. When the project involves a new or revised technology system, one common strategy for identifying technical risks is a security threat and risk assessment.[41]

[40] 4.10 Information Management Policy (October 1, 2008) p.1.

[41] See for example the OIPC privacy impact assessment template published in 2015 at p. 3 that recommends completing a security threat and risk assessment when the new initiative involves a new system. Newfoundland's Privacy Commissioner also has guidance published in 2015 recommending pre-TRA, TRA, and vulnerability assessments: https://www.atipp.gov.nl.ca/info/pdf/Privacy_Impact_Assessment_Guide_June_2016.pdf.

[88] The Security Safeguards section of the PIAs for both the AccessPro and FOIA website projects use the language of the contract that engaged Unisys on these projects. IAP Services staff confirmed that the Technical Safeguards section of the PIAs were copied and pasted from these Unisys documents and no independent assessment or analysis of technical safeguards was done. Perhaps as a function of the copy/paste approach to filling in the Technical Security section of the PIAs, the description of technical security and technical risks identified focus on the Unisys aspect of the projects and the cloud hosting. Neither of the two PIAs distinguishes risk in relation to Unisys (configuration, hosting, and technical services) as distinct from risk in relation to CSDC (the product itself).

[89] There are no risks identified with the product's architecture or foundation in the PIA documents, despite clear risk flags in other aspects of the processes, such as no vulnerability assessment flagged by the ARB, the mounting concerns among the user testing group as to the quality of the product and it being apparent to users that documents were stored together with status markers as simply display filters.

[90] Following discovery of the unauthorized download activity on the FOIA website, CSDC and Unisys retained an independent firm on April 7, 2018 to conduct a full security assessment and testing of AccessPro and the FOIA website. The first set of results from the full security assessment and testing were delivered April 12, 2018 and found 16 security risks with AccessPro and 12 security risks with the FOIA website, of which 25% are categorized as high or critical risk.[42] The tests were performed again following mitigations. The second set of results were delivered May 28, 2018 and June 5, 2018 respectively and found two risks remained with each application (four risks in total), all categorized as medium risk.

[91] Of the high and critical level risks identified in the April 12, 2018 reports, several are also well-known vulnerabilities.[43] The higher-level risks identified in relation to both applications found that the applications were vulnerable to:

- the upload of malicious files,
- cross site scripting attacks,
- external entity processing attacks,
- user interface redress attacks and ClickJacking attacks,
- cross site request forgery attacks,
- authorization flaws that allow a user to retrieve attachments for other users, and
- directory traversal.

[92] The results of these vulnerability scans are significant for two reasons. First, these scans were completed in a matter of days, demonstrating that the time needed to properly identify security risks was not extraordinary. Second, the majority of the vulnerabilities in addition to the one found to be the immediate cause of these privacy breaches were successfully mitigated by the time of the second vulnerability scan.

[42] stratum//security Report of Findings Regarding the Application Security Assessment of the backofficestag.acol.ca Web Application; stratum//security Report of Findings Regarding the Application Security Assessment of the portalstag.acol.ca Web Application.
[43] See OWASP Top 10 Project 2013, footnote #8.

[93] In summary, the Risk Mitigation sections of the PIAs for both AccessPro and the FOIA website fail to identify the risks to personal information from the improperly designed and tested architecture. As a result of the failure to identify the technical risks, a security threat and risk assessment, vulnerability assessment, or penetration testing were not included in the PIA documents anywhere. Vulnerability and penetration testing would have been an appropriate way to determine the specific technical risks at play and could have led to appropriate mitigation strategies.

(b) Failure to incorporate and mitigate risks identified elsewhere

[94] The Department's Cyber Security staff and I both recommended that a STRA specific to the FOIA website be completed. This recommendation was not incorporated into the PIA documentation. Instead, the FOIA website was evaluated in a STRA with a broader focus that was completed more than a year after the FOIA website was launched.

(c) Failure to take action on mitigation strategies identified in the PIAs

[95] Another core element of any PIA is to follow through with implementing or acting on mitigation strategies set out. Both PIAs identified a Unisys failure to fulfill its commitments to handle personal information as anticipated as a potential risk. The mitigation strategy identified in both PIAs was to "implement a monitoring plan for IAP services to monitor compliance." Department staff confirmed that no monitoring plan was implemented.

[96] Failing to follow through on mitigation strategies in a timely way or failing to follow through at all renders the risk assessment process of the PIA ineffective and meaningless. For a PIA process to be an effective safeguard it requires leadership and a due diligence approach. A PIA process is intended to go beyond filling in blanks on a template without follow up, beyond passive acceptance of untested conclusions or unverified claims and beyond blind trust in vendor claims. It requires critical analysis, verification and a willingness to delay or abort projects where risks cannot be fully defined or adequately mitigated in time to provide effective protection.

[97] IAP Services recently hired two new employees with a stronger technical background to assist with the PIA drafting process. A strengthened knowledge base within the IAP Services group is a step in the right direction.

[98] In summary, the evidence establishes that the following shortcomings in the privacy impact assessment process contributed to the implementation of the FOIA website with the storage database design vulnerability:

- The privacy impact assessment process was neither diligent nor rigorous.
- The Department relied on one vendor for technical security measures included in the PIA instead of conducting its own analysis.
- The Department failed to incorporate risks and mitigations identified during the project into the PIA.
- The Department failed to implement security mitigation strategies identified in the PIA.
- The Department failed to recognize security risks despite indicators of risk during the design and implementation phases of the projects.

