HANSARD

NOVA SCOTIA HOUSE OF ASSEMBLY

COMMITTEE

ON

PUBLIC ACCOUNTS

Wednesday, January 16, 2019

Legislative Chamber

January 2019 Report of the Auditor General:
Information Access and Privacy Information Technology Projects

Printed and Published by Nova Scotia Hansard Reporting Services

Public Accounts Committee

Mr. Eddie Orrell (Chairman)
Mr. Gordon Wilson (Vice-Chairman)
Mr. Ben Jessome
Ms. Suzanne Lohnes-Croft
Mr. Brendan Maguire
Mr. Hugh MacKay
Mr. Tim Halman
Ms. Lisa Roberts
Ms. Susan Leblanc

In Attendance:

Ms. Kim Langille
Legislative Committee Clerk

Mr. Gordon Hebb
Chief Legislative Counsel

WITNESSES

Office of the Auditor General

Mr. Michael Pickup,
Auditor General

Mr. Andrew Atherton,
Assistant Auditor General

Ms. Janet White,
Audit Principal

House of Assembly
Nova Scotia

HALIFAX, WEDNESDAY, JANUARY 16, 2019

STANDING COMMITTEE ON PUBLIC ACCOUNTS

9:00 A.M.

CHAIRMAN
Mr. Eddie Orrell

VICE-CHAIRMAN
Mr. Gordon Wilson

MR. CHAIRMAN: Order please. I would like to call the meeting of the Public Accounts Committee to order.

Today we have a presentation from the Auditor General on his report. Before we start, I would like to remind everybody in attendance to put your phones on vibrate or silence.

We will start with introduction of committee members, starting with Ms. Leblanc.

[The committee members introduced themselves.]

MR. CHAIRMAN: On today's agenda, we have officials from the Office of the Auditor General with us to discuss the January 2019 Report of the Auditor General. I will let you introduce yourselves.

[The witnesses introduced themselves.]

MR. CHAIRMAN: We'll start with opening remarks before we have questioning. Mr. Pickup.

MR. MICHAEL PICKUP: Good morning, and thank you for the opportunity. To begin, I want to say thanks to the people in my office for this week, and the Department of Internal Services for their professional dealings, and my colleagues at the Office of the Information and Privacy Commissioner whom we worked with together.

Yesterday morning, I tabled my special performance audit report to the Legislature on the 2018 privacy breach of the Freedom of Information Access website that resulted in the inappropriate disclosure of personal information. A few hours later, the Information and Privacy Commissioner and I co-hosted a media conference to communicate our findings and recommendations regarding this matter directly to the people of Nova Scotia via the media. From our work, we determined that the significant and damaging - and still somewhat uncontained - breach was wholly preventable.

It is worth reminding ourselves that this is not an abstract, technical glitch without consequences. This is a serious matter with real human impacts. One example of the trauma that persists for some Nova Scotians includes the mother whose unfortunate and difficult family situation and specific details identifying the child's name and school who were part of this avoidable breach. This is all very disturbing and far too real.

In my report, I have made five recommendations that I believe will help repair some of what is broken at the Department of Internal Services. However, the repairs will only work if the people carry through and make their promised changes as outlined, and that they fully address the matters.

My purpose here this morning is to answer your questions to help you understand my report's findings and recommendations within the mandate outlined in the Auditor General Act. Specifically, I am here to work with you to help equip you in your role as representatives of the people of Nova Scotia as you probe and hold leaders and decision-makers to account at the Department of Internal Services for this utterly preventable disaster.

I believe the people of Nova Scotia now look for signals, actions and assurances both now and in the future that when it comes to information and privacy protection, the right fixes are being made by the right people, and those fixes are sustainable and being monitored.

We will now be more than happy to take your questions this morning.

MR. CHAIRMAN: Thank you. We will now open the floor to questions, beginning with the PC caucus and Mr. Halman.

MR. TIM HALMAN: Mr. Pickup, I want to thank you for your opening remarks, and your statement that the events that have transpired are not without consequences. I want to thank you for that. As we delve into your report, I hope we can all remember that

we are talking about actions that have occurred, events that have transpired that impact Nova Scotians - that impact everyday people who are just trying to go about their business.

It was a very interesting report. I've certainly followed this case very closely over the past year. I think we would all agree that one of the fundamental roles of government is to ensure the safety and security of its citizens and residents. Certainly in the digital age, that applies to securing our data - securing our information.

The Minister of Internal Services has indicated that she takes privacy very seriously. In your report, did your audit find anything that supports that statement?

MR. PICKUP: I think it works best for me when I talk to specifics. Specifically, I can talk about what worked and what didn't work well. Ultimately, without using up too much of your time, we certainly have indicated that risk management did not work well. This project was assessed at low risk when all indicators, without using hindsight, would suggest that this was greater than low risk, and that project management was inadequate. To stick to the specifics of the case, for me, it was those two key areas of shortcomings that resulted in this.

MR. HALMAN: Specifically, did your audit report find anything to support the statement by the minister that the department takes privacy very seriously?

MR. PICKUP: If I look to actions, for example, and I will use this - it will sound like an odd example when I start the answer. I would say that the proof in the pudding - that the assessment of this was low risk after the breach - was demonstrated by the fact that when the department then acted to do a security assessment, they found over 20 other vulnerabilities, up to seven of which were critical.

That might seem like an odd example, but I use it twofold. One, to demonstrate that clearly a risk assessment should have been done; and two, to also show that once they became aware of this, they took that action. That didn't come after the audit. That occurred at the time. It's a twofold example.

MR. HALMAN: Am I correct in saying that if privacy was taken seriously, a proper risk assessment would have been in place? Is that correct?

MR. PICKUP: I believe that the expectation of a risk assessment and good project management is not an unreasonable expectation. The types of things we're talking about, like doing security assessments, are standard operating procedures, the basics. These are not far-fetched ideas. These are not best practices that you might do somewhere in the private sector in another country. These are the standards and the expectations that government should be held accountable for.

MR. HALMAN: Can you tell us, what specifically were the obstacles to a proper risk assessment? If privacy is taken seriously, then I think for Nova Scotians, it's fair to say that steps would have been taken, put in place to ensure proper risk assessment if privacy is taken seriously. What steps should have been in place to ensure proper risk assessment?

MR. PICKUP: I think it goes in tandem with what you said. It's not only ensuring that proper risk assessments, security assessments, vulnerability assessments get done, but it's also taking the time to really assess the risk well from the beginning.

When we look at this and we see Nova Scotia was the first jurisdiction in the world to implement the two of these things together, and we look at the five or six other key things that were happening at the time, all indications were that this was something greater than low risk.

The mistake from the beginning was to call this low risk and place undue reliance on the vendor and not do the appropriate procedures right from the get-go. Everything that happened after that all relates back to some of those initial decisions that, frankly, were in error.

MR. HALMAN: As you're aware, in 2016, the report highlighted a number of concerns that we saw play out in this failure in privacy. In my mind, Mr. Pickup, if an individual in a position of leadership takes an issue seriously, they're going to take steps to ensure, as you say, that there is a proper risk assessment. Did your investigation, audit, indicate or suggest that the department was taking those 2016 recommendations seriously? Was there any evidence of an action plan to remedy this, as was outlined in 2016?

MR. PICKUP: I'm working to try to keep my answers shorter to not use up your time, so if I need to expand, just encourage me to expand upon the answer.

The typical approach for us on following up previous audits, and in this case, 2016 AMANDA that is referred to - we give the government two years to deal with the recommendations and then we come back on every audit, on every recommendation, and do what we call follow-up, which is a look-see to see what did you do with it. Regarding the AMANDA audit from 2016, we will be reporting in March of this year whether those recommendations were implemented.

Last night, I was flipping through some of my own summaries and things to see if the AMANDA audit from 2016 had been called into the Public Accounts Committee at the time and whether there was an action plan or follow-up or things suggested, but when I was flipping through my notes from what I saw, the AMANDA audit had not been called into the Public Accounts Committee. So I don't think an action plan had been filed.

MR. HALMAN: Yesterday, as you're aware, the Privacy Commissioner indicated and spoke of the concern that when privacy issues were brought up at the department, they were laughed at. I find that quite alarming, especially in the context that this has been presented where privacy is being taken seriously. Behaviour such as that, one can conclude that, no, that's not the case. If some key people in the department, if there's a culture where people are kind of scoffing or laughing at that, that is very problematic and troubling.

I'm curious - in your audit, did your investigation uncover similar instances where the notion of privacy concerns were being laughed at?

MR. PICKUP: We did some of the work together with the Privacy Commissioner, so some of the interviews would have happened together. The nature of her work is a little bit different than ours in terms of what her investigation included. In fairness to her and to the committee, I won't go into her report in terms of what she concluded, but I will say we did some of the work together.

Our audit is more focused on the criteria and looking at the criteria, answering the questions, and less about those types of comments. I think I will probably leave it at that.