4.2.3 *Conclusion*

[99] Earlier I listed factors relevant to evaluating whether or not a public body has met the reasonable security standard in s. 24(3) of *FOIPOP*. In this case, four factors stand out:

1. **Sensitivity of the data**: The information held on the FOIA website included highly sensitive personal information. Department staff certainly knew this as they were intimately familiar with the records that would be placed on the FOIA website. This meant that a high level of rigor was required to ensure that the highly sensitive data was secure.
2. **Foreseeability:** The evidence established that the type of database employed in this case is common for web-enabled databases storing public information. In addition, it is common knowledge that manipulating document identification numbers may allow users to access other data in the database. The evidence also established several points during the project management, security assessment and privacy impact assessment processes where privacy and project leaders were aware of the lack of technical assessment and security testing that could have pinpointed the vulnerability. The risk, therefore, was foreseeable.
3. **Trust:** In this circumstance, the data was held and managed by a government department. But not just any government department, the department tasked with leading the government's privacy program. Department staff responsible for these projects include the government's chief privacy officer and staff within the IAP group. These individuals are relied upon by other government departments to guide implementation of new projects, programs and systems in a privacy compliant manner. The level of trust placed in IAP and in the Department itself by citizens and other government departments also informed what would be considered as reasonable security in these circumstances.
4. **Format:** The format of the personal information in this case was electronic and was intentionally being made available via the internet. Records in an electronic format and using the internet for authorized disclosures requires that the technology be vetted for cyber security. Choosing to make personal information vulnerable by formatting it electronically on a website places a higher burden on the public body to ensure that it is secure. The design of the FOIA website was such that all records were stored in a common area. The only thing distinguishing public from private records were document status filters. Reasonable security in this circumstance would mean that officials employ diligent testing and cyber risk assessments to identify and mitigate risks associated with the technology design choices.

[100] Ultimately, this series of privacy breaches was caused by a serious failure of due diligence in the selection and deployment of a new technology tool by the Department. The need for independent and knowledgeable technical assessment and security testing of a tool being considered for deployment cannot be overstated in the age where applications, software and web-enabled technology tools of all size and description are being developed by vendors and marketed to public bodies regularly. Taking the time to diligently assess a tool at all stages of a project, before deployment, is not only necessary to meet the requirements of Nova Scotia's existing policies, it is also statutorily required by our privacy laws.

Finding #2: The Department failed to make reasonable security arrangements for the FOIA website in accordance with s. 24(3) of *FOIPOP*.

[101] Shortcomings in the project management process, the security review process and the privacy impact assessment process all contributed to the deployment of a technology tool containing a well-known and foreseeable vulnerability. The Department failed to make reasonable security arrangements when it decided to place Nova Scotians' personal information in this tool accessible to anyone on the internet. This is the root cause of these breaches.

Recommendation #1: Strengthen privacy leadership and due diligence in the privacy impact assessment process.

(a) Provide up-to-date, rigorous privacy and risk assessment training for all privacy staff and management within the IAP Services unit within six months.
(b) Create a detailed PIA standard operating procedure within six months that specifies the following:
    i. A mandatory requirement that PIAs be completed on all new or significantly modified programs, processes, systems or activities involving personal information.
    ii. A mandatory requirement that PIAs be completed at the conceptual, design and implementation stages for all technology projects involving personal information.
    iii. A requirement for specific assessment and approval from cyber security and technology subject matter experts that is independent of vendor-provided information for all projects involving personal information.
    iv. A recommended consultation with the Office of the Information and Privacy Commissioner for all projects involving sensitive personal information, data linking and/or common or integrated programs or activities. Consultations should begin no later than the beginning of the design phase of a project and should include a follow up consultation during the implementation phase.
    v. A prescribed process for confirming that mitigation strategies are completed.
    vi. A requirement that mitigation strategies and responsibility for follow up be assigned to identified positions.

4.3 Did the Department take reasonable steps in response to the privacy breaches as required by s. 24(3) of *FOIPOP*?

[102] When we evaluate the reasonableness of a public body's actions following the identification of a privacy breach, we consider whether the public body followed best practices in managing the breach. These best practices are known as the "four key steps" which include:[44]

1. Conduct an investigation and contain the breach
2. Evaluate the risks
3. Notification
4. Prevention

Step 1 – Investigate and Contain

Investigation

[103] The Department's initial investigation following receipt of concerns about the FOIA website very quickly identified that there was a serious problem. IAP staff were able to replicate the technique of displaying documents from a manually inputted URL. Although they did not know the extent of the vulnerability, nor whether or not any privacy had been breached through unauthorized access, they recognized the seriousness of the vulnerability and immediately took the site off-line. This action halted any further potential privacy breaches from the website's vulnerability.

[104] In the two days immediately following disabling the website, the Department and its vendor partners were focused on creating a 'workaround' to the vulnerability. Fortunately, prior to relaunching the website, Unisys discovered the first pattern of unauthorized downloads and so the decision was made to conduct further investigation before relaunching the system. That lead to the hiring of the independent security firm whose investigation revealed a further 28 security risks with the two systems, 25% of which were categorized as high or critical risk. This clearly illustrates how essential it is that privacy breach investigations are thorough and methodical. Public bodies must resist the urge to 'fix' problems before a thorough investigation has been completed and all outstanding privacy risks have been properly mitigated.

[105] The Department's Cyber Security staff, in collaboration with Unisys, analyzed Unisys' server logs to identify the 12 IP addresses showing suspicious patterns of access. These efforts were effective in discovering the scope of the privacy breaches based on the information available. But, as noted earlier, it is possible that there were individual unauthorized accesses that were not captured using the suspicious patterns analysis.