MR. HALMAN: You have indicated that you conducted some interviews together with the Privacy Commissioner. Am I correct in saying that?

MR. PICKUP: Yes, and if you want - I'm just looking to Ms. White - we can give you more details.

MR. HALMAN: With respect to that, was there collaboration between the Privacy Commissioner and the Office of the Auditor General to construct interview questions together, for example? Was there collaboration on that level - since we have a common person that we're interviewing, perhaps we will meet in advance to construct some questions?

MS. JANET WHITE: The interviews actually took place quite early in our process. We hadn't developed our plan and what we were going to look at. It was really sort of digging up just what was going on and what was out there.

We did collaborate on the technical aspects of the questions because that was what we were bringing to the table. The Auditor General's Office was bringing that technical piece, so we had our IT professional word the technical questions, if you will.

MR. HALMAN: The Privacy Commissioner indicated yesterday that she is very worried that the necessary changes that are required to ensure the safe storage of Nova Scotians' private information won't be made. I can only conclude from that statement that it is because those responsible for this breach are those responsible now to carry out these fundamental changes. Do you have concerns about that? Do you share the same concerns

or level of worry as the Privacy Commissioner with respect to implementing changes within the department?

[9:15 a.m.]

MR. PICKUP: I'm going to answer that directly, but firstly, I would say that any of these audits that we do, I'm absolutely concerned and interested, both as an Auditor General and as a Nova Scotian, that things get done. The whole point of doing these audits is not just to come up with the conclusions and the recommendations. It's to see that change occurs and that things are being implemented, so I'm always concerned that things get done on every one of these audits. Having said that, on this audit, of course, given the nature of it with privacy, I'm very concerned and interested to see that things get done.

I would remind folks that we do these audits, and we report to the Legislature, and this is a tool for all MLAs to hold the government accountable for making these changes. I do hope this is one that the members of the Legislature will continue to monitor to look to the government to ask what's happening. Frankly, we didn't see a lot of that on the AMANDA audit, when we did that audit. Really, there was not a lot of follow-up to see what happened with those recommendations so I hope on this one, it will be different. I say that both as the Auditor General and as a Nova Scotian who is equally concerned about my privacy as well.

MR. HALMAN: Mr. Pickup, I want to thank you for your encouragement with respect to the Opposition asking tough questions. That is a fundamental ingredient in a healthy, dynamic democracy, where Opposition has the opportunity and the proper format to be able to ask tough questions of government. I want to thank you for that encouragement. I know my colleagues in the Official Opposition and in the NDP caucus will certainly appreciate that.

In your report, you speak to the project sponsor, but you do not name that person or indicate their role. The privacy commissioner has indicated that the sponsor was the chief information and access privacy officer. Can you confirm that this is who you understand to be the project sponsor?

MS. WHITE: Yes, that was the project sponsor.

MR. HALMAN: May I ask why in your report you didn't indicate that?

MS. WHITE: Typically, the way that we write our reports, we don't identify specific individuals or positions.

MR. HALMAN: It's interesting. I think fundamentally what Nova Scotians want to know is where the buck stops. Who is accountable? This is arguably the biggest privacy breach in the history of our province. We can ask questions about process, which is critical.

Fundamentally, I think Nova Scotians want to know all the key players. That, to me, is so key in knowing where the buck stops. Definitely, I see an issue with that in the report.

While your report definitely investigates and looks at the causes, I think we also need to keep in mind moving forward that there has to be a level of accountability. Certainly the spirit of your report talks about standard operating procedures. It's just a standard operating procedure that we have service expectations that in contracts individuals know the financial obligations.

Here's my question: Who should be held accountable for this lack of oversight? Fundamentally, that's what this is about - a lack of oversight, someone or some people not doing their job. Who should be held accountable for this lack of oversight?

MR. PICKUP: Just to go back to some extent and to expand upon it, if you wish, to my answer to a previous question, we do these reports in accordance with the Auditor General Act, and we say, okay, here are the findings, and we report to the Legislature. Really to me, this is a tool for the members of the Legislature then to look to government to hold government accountable for past results, what has happened, and then for fixing things going forward and to improve better government.

What those questions mean in terms of accountability and what members of the Legislature do with that report, really is up to members of the Legislature. Similarly with the recommendations we make, it's not up to the Auditor General to implement those recommendations. It really is up to the government to look to implement those and for members of the Legislature to hold the government accountable as they see fit.

In terms of answering who is accountable, under our system of course, it is the minister who leads the department. We deal with the minister. We deal with the deputy minister as the key person running the department day to day, but ultimately, I think our system of government is clear in terms of accountability.