---

[44] This practice is articulated by the OIPC in our guidance document "Key Steps to Responding to Privacy Breaches" available on our website at https://oipc.novascotia.ca. It follows the same approach other jurisdictions use. See, for instance: the Office of the Privacy Commissioner of Canada, "Key Steps for Organizations in Responding to Privacy Breaches": https://www.priv.gc.ca/media/2086/gl_070801_02_e.pdf; the Office of the Information and Privacy Commissioner for British Columbia, "Privacy Breaches: Tools and Resources": https://www.oipc.bc.ca/guidance-documents/1428; the Office of the Information and Privacy Commissioner of Alberta, "Key Steps in Responding to Privacy Breaches" https://www.oipc.ab.ca/media/652724/breach_key_steps_responding_to_breaches_jul2012.pdf; and the Office of the Information and Privacy Commissioner of Ontario, "Privacy Breach Protocol: Guidelines for Government Organizations": https://www.ipc.on.ca/wp-content/uploads/Resources/Privacy-Breach-e.pdf.

[106] Our investigation confirmed that the Unisys server logs were maintained for a one-year period (April 2017 to April 2018) in accordance with Unisys' records management practices. The earliest entry on the logs provided by Unisys and reviewed by the Department is April 17, 2017. Therefore, no information about activity on the site is available between January 6, 2017 and April 16, 2017 and so could not have been reviewed for unauthorized access or suspicious activity.

[107] A thorough privacy breach investigation should provide information relevant to containment as well as prevention strategies. An investigation should be focused on identifying what happened and on the root causes for why it happened. The Province's privacy breach management protocol incorporates this best practice under a section titled "Investigation and Mitigation to Prevent Further Breaches."[45] Although the Department investigated to inform its containment strategies, we established through our investigation that the Department stopped short of fully investigating the AST connection and investigating internally how it came to deploy this technology solution containing significant technical vulnerabilities.

Containment

[108] The security issue was initially reported to the Department on April 5, 2018. As noted earlier, the website was disabled at 8:26 a.m. on April 5, 2018. On April 7, 2018, as a result of Unisys' review of server activity logs, the first breach was discovered. In response, the Department began a full security assessment and testing of the site.

[109] A conference call the morning of Saturday, April 7, 2018, included briefing the deputy minister on the matter. Unisys provided the Department an email summary of the discussion which we reviewed in our investigation. The discussion summary is clear that on that date, the Department understood that the immediate cause was a vulnerability inherent in the design of the technology. The Department asked Unisys whether the vulnerability affected other programs on the Amanda platform or the payment interface on the FOIA website. The answer to both questions was confirmed to be no.

[110] The Department's first responsibility in privacy breach management is containment and mitigation of the risks associated with the breach. In this case, the individual behind breach #1 and that individual's purpose and motive in downloading all the available documents from the FOIA website was unknown. The nature of the download of a high volume of documents over the span of a few hours suggested the unknown actor had used a computer program to effectuate the systematic download of all documents. The Department felt a sense of urgency to identify the actor and recover the downloaded material. The options for recovering breached material are to seek a voluntary return of the records from the individual, to force the return of the material through civil law mechanisms or to engage police in a criminal investigation process. In this case, based on the apparent deliberate and comprehensive actions by the unknown actor and based on the sensitivity of some of the information involved, the Department decided to engage the police as the option most likely to result in quick containment.

[45] Managing a Privacy Breach: Protocol and Forms, July 2017.

[111] The Department initiated a complaint with the HRP at approximately 8:00 p.m. April 7, 2018. The initial report to the HRP was that an unknown person had gone into the portal, and using a computer program, downloaded every document there. The incident was reported to police as a cyber breach. This formed the basis for the HRP's criminal investigation. Under its investigation, the HRP quickly obtained a production order to force the internet service provider to produce the identity of the IP address owner and the associated physical address. The HRP then quickly obtained a search warrant, and following a search of the property, seized the equipment which stored the data downloaded from the FOIA website.

[112] The Department decided to hold off on notifying the public of breach #1 to allow time for the HRP to investigate. The Department identified the concern that if the breach and investigation were immediately announced to the public, the responsible individual may be unpredictable and may either destroy evidence of a possible crime, make copies of downloaded material or publish sensitive information to the internet.

[113] Department officials initially advised my office of the breach on April 9, 2018 and then visited my office to provide further details on April 10, 2018. At that time, IAP officials indicated that police were recommending a delay in notification in hopes of avoiding tipping off the responsible individual and therefore putting the personal information at risk. On that basis, and consistent with the OIPC's published guidance on breach notifications, I agreed that a delay of a day or two in order to not interfere with the HRP investigation was reasonable.

[114] Our subsequent investigation confirmed that although the HRP acknowledged those concerns, the HRP did not recommend that the Department delay notification to the public. The Department made its decision out of concern for the possible impact on containment. The first public notification was made via news release on April 11, 2018, six days after the initial discovery.

[115] The best practices of privacy breach management are well documented and do contemplate that in cases where law enforcement authorities are engaged as part of the containment strategy that notification to affected individuals may be delayed in order not to impede a criminal investigation.[46] In this circumstance, with the number of unknowns about the individual responsible for the deliberate download of every document available, I am satisfied it was reasonable for the Department to engage police in an attempt to quickly recover the breached information and it was reasonable to delay public notification of the breach by a few days to allow the containment strategy to proceed unimpeded. The evidence reveals that the Department acted in good faith and that staff were motivated by a desire to contain the privacy breach #1. This containment strategy did effectively result in securing the downloaded material in police custody before it was used, disclosed or copied.

[116] However, the HRP investigation could only go so far. The HRP confirmed that once its investigators clearly understood that the breach was possible because of the construction and functioning of the website and that there were no clear user terms and conditions or privacy statement on the website to caution individuals on the limits to authorized access, the elements of

[46] Key Steps to Responding to Privacy Breaches, https://oipc.novascotia.ca/sites/default/files/publications/Key%20Steps%20-%20Full%20-%20Final%20-%202015Oct27_0_0.pdf, p.9.

possible criminal offenses could not be established. As a result, no charges were laid against the individual associated with breach #1.[47]

[117] In May 2018, police public statements indicated that eventually the seized equipment will be returned to the individual.[48] More recently, the HRP has indicated to the Department that the final disposition of the seized equipment and, more importantly, the downloaded personal information, has not yet been decided.

[118] Following the decision not to lay charges in relation to breach #1, the HRP no longer had sufficient grounds to obtain production orders or search warrants in relation to the 11 additional IP addresses eventually identified as also having breached private information accessed via the website.

[119] Without an ongoing HRP investigation, the Department undertook limited alternative containment strategies. Facts confirmed in our investigation relevant to the analysis of containment are:

- Nine of the remaining 11 IP addresses were associated with the Atlantic School of Theology which receives its IT services through Saint Mary's University (SMU).
- The Department initiated communications with SMU to attempt to voluntarily recover the downloaded materials and learn more about the nine associated IP addresses.
- SMU confirmed to the Department that the physical location of all nine IP addresses was a public computer lab at its Atlantic School of Theology (AST).
- The Department, through civil action, determined that the two IP addresses associated with the Bell Aliant network were also assigned to the Atlantic School of Theology through SMU.
- Our investigation determined that the IP addresses used at the AST were used to grant access to visitor wifi and so any information downloaded from the FOIA website was downloaded to a personal computer, not to SMU or AST's servers.
- SMU and AST confirmed that when a visitor accesses guest wifi, the system records the device identifier - a unique number assigned to machines. The device identifier for all 11 downloads at issue here was the same.
- Internet traffic accessing documents stored in the database behind AccessPro and the FOIA website prior to the earliest logged activity on April 17, 2017, is not known because logs prior to that date were not kept by Unisys.
- Unisys confirmed to the Department on April 7, 2018 that the IP address involved in breach #1 was associated with a valid transaction on a different government website hosted by Unisys and that details were available.
- On April 9, 2018, we suggested the Department may be able to identify the individual connected to the IP address from its own transaction logs or the Unisys server logs if the individual had opened a portal account or done other transactions.

[47] IAP officials confirmed that while there was a privacy statement on the website, there was no requirement for users to first confirm that they had read and understood the privacy warnings before being granted access to the site.
[48] https://www.cbc.ca/news/canada/nova-scotia/police-drop-charges-in-nova-scotia-government-breach-1.4651543

[120] The Department raised concerns about the use and sharing of personal information across government departments for the purpose of identifying individuals suspected of committing privacy breaches.

[121] The Department reported receiving an anonymous letter in August 2018. The letter indicates that the individual suspects that he or she is "solely responsible for all outstanding contacts to your system." The letter indicates that the access was through AST and "very likely through the Bell IPs." Department officials now hypothesize that the same individual is responsible for all 12 of the breaches. On that basis, I made the interim recommendation to the Department that it obtain the device identifier number from the AST and ask the HRP to advise whether the device identifier number associated with the 11 accesses at AST matches the device currently in the custody of the HRP. If it does, then all 12 breaches are, for now, contained.

[122] While I would be very relieved to learn that the device holding the sensitive personal information of Nova Scotians from all 12 breaches is in HRP's custody, I do not believe that the accesses that occurred at AST were by the same individual for a number reasons:

- Some of the AST accesses are on the exact same days as breach #1 was occurring. Why would an individual use an automated program to download all material and then go to another location and pick individual files to download from the same set of documents on the same day?
- The pattern of information sought in breaches #2 - #12 show a different search strategy than the one used in breach #1.
- There is no indication that the individual who used AST wifi had the same technical skill as the individual involved in breach #1.
- The accesses at AST start on February 27 and continue through April 3. It does not make logical sense that an individual who had downloaded all documents available on the website between March 1 and 3 would use guest wifi 10 times after he had the complete data set to then go to AST to look up records he already had on his own computer.
- The anonymous letter describes a search strategy that only matches the AST-related downloads.
- The author of the anonymous letter says he destroyed all of the data. The HRP has a device in custody containing all of the data from breach #1. So, if the author is telling the truth, the destroyed data is not the data from breach #1.

Finding #3: **Containment action reasonable but not complete.**

[123] With respect to containment I find:

(a) The Department took quick initial action to stop any further breaches by disabling the FOIA website.
(b) Breach #1 remains partially contained because there is no final confirmed plan for retrieving and/or destroying of the data downloaded onto the equipment seized by the HRP.
(c) Breaches #2 - #12 remain uncontained. More than 600 documents containing personal information were downloaded onto a personal computer and have not been recovered.

Recommendation #2: Contain the breaches.

Immediately take further steps to contain these breaches as follows:

(a) Breach #1: Continue to communicate with HRP and obtain final confirmation that the documents downloaded have either been destroyed or that the equipment has been permanently seized and secured by HRP.
(b) Breaches #2 - #12: Work with AST to identify strategies that would allow the Department to communicate with the user associated with breaches #2 - #12 should that individual log back onto the AST/SMU wifi system. Use the communication to seek voluntary compliance with the Department's need to secure the return or destruction of the lost data.[49]
(c) Search the internet to determine if any of the documents have been shared or posted in other locations. If so, investigate the posting and work to scrub/delete. Repeat the search strategy periodically for the next 12 months.

Step 2 – Evaluate the Risks

[124] As soon as the Department became aware of breach #1, employees began the task of reviewing and categorizing the types of information that were downloaded from the FOIA website according to its sensitivity. The evidence established that IAP staff recognized that more sensitive information carries higher risks. At one end, some records contained no personal information. This was mainly records intended to be disclosed to the public. At the most sensitive end of the spectrum is extremely sensitive personal information such as medical information, allegations of child abuse and intimate family details frequently contained in Department of Community Services files and Department of Justice files. Social Insurance Numbers are also highly sensitive because of their usefulness in creating false identities.