Again, often I know these answers can be long and I'm trying not to totally use up your time, so maybe I'll keep it at that and if you want more, you can encourage me to expand.

MR. HALMAN: You've indicated that it is the minister that is ultimately responsible. We know that the minister has indicated to this House that she takes privacy very seriously. In your interpretation of your report, do the minister's remarks match up with the evidence that is in your report? With everything you've outlined, do you believe privacy was not taken seriously?

MR. PICKUP: I think I'll give a threefold answer to that. One, we cannot excuse the results and explain away the results or take away the results of this audit. Clearly what

should have been done to a reasonable expectation was not done. There's no changing the fact that those things were not done.

The second part of my answer would be - the response to the recommendations. There were favourable responses to the recommendations. There are indicators of actions that are going to be taken. A small concern or advice/hope - whatever the right verb or noun would be - is that a lot of those responses to the recommendations in our report don't have timelines, so I hope members of the Legislature will hold the department to timelines to fix these things so that they don't go on for years.

Third, I think in my dealings - I can speak to my dealings with the department. Certainly I'm troubled by what happened in the findings, there's no changing that. But in terms of my sit-down and discussions with the senior folks running the department, they weren't spending their time arguing with me over whether these things are serious and whether they happened - the focus was on fixing things. Again, those are words until things get done. I'm hopeful, but hope only goes so far. Now we have to see things get fixed.

MR. HALMAN: In your opening remarks, you indicated that this was an inappropriate disclosure of privacy information. The Privacy Commissioner has indicated that she sees this as an illegal disclosure of privacy information. Do you believe what's happened in this breach was illegal, a violation of FOIPOP?

MR. PICKUP: Our audit objectives didn't include looking at the legality, compliance, non-compliance with the privacy Act. That was part of why we did this work in tandem. Those were her areas to look at. In keeping with my earlier comment, I think in fairness to her and in fairness to the committee, I'm not going to speak to her conclusions in her report for the risk of not contexting something correctly.

MR. CHAIRMAN: Thank you. That concludes the time for the PC caucus. We will now move to the NDP caucus and Ms. Roberts.

MS. LISA ROBERTS: Thank you, Mr. Pickup and Ms. White, and for your work on this audit. Just to follow up on your last answer, Mr. Pickup, do you feel that this committee would be better served - and that Nova Scotians would be better served - if, in fact, the Privacy Commissioner would have been able to join us at the Public Accounts Committee today?

MR. PICKUP: I'm here to speak to our report and in fairness to the committee and in fairness to me, I think issues of who the committee brings before it is really the business of the committee and not for me to weigh in on.

MS. ROBERTS: Yesterday in her comments following the release of the two reports, the minister characterized this situation as complex, and yet this audit characterizes these issues as a lack of very basic oversight and management. Can I ask for your comment

on that contradiction which I am seeing as I look at the reports and at the response? Do you think that the problem in this case was one of complexity, or is this something that the department should have been capable of?

MR. PICKUP: My answer will be in fairness to others not to comment on anything anybody else said. I don't know the context of it, and I don't fully know the discussion around it. I think it's more appropriate if I stick to what I believe are well-founded audit conclusions.

To answer your questions, these were basic things we were looking at, so the failure to do some of the risk-assessment-type work, security assessments, threat assessments - the idea of doing those was not a far-reaching standard to hold somebody to. Is the world of IT complex? Yes, remembering passwords on 18,000 devices that we all have and changing them every month can be complex. But in doing security assessments and risk assessments, the concept that something might be higher risk because we're the first people in the world to implement it, to me, is not complex. That is fairly basic.

I look at this report and the discussion around it and the summary page, and much to the credit of the team that I have and the hard-working folks in the office, I think in reading those things, you don't need an IT degree to understand the things that we're talking about that ought to have been done as basics. I will hold to that rather than commenting on specifics of what somebody may have said.

MS. ROBERTS: I guess it jumped out at me as well in the additional comments from the Department of Internal Services that are included, in fact, in your audit report. On Page 17, it says: "What was learned in April 2018 is that despite the best of intentions, this site was the source of the unauthorized disclosure of information belonging to hundreds of Nova Scotians. This was not due to a single decision or oversight failure by the government, but rather a series of decisions, governance issues, and design shortfalls within a complex IT environment."

Reading that, I feel like there's an element of excusing away the lack of appropriate action and oversight. I don't know if you want to comment on that at all.