[125] The Department recognized the spectrum of risk in how it categorized the breached information and affected individuals. For example, individuals whose date of birth and/or identification such as Social Insurance Number were breached were offered credit monitoring services for one year paid for by the Department. All of the affected individuals were notified by letter mail and the Department established a dedicated phone line and email address to make it easy for individuals to call and receive additional information.

<u>Cause and extent of the breaches</u>
[126] The cause of the breaches was in the basic structure of the storage database behind the website that allowed unfettered access to documents not intended to be disclosed publicly coupled with a dozen known instances where this vulnerability was exploited using known techniques for searching databases connected to the internet.

[49] The Department need not comply with recommendation 2(b) if HRP is able to confirm that the device identifier of the machine used at AST is the same as the device currently in HRP custody.

[127] This series of breaches was extensive, involving a high volume of unauthorized accesses to and downloads of records affecting hundreds of Nova Scotians. The fact that 11 of 12 breaches remain totally uncontained is a serious ongoing concern.

[128] The following table prepared based on the server log data obtained by the Department from Unisys demonstrates the scope of the breach of personal information. Here, total attempted downloads show the number of times a user attempted to retrieve a document using the common URL and document number pattern. The difference between attempted downloads and total documents downloaded reflects where there was no document in the storage database associated with the requested document number. The difference between total documents downloaded and total documents containing personal information reflects the number of documents downloaded that were intended for public disclosure and therefore did not contain personal information.

Privacy Breach	**Dates of Activity**	**Total attempted downloads**	**Total documents downloaded**	**Total documents containing personal information**
#1	March 1-4, 2018	40,736	7675	6920
#2	February 27, 2018	14	14	7
#3	February 27-28, 2018	327	286	213
#4	March 1, 2018	49	46	34
#5	March 2-5, 2018	48	46	32
#6	March 8, 2018	80	73	63
#7	March 9, 2018	42	34	25
#8	March 12, 2018	21	18	15
#9	March 13, 2018	24	21	15
#10	March 19, 2018	100	91	77
#11	March 27, 2018	67	63	51
#12	April 3, 2018	122	113	86
Total		**41,630**	**8480**	**6920**[50]

Individuals affected by the breaches

[129] Identifying individuals affected by these breaches was time-consuming and tricky. It involved identifying personal information contained in thousands of documents. Employees were required to cross-reference document RSN identifiers on a server log of downloads against lists of documents stored on the site. In addition, disclosure packages containing personal information buried deep in the substance of the disclosure required the entire package to be read in detail.

[130] Some individuals were affected by multiple breaches if documents containing their personal information were downloaded multiple times or by more than one user. Documents that were uploaded to the server after the last date of unauthorized access were not breached and therefore any individuals whose personal information was only among those documents were not affected.

[50] Note that the total number of documents containing personal information is 6920 as all of the documents accessed in breaches #2 - #12 involved records also downloaded in breach #1. The total number of documents containing personal information downloaded during breaches #2 through #12 was 618.

Foreseeable harm from the breaches

[131] The possible harm from these breaches is across a spectrum, from the low risk scenario of a name, limited contact information and the nature of his or her access to information request, to extremely high risk for individuals whose substantive personal information of a highly sensitive and intimate nature was breached.

[132] Harm to reputation or embarrassment is foreseeable for many of the affected individuals, but more so for those whose highly sensitive and intimate personal information was breached. The potential to use the information within some of the most sensitive files to find and target vulnerable individuals exists. Individuals whose date of birth and personal identifier were breached would be open to potential for identity theft or fraud if that information was obtained by criminals or sold on the black market for personal information.

[133] Learning that intimate details of one's personal life was available in electronic form on the open internet and was accessed by unknown individuals with an unknown outcome is very unsettling and distress-provoking for those individuals. The tort of "intrusion upon seclusion" recognizes the emotional and other harms from a privacy breach and there is potential litigation exposure for the Department.

[134] More broadly, there is a foreseeable harm to the public trust in government's ability to safeguard sensitive personal information as a result of these breaches. The Department implemented a technology tool that it had not properly assessed and did not follow government information management or privacy policies designed to ensure risk assessments on technology projects involving sensitive personal information would be done. The very unit responsible for advising other departments on privacy did not perform an effective, due diligence-oriented privacy impact assessment.

[135] Overall, the risks from these extensive breaches, involving some of the most sensitive and intimate of personal information held by the government which is yet to be fully contained, are high.

Step 3 – Notification

[136] Proper notification to affected individuals requires accurate identification of those who are affected by the breaches. In the early days of responding to the breaches, the Department decided to notify all access to information applicants whose information was on the FOIA website on the date that it was disabled, deeming them all to be affected individuals even though it could not be precisely determined who was affected and who was not. This meant that some individuals who were not actually affected by the breaches received notification.

[137] Sending a notification to an individual who was not actually affected by a privacy breach causes harm in the form of unnecessary worry and anxiety and provokes a sense of violation. An individual might expend energy taking steps to mitigate the breach or might suffer emotional harm for no reason. The challenge in this case is that there is the possibility that any individual applicant on the website had his or her privacy breached. It is possible that some third party inadvertently or intentionally accessed personal information using a modified URL. These

limited types of breaches could not be identified by the Department. So, in fact, there is some risk to all applicants who used the FOIA website.

[138] Further, our analysis of the Department's catalogue of breached documents and affected individuals identified instances where individuals are identified in the document information but were not included on the list of affected individuals. Department witnesses gave conflicting statements regarding whether substantive records were fully reviewed to determine if all individuals whose personal information contained within the records were identified and by whom. Department documentation of notifications indicates that individuals were not clearly notified of the number of times they were affected by the breaches. Some individuals had multiple documents containing their personal information downloaded or had documents downloaded by multiple users.