MR. PICKUP: My first comment, just for context on the context - in those responses, I'm going to be fairly easygoing here to say we pretty much let the departments write what they want to in terms of additional comments. This is a chance for them to write their comments. We don't audit this. We don't do a lot of back and forth. If there was something here that was obviously ridiculous, we would have a discussion to say, are you sure you want to say that? I'm not too comfortable with that. But other than that, this is a chance for them to put something there. This is a chance for a discussion.

If the committee chooses to call the department in and have a discussion with them on that, it may be worthy, and I said I wasn't going to comment on the Privacy

Commissioner's report, and I'm not going to other than to remind you of something that she put in there in terms of some of the quotes from some of the people in the department, one of which was a person who said they would do the same thing over again.

If the committee chooses to call in the department, that may be a discussion to have with the senior folks who come in. To ask something like, why would somebody say they would do the same thing over again if the lessons have been learned?

MS. ROBERTS: Indeed. Accepting that this was a lack of basic oversight, and assuming that the skill set required to do adequate oversight does exist within Internal Services, since it is the department of our government that is charged to have this expertise, what prevented that skill set from being deployed with this project?

MR. PICKUP: I believe, to really narrow it down to the ultimate failure at the beginning, was assessing this thing as low risk. It all fell apart from there. When you assess something as low risk and you place undue reliance on outside vendors and then not doing those risk assessments - the security, vulnerability and threat assessments - that ought to have been done, you miss the boat right away because you did that.

[9:30 a.m.]

So I think the question to the department that I can't answer would be - if somebody wants to pose it to them - how could you have possibly thought this was low risk, given all of these things that existed?

Again, I go back, I guess - to me, the proof of the pudding is that when this breach happened and they said, let's do the security assessment thing now, and then to come up with 20-plus vulnerabilities - half a dozen or seven of which were critical that could have been identified if you did this at the beginning.

I don't think it's a question necessarily of the skill set not being there. It's the same thing with the Architecture Review Board. You had the skill set there. You had the experts. You had the people. You had this board that said you have a six-month approval as a pilot - come back to us in six months and then you don't go back and tap into those folks and use them. There's where the mistakes ultimately occurred at the beginning, and it all went downhill from there.

MS. ROBERTS: So if I can tap the expertise of your office a little bit more to understand - how does a decision get made to determine that a particular project is low risk without doing a threat assessment? To arrive at that decision, you would think that you would look at the threat. Explain that.

MR. PICKUP: The initial risk assessment would be overall project. What risk level is this overall project? We might call it the inherent risk. This is where you would look at

things like - we're the first ones in the world to do this. That might suggest overall risk being higher, therefore we're going to do more detailed work, like a more detailed risk assessment, security assessment, penetration testing, all of these things. So it's that initial overall sense of how risky it is.

So we gave four or five indicators to say: first in the world to do this, the department going through organizational change. A number of things suggested that overall the risk was greater than low. Then you move into doing things like vulnerability assessments, security assessments as well.

MS. ROBERTS: In the course of the work of your audit, how would you characterize the conversation that was had, that reached the conclusion that this was in fact a low-risk project for the department?

MR. PICKUP: I guess it would be to some extent the omission of a full consideration of the potential impacts of something, like being the first in the world. Why is being the first in the world important? I think being the first in the world to do something is important because you don't have case history. You can't say, well, 35 jurisdictions implemented this, in 34 of those cases there were no issues but in one case there were five issues - we know going into it, high likelihood not many issues. So there was the omission of the full consideration of the risks around being the first jurisdiction.

It's not just, as I said, simply about being the first. It's what that gives you and does to you by being the first is not being able to look at other examples. So it's the omission of fully considering those types of things. It's things like the reliance placed on the outside vendors without a full consideration of that as well. It really is about sitting down and looking at the risks from the beginning.

MS. ROBERTS: Speaking to the relationship with the outside vendor, I'm just going to read a quote from the audit report. "The private sector is largely driven by their own goals and government must maintain responsibility for the public interest . . ." That seems like a very basic statement of fact. It's certainly how I understand our work here as legislators, as members of the Nova Scotia Legislature - it is to work for the public interest. But it seems that in this case, not only did the Department of Internal Services outsource development of a website, but it also outsourced protection of our privacy. We saw the results of that.

Can you speak to the relationship with the vendor? How long had this vendor been working with - I guess this department was new, yet it seemed like the relationship was long and established.

MS. WHITE: The relationship with this particular vendor had been going on for about 20 years at least. There are various versions of AMANDA in play at government, which is what this vendor was providing, and in various departments. It started in Service

Nova Scotia. It also extends into the Department of Community Services. The relationship is not just with Internal Services, and as Internal Services was being created, it established an even deeper relationship as those people and those applications were starting to come into that sort of centralized department.

MS. ROBERTS: As I understand, the total budget for this project that went so off the rails - the annual expenditure on this would have been in the range of $65,000. How much would the government spend on the whole AMANDA suite of servicing in a year? Is it partly the dollar value of this element of the work, the relatively small dollar value, that maybe led to that assessment - well, it's only $60,000 on top of however much. Was that maybe why it was deemed low risk?

MS. WHITE: That was not mentioned to me during the process, whether the dollar amount had any impact on how it was determined to be low risk.

MR. PICKUP: Two quick things, and I'm trying not to use up your time. I'll remind you of Paragraph 32 in Recommendation 5, on these contracts. When the team brought this to me to say that there weren't contracts in place with service expectations and financial obligations - I'll be honest - I said, haven't we done enough audits with that being an issue that people across government have learned to put contracts in place and have service expectations there? That is not what I would call a far-reaching concept.

The other point I was going to make is I did bring with me Chapter 3, which was the AMANDA audit from 2016. AMANDA was implemented in 1999, and at that point in 2016 when we reported, it had cost over $50 million to date, with about $4 million annually in spend.

MS. ROBERTS: The Architecture Review Board, I don't entirely understand it. Who convenes it? Who chairs it? Who would sort of trigger it being called into service to review a project like this?

MS. WHITE: The Architecture Review Board is made up of various members from throughout government. There is somebody from privacy on there. There is somebody from infrastructure, cyber security. There are different players that convene. I'm not sure about how often they meet and that kind of thing, but people submit projects and the projects are reviewed by the Architecture Review Board. More information is requested or not. Projects are approved or not through that process.

Right now, from what I understand, they are going through a change in their terms of reference. Maybe the department could broaden on that for you.

MR. PICKUP: One quick thing on that Architecture Review Board, to me, that I was kind of left shaking my head on is that it's not us who recommended you have this board. It's not us who put it in place. You have the group. You have the technical experts.

You have defined what they should do, that they're there. When they gave the department a six-month pilot approval, that sent a message that this thing should have been watched more closely. I find that, frankly, a big miss.

MS. ROBERTS: Yes. Do we know from the scope of your audit - and I know that the Privacy Commissioner also spoke to this - the extent of the breaches? We've talked about it as a privacy breach that was discovered April 4, 2018, but given that the FOIPOP public portal was basically an open door with no key from January 2017 until April 2018, is there any way of us knowing how many different breaches of personal information occurred during that time?

MS. WHITE: No, there is no way to tell. They used the logs that were available to determine who downloaded what pieces of information. However, there is a period of time where they do not have the logs, and some breaches may have occurred during that time.

MS. ROBERTS: Did you find any indication of a discussion at the level of the department about using a separate portal or limiting the design of this portal to only have it used for public disclosures?

MS. WHITE: Can you repeat that please?

MS. ROBERTS: Was there any discussion of using this new public-facing portal only for public disclosures - the sort of disclosures that are triggered by access-to-information requests by journalists or by caucus offices, et cetera?

MS. WHITE: That would have been a conversation that would have happened during their implementation process. We didn't look at that design aspect of it. We looked at how it was designed and what happened.

MS. ROBERTS: I would like to understand a little bit more of the threat risk assessment. I understand being the first in the world is a particular risk. What other elements would be considered in the threat risk assessment?

MS. WHITE: A threat risk assessment would look at things - a security assessment is part of a threat risk assessment, penetration testing, things in the environment, things from within the system. You would hire someone to see if they could break in, crack in. That would be part of the threat risk assessment overall.

MS. ROBERTS: Right now, in government, given what you know about the various systems that exist on the AMANDA 7 platform, I guess it is now, are there other systems that are vulnerable?

MS. WHITE: We did not look at any other systems in terms of their vulnerability. This specific vulnerability was the one we looked at for this specific system.

MS. ROBERTS: What should Nova Scotians expect the government to do to ensure new contracts with vendors do more to protect their personal information?

MS. WHITE: I think that the service expectations need to be laid out very clearly. They also need to make sure that they are staying current and up to date. Things are changing significantly at a very quick rate, so contracts have to change and be updated as well.

MR. CHAIRMAN: Order, please. That concludes the time for the NDP caucus. We'll now move to the Liberal caucus. Mr. Maguire.