[139] Failure to identify all affected individuals means that those unidentified individuals did not receive notification of the privacy breaches and are unaware of the outstanding risks or steps they may take to mitigate potential harm arising from the breaches. Failure to clearly identify the affected individuals if their personal information was breached on multiple occasions does not provide individuals an opportunity to understand the full extent of the risks they face.

[140] The Department confirmed that its notification strategy was to only notify access to information applicants. Individuals whose personal information appeared within the records were not notified for a number of reasons. First, often the identifying information was limited. For example, the record may only have contained a first name. Some of the information was very old and frequently the records did not necessarily include an address of these third parties or the address information is likely out of date. Finally, the Department raised concerns with notifying children.

[141] Both under and over notification of individuals occurred in this instance and both carry distinct risks for individuals. Accuracy is important when identifying who is affected by a privacy breach.

[142] The Department's approach to notification was in phases. The first notification was a general public notification by news release on April 11, 2018, approximately 4.5 days after discovering the first privacy breach. The public notification was an important first step and, in my view, was an effective way of providing good general information in a very timely fashion.

[143] The second phase took place April 12 - 13, 2018, consisting of notification letters to 328 individuals whose breached information was deemed highly sensitive and included an offer of free credit monitoring. The third phase, on April 18, 2018, consisted of notification letters to 412 individuals whose breached information was deemed lower risk.

[144] Individual letters included a description of the breach, nature of the information disclosed, steps taken to contain the breach, contact information for a dedicated email and phone line where affected individuals could have specific questions answered and contact information for the OIPC with a statement of the right to file a privacy complaint.

[145] *FOIPOP* does not contain specific requirements for a public body to notify either the Commissioner or affected individuals. The best practices hold that notification of affected individuals where there is potential for harm or embarrassment should happen at the first reasonable opportunity.

[146] I have canvassed in other review reports what "at the first reasonable opportunity" means.[51] The reasonableness of the timing is measured by whether it is objectively diligent and prudent in all the circumstances. Guidelines and laws tend to be imprecise with regard to time limits on notification to affected individuals because circumstances must be accounted for.

[147] Guidelines around notification in Canada suggest multiple formats for notification to affected individuals, always with the purpose of best facilitating the individual taking steps to mitigate harm. It is not necessary that each individual receive the same form letter notification after the investigation is complete. A public body can take a tailored approach to notification at multiple stages of the investigation if that would best facilitate mitigation of harm. For example, initial notification by phone call to provide the individual preliminary ability to manage the risks, followed by formalized notification later in the process, may provide the individual better opportunity to mitigate the potential damage caused by the breach. Typically, this is taken to mean within days or possibly weeks of identifying a breach, but not months.[52] The reasonableness of the time period can also be impacted by the circumstances. Best practices also acknowledge that if a police investigation is part of the containment strategy, this may weigh in favour of delaying notification to allow maximum opportunity for containment to be effective.[53] A very high volume of records to be analyzed in order to identify affected individuals could also weigh in favour of some delay in order to accurately notify individuals.

[148] In this case, the broad scope and large number of affected individuals, coupled with the public attention to the disabled website, weighed in favour of an initial general, public notification. The Department followed up with tailored individual notification letters with dedicated phone and email contacts to make it easy for affected individuals to ask questions.

[149] Overall, the initial phases of notification, the multiple methods and tailored approach, were effective. The timing of notification, given the active containment strategy involving police and the large volume of records and individuals, was reasonable.

[150] I accept that while there is some risk of over notification because all access to information applicants received notification, I find that this approach was reasonable for the following reasons:

- There is an outstanding risk of unidentified unauthorized accesses; and
- The information was vulnerable for more than one-year time period.

---

[51] IR18-01, August 1, 2018.
[52] The European General Data Protection Regulation (GDPR) requires notification to oversight agencies within 72 hours and "without undue delay" to affected individuals. Numerous American notification laws require notification "immediately" but not later than 45 days.
[53] Key Steps to Responding to a Privacy Breach https://oipc.novascotia.ca/sites/default/files/publications/Key%20Steps%20-%20Full%20-%20Final%20-%202015Oct27_0_0.pdf.

[151] However, the risk of under notification remains an issue. Records accessed through access to information requests can contain significant and sensitive personal information. While there is without question some practical challenges to further notification, reasonable security, in my view, requires further action.

[152] For breach #1, while there are many individuals whose information is contained in the 6920 documents containing personal information downloaded by this individual, the computer is currently in police custody. Therefore, I do not recommend that any further notification occur with respect to this breach. However, with respect to breaches #2 through #12, the records were downloaded to an unknown computer. Those breaches involved access to a total of 618 documents containing personal information.

Finding #4: Notification efforts reasonable and timely but not complete.
[153] Overall, the Department's timing and multiple methods of notification were reasonable. However, problems with under notification must be corrected.

Recommendation #3: Correct under notification to affected individuals within 60 days.[54]

Identify all individuals whose personal information was disclosed within the 618 records accessed in breaches #2 - #12 and take all reasonable steps to notify them using the following guidelines:

(a) For each identified individual, determine whether the available information is sufficient to accurately identify the affected individual. If only a first or partial name is available, determine if there is other information in the file that could assist with identification.
(b) If the individual is identifiable, rate the risks associated with the information disclosed. Included in this risk rating will be an assessment as to whether or not a breach notification itself could result in the unintended breach of other personal information (such as the identity of the access to information applicant). Such a result would mitigate against third party notification.
(c) If the individual is a minor, consider whether the minor is capable of understanding the purpose of the notification and capable of taking action necessary to protect herself against the risks associated with the breach. If not, make a reasonable effort to identify and notify the minor's legal custodian.
(d) If the risk is sufficient that notification is required, search for current address information. The search can include requests to other government departments for current address information as authorized by s. 27(f) and 27(g) of *FOIPOP*. The collection of this information by the Department of Internal Services is authorized under s. 24(c) of *FOIPOP*.