MR. BRENDAN MAGUIRE: Good morning. I would like to start by saying that I think everybody on this committee and all government recognizes and acknowledges how serious of a breach this was and fully recognizes the role government has in this incident and are committed to making the change to better protect Nova Scotians. A big thank you to the Auditor General and the office for this very comprehensive and important report.

It seems to me just looking at the private sector and looking at government that 2018 was the year of data breaches. That seemed to be one of the big headlines in all the media from some of the giant social media companies - companies like Under Armour and things like that. Some of the weaknesses in their databases were exposed, and in some cases, billions of pieces of public or private information was exposed.

When a private company like Facebook, for example, is breached, there's a loss of public trust. There's an impact on their bottom line, their shareholders. They usually react immediately to try to restore public trust. In the private sector, if I feel that my data is not fully protected in a company like Facebook, I can just stop using their product - simple as that. When it comes to governments, the public doesn't have that luxury. They have to continue to use their services.

Your recommendations were very specific on what needed to happen to prevent future data breaches and to protect the public's information. What was the reaction from the employees at Internal Services, and from government? In your opinion, what was the reaction to those very important recommendations?

MR. PICKUP: I'm going to give my response based on my dealings with the senior folks in the department. One that I think is important is that there are some pretty serious findings in here, but there was never an attempt to question whether the findings were wrong, unless there was a back and forth on a technical issue. There was no attempt to minimize these, no attempt to dismiss them, no attempt to say we got it wrong.

[9:45 a.m.]

What I respected was, I think, a sense that what we were doing here was going to add some value. That, yes, the department was going to have some tough days to answer as to why these things happened, as they should. Ultimately, I felt that the team and our office was being respected in terms of being able to bring something to the table to help prevent this ultimately for the people of Nova Scotia, which is what we're all trying to do.

MR. MAGUIRE: Absolutely. Do you feel that there is an action plan in place or that there are remedies from the department based on your recommendations? Will you be keeping a close eye on that for all Nova Scotians to ensure that that data is protected, that it's secured properly, and that these issues don't arise in the future?

To me, obviously this is very unfortunate, and it is something that should never have happened, but it's also a learning experience for everybody involved. I kept hearing you saying "low risk threat," and I think what your recommendations and your report should do is open the eyes of everybody involved that any threat is a threat and that when these audits happen and when these recommendations come down, we need to react accordingly.

In your opinion, are they reacting accordingly? If and when an action plan is put in place, will your office ensure and give oversight to make sure that these are put in place? There's a lot of questions there, sorry.

MR. PICKUP: Yes, I'm keeping track of four, I think, in my head. The chairman can steer me if I have missed any of them, because it wouldn't be intentional. I would certainly come back to them.

One, the responses are concrete. I think I was going through the responses last night to our recommendations in this report. I'm not talking about any external action plan that was released. I won't comment on that.

In terms of the responses to our recommendations, I think last night going through them, I might have counted up 14 or so concrete things in the responses to the recommendations - I think I counted up probably 14 things. I hope members of the Legislature will look to the department to say, okay, you responded to the Auditor General's recommendations. We know he will be back in two years, but this is not stuff that can wait two years to make sure it's being fixed.

I hope that perhaps the committee will hold them accountable to say, okay, you gave these responses. Where are you on timelines of getting these things done? I have to be encouraged that they favourably responded. I have to be encouraged that there are tangible things in there. Now I have to be hopeful that they are held accountable by the appropriate folks and by the Legislature to do these changes. I believe that they want to.

In terms of the action plan, not having looked at the detailed action plan that they released, given the type of thing, this is a big deal for us. This is a big deal for everybody. When the team brought this to me and this all became public and as we were working through it, this was very upsetting, I think for all of us.

Having said that, we're going to keep a closer eye on this and see how government is dealing with the recommendations, probably stay closer to it rather than just waiting the two years. I will probably be in contact with the senior folks in the department more often for regular updates. We have had some of that discussion that we will probably do that - which is unusual. This is unusual, but this situation is unusual. We are going to stay closer to the department and not just wait the two years, and then use this also as an example to keep us informed from a risk perspective to see if there are other concerns we have that maybe we should be auditing something else along this as well.

I think I answered your four questions.

MR. MAGUIRE: Yes, you definitely did. Ultimately, to myself and most if not all Nova Scotians, this comes down to public trust. This comes down to maintaining the private information of all Nova Scotians when we access different portals on government websites. I think sometimes - myself, I know - you take for granted that your information is going to be safe and secure. If and when all of these recommendations are implemented, in your professional opinion, do you believe this will help restore the trust of Nova Scotians that their data will be safe and secure when dealing with government websites and government officials?