[54] The Department need not comply with recommendation 3 if HRP is able to confirm that the device identifier of the machine used at AST is the same as the device currently in HRP custody.

Step 4 – Prevention

[154] In order to prevent a similar breach in the future, it is essential to understand the root cause and to evaluate all of the factors that contributed to the breaches occurring. In accordance with my findings above, the immediate cause of these breaches was a vulnerability in the design of an internet-enabled technology tool. Shortcomings in the project management process, the security review process and the privacy impact assessment process all contributed to the deployment of a technology tool containing a well-known and foreseeable vulnerability. Underscoring each of these shortcomings is a serious failure of due diligence in the selection and deployment of a new technology tool. When the FOIA website was launched with the design flaw it placed sensitive personal information where it could be accessed by anyone on the internet.

[155] The best practices for post-incident review and developing a prevention strategy following a privacy breach of this scope and sensitivity calls for a comprehensive, reflective review by the public body and concrete actions taken as part of an effective privacy breach management protocol. The Province's privacy breach management protocol includes a post-incident review requirement. It states:

> "Privacy breach investigations should be led by the privacy designate/IAP administrator with the support of the program/business area leadership…The investigation will include a review of the business practices and procedures, access controls in place, security (physical and technical), and interviews with staff involved."[55]

[156] The purpose of this type of post-incident review set out in the Province's privacy breach management protocol is stated:

> "Most likely it will be apparent how the breach occurred early in the response process. However, it is important to revisit the root cause of the breach after it has been resolved to ensure the reasons for the breach are well understood and have been rectified."[56]

[157] In keeping with this policy and with best practices, I expected that the Department and IAP staff would either have organized or were planning to organize and lead a post-incident review process. In a meeting with senior executive members of the Department in December 2018, they confirmed that there was a debrief/lessons learned exercise with staff from all areas on May 17, 2018. Curiously, when we interviewed staff through the spring and summer of 2018, none mentioned any internal review process or any post-incident meetings.

[158] When asked about post-incident review and lessons learned, some themes were repeated by several employees including:

- the Department is committed to continuous improvement,
- more rigor was needed in this case, and
- the environment at the time was challenging because of centralization and restructuring so there was confusion about who was doing what.

[55] Managing a Privacy Breach: Protocol and Forms, July 2017, p. 15.
[56] Managing a Privacy Breach: Protocol and Forms, July 2017, p. 15.

[159] Department employees did not connect these general comments to an internal post-incident review process or specific prevention actions or plans.

[160] A few individuals, including at the senior management level, stated that they have been directed to ensure that vulnerability and penetration testing is conducted at the application level on all new technology projects (but not projects in development or already deployed). The mechanism to require this is not clear. A key employee stated he had been asked to develop a new corporate standard for industry certification/accreditation that will be required for technology projects.

[161] It is troubling that months after the privacy breaches, erroneous understandings about the nature of the breaches, their root cause and how to prevent them from occurring again persisted within the Department. Department witnesses and documents characterized the cause of the breaches as manipulation of the website address.[57] One employee expressed the view during our investigation that the cause of the breaches was individuals using the website in a way that was not intended and maintained the view that the unauthorized downloads were theft. One employee expressed that her lesson learned was she hoped not to have to work with Unisys again. A management level employee expressed that the Department does not have time to conduct a post-incident review.

[162] Of greater concern are comments suggesting that the risks surrounding technology tools and the responsibility to mitigate them are not well understood within the Department or across government. A few employees expressed residual concern during our investigation that the Province of Nova Scotia has demonstrated a culture of high tolerance for cyber security risk. Examples were provided of projects where cyber security recommendations were made but the project continued to move forward despite them. Multiple employees talked generally about their experiences of an angry phone call from a project owner to a 'higher up' person in the Department to intervene if a risk concern was raised that the project owner was not prepared to act on. Employees described project planning occurring in government departments that do not sufficiently budget for the time and money needed to conduct adequate security testing and the friction that may arise as a result. One employee provided an example of a meeting where an individual who raised a concern about technical infrastructure compliance with standards was mocked by a vendor and, of the room full of Department directors, none intervened to support the individual raising the concern. A senior management level employee expressed pride in being an innovator, said that she would do the same again, and expressed that reasonable security is only one line in the *FOIPOP* legislation.

[163] While it appears that key individuals are working on some new safeguards that have potential to assist with preventing this occurring again, broader issues with respect to the understanding of this incident and what led to it, as well as with respect to the overall minimizing of cyber security and privacy risks, remain. An internal post-incident review process could assist with both.

[57] Recorded in the "step by step" breach management documentation, p. 4.

[164] In October 2018, the Department retained a service provider to conduct a post-incident review/lessons learned exercise. That process is ongoing. In addition, the Department will of course have the recommendations from this office and the Auditor General to inform improvements in its processes. Learning from what went wrong in this case should be immediately applied to all technology projects in development or already deployed that have not received adequate technical review, vulnerability assessment or penetration testing. The failure to realize what the risks are or what risk questions needed to be asked is the first order issue in this case. Therefore, any other technology projects deployed that have not received rigorous risk assessment and technical review or testing are prone to the same issue, whether or not they have experienced a privacy breach.

[165] When the full security assessment was eventually procured for AccessPro and the FOIA website, more than two dozen other vulnerabilities were identified that the Department was unaware of. The Department, responsible for technology, security, and privacy for all of government, must go beyond risk management that looks to mitigate discreet single issues once identified. Rather, it must move to accepting that diligence in risk management is all about identifying unknown or unforeseen risks as much as possible by employing methodical risk assessment tools.

[166] The failure to take stock of what other technologies have been deployed or are in queue to be deployed but have not received adequate technical review or testing leaves the distinct possibility that Nova Scotians have reason for ongoing concern about cyber security, technology and the risk to personal information under the care of the provincial government.

Finding #5: Post-incident review and effective prevention plan not yet implemented.
[167] The Department lacks a comprehensive, methodical plan to prevent a similar occurrence in the future. The Department has failed to take steps to identify if other technology projects or applications deployed or in development are at risk from similar lack of technical review, vulnerability and penetration testing.

Recommendation #4: Conduct internal post-incident review.

I recommend that the Department:

(a) Provide all Department employees with a copy of this investigation report and direct all employees who participated in procurement, project management and privacy to read the report.
(b) Complete the post-incident review process begun in October 2018 by February 28, 2019. Engage the IAP Services unit and executive, the Cyber Security unit and executive, the project manager on the FOIA project, the Project Management unit managers and executive, the Business Relations unit, the Architecture Review Board, and the Department executive in a post-incident review in accordance with the Department's Managing a Privacy Breach protocol document.

Recommendation #5: Review other technologies for security vulnerabilities.

I recommend that the Department:

(a) Within one year create an inventory of technology solutions, devices and applications that involve the use of personal information across government and rate the cyber security vulnerability and penetration risk based on modern standards of cyber security risk assessment.
(b) Create a plan to mitigate cyber security vulnerabilities beginning with systems storing the most vulnerable personal information and/or having the highest risk vulnerabilities and then update PIAs as appropriate. By July 2, 2019, provide this office with an update on the status of the plan including proposed timelines.

Additional procedural administrative safeguards

[168] The evidence establishes that the ARB operated as an administrative safeguard, but that shortcomings in its operational scope and standards required prevented it from being an effective safeguard in this case.

[169] As mentioned above, the ARB was initiated in 2010 as the body to, among other things:

- review and approve technology-oriented standards,
- monitor compliance to technology and information standards within the province,
- review and approve architectures of critical projects and initiatives, and
- provide architecture guidance and governance at the ideation stage of potential projects.

[170] The ARB is chaired by the director, Enterprise Architecture (or a designate) and its membership consists of representation from provincial information technology and information management sectors within government. Members have one vote. Members representing privacy, security and records management have "a veto for their specific mandate" of projects under review by the ARB[58] indicating a special importance for review of technology by members representing those interests.

[171] As canvassed above, the ARB's operationalized scope appears to be narrower than the terms of reference mandate would allow or suggest. Department witness statements indicated that the ARB is often viewed as a roadblock and red tape for projects and that the ARB lacks the authority to require projects to comply with requirements. Department witnesses acknowledged that more formalized procedures for approvals and conditional approvals, clear and formalized standards, and diligence checklists would assist the ARB to be more effective.

[172] The ARB gathers together representatives with expertise in technical solutions, information management, privacy and cyber security to review and approve technology initiatives. This body, if deployed to its potential, offers the possibility of an effective due diligence checkpoint and administrative safeguard for all technology deployments across the province.

[58] ARB Terms of Reference, p. 4.

Finding #6: The Architecture Review Board was ineffective as a safeguard.
[173] The Architecture Review Board was rendered ineffective as an administrative safeguard by insufficient authority, too narrow a mandate in practice, and lack of explicit formalized processes and technical security standards.

Recommendation #6: Clarify and strengthen the role of the Architecture Review Board

I recommend that within six months, the Department:

(a) Clarify the Architecture Review Board mandate, policy and triggering process so that all new technology initiatives and significant changes to technology deployments involving personal information are reviewed by the ARB.
(b) Clearly establish and communicate the ARB's authority to approve, deny, amend or delay technology projects to ensure diligent risk assessments and risk mitigations before deployment.
(c) Develop clear operational procedures, technology standards and mandatory project information requirements to ensure the ARB can effectively assess technology projects and carry out its mandate.

5.0 Conclusion

[174] In the spring of 2017, I wrote to government recommending that our privacy laws be modernized. This investigation, along with other recent privacy breach investigations, have made it clear that our privacy laws are woefully lacking. As a result, I have again written to the Premier and to the Ministers responsible for our privacy laws to recommend that the changes I recommended almost two years ago be implemented. My letter focuses in particular on amendments to improve privacy breach management, notification and the powers of my office to conduct investigations.

[175] There is significant work to be done to ensure that the Department places itself in a position where it has a comprehensive, methodical plan to prevent similar occurrences in the future. Privacy impact assessments must involve meaningful critical analysis, verification and a willingness to delay or abort projects where risks cannot be fully defined or adequately mitigated in time to provide effective protection.

[176] In response to this report, the Department has advised me that it accepts all of my recommendations. In the months ahead, we will have ongoing discussions with the Department to address any challenges it identifies with implementing the detailed components and timelines associated with the recommendations. Ultimately, the ongoing role of my office is to oversee compliance with the recommendations.

6.0 Acknowledgements

[177] I would like to thank the many people who cooperated with this investigation from the Department of Internal Services, the public, Halifax Regional Police, the Atlantic School of Theology and Saint Mary's University. The purpose of these investigation reports is to ensure that any lessons to be learned from a privacy breach are shared for the benefit of Nova Scotians and for the education of all.

[178] I would also like to thank Janet Burt-Gerrans, Senior Investigator, who led this investigation and contributed to the drafting of this report. I am grateful to Carmen Stuart, Director of Investigations and Mediation, who assisted with this investigation.

January 15, 2019

Catherine Tully
Information and Privacy Commissioner for Nova Scotia