MR. PICKUP: I think satisfactorily implementing these recommendations and doing the actions committed to should go a long way to being more prudent in terms of managing these issues. I think as you alluded to, in doing anything today, you're never going to have 110 per cent certainty that nothing is ever going to happen, but you have to take all the reasonable steps.

I think doing these things that we do recommend and that the department indicates are the actions forward should put the province in a more reasonable position to say we are managing privacy, we are managing this information, in a more prudent way. That should give us more certainty than we had on the protection of information for people.

MR. MAGUIRE: I'll leave it with this and then I'll pass it on to another member of the team. As MLAs and as members of this committee, I think we all take this issue very seriously. We will all be keeping a very close eye on these recommendations. I know government will be doing everything within their power to ensure that this doesn't happen again.

With that, I'll pass it on to my colleague. Thank you for your time.

MR. CHAIRMAN: Mr. Jessome.

MR. BEN JESSOME: Two quick points to start. As we're critical of this situation, I think that it's important that we acknowledge two things - firstly, that we're dealing with the exposure of individuals' personal information. I don't think that should be lost. I know that's why we're here, but I think that it's important to acknowledge that.

Secondly, at the risk perhaps of being criticized for - I don't mean to sound like I'm undermining the severity or trying to avoid acknowledgement of the severity of the situation, but we're also dealing with department officials whose livelihoods revolve around the work that they do. Yes, there were mistakes made, but I think that I would just like to acknowledge the fact that they are invested in Nova Scotians as well.

I will table for the benefit of the committee an April 20th document that the minister has signed reaching out to solicit the services of the Auditor General's Office - indicating, I guess, further acknowledgement that there were mistakes made and an effort to attempt to rectify the situation.

In saying all that, I would like to focus on the relationship or the commentary in the initial section here related to a lacking or inadequate amount of consultation with the ARB. Can you comment on that statement, that there was lacking consultation completed with the ARB?

MS. WHITE: At the time that this project was being implemented, the ARB had specific guidelines for the types of projects that it was to look at. It would be things that touch the architecture of the government's network. The pieces that touch the government network were submitted for that six-month pilot project. The other parts did not have to be submitted to the Architecture Review Board at that time, so they were not.

MR. JESSOME: What I'm specifically trying to understand is that this is a group that has a mandate to oversee and approve these types of initiatives. What I'm trying to understand is if there was a go-ahead given that was done either without a recommendation to do so - right now, I'm seeing that there was a recommendation to move forward produced by the ARB. Why wouldn't government move forward with that recommendation in place?

MS. WHITE: Paragraphs 11 and 12 of the report basically lay out how the Architecture Review Board was part of this process. Yes, there was an approval for a six-month pilot for a piece of this project, not the entire project. The Architecture Review Board did not see the entire project either from the original application side of things nor the portal.

MR. PICKUP: I just want to add one more thing that I think is an important point. We remind you of this in Paragraph 12. When that six-month approval came for that part of it that Ms. White referred to, the ARB required that it be resubmitted to that group for

final approval, but the project went ahead without the final approval. They got a six-month approval for a piece - bring it back before you get final approval. They didn't bring it back.

MR. JESSOME: Can you comment on whether - I guess what I'm trying to ask is, was the timeline to initiate these components expedited to an unreasonable point? My thoughts are, was there a timeline that people involved were required to meet that was unreasonable in terms of identifying the risks or mitigating risks? Or was it just related to oversight, period?

MS. WHITE: If I could just go back to Mr. Pickup's last comment about the project that did not come back - that particular piece of the project actually did not occur anyway, but it still was not called back. No one knew what happened to that project. That piece was not implemented, just to be clear there.

Can you repeat your last question?

MR. JESSOME: I'm just curious if timeline had any impact on the oversight.

MS. WHITE: Both projects, the overall thing, because it was a low-risk project from the beginning - as Mr. Pickup had indicated previously, the timelines were explained to us, and no one seemed to have an issue with meeting those timelines because those other individual pieces were not intended to be done.

[10:00 a.m.]

MR. JESSOME: If only one component didn't end up being implemented anyway, as you have stated - should all the components have funnelled through the Architecture Review Board, before initiation?

MS. WHITE: At the time that this project was going through, there was not a clear expectation of whether or not it should go through, so the whole project did not go through the ARB.

MR. JESSOME: Okay, I understand. As your office has stated, there is the review of the mandate of that group that's under way. Okay.

I know I have a couple more minutes left, but I think Ms. Lohnes-Croft is going to jump in here.

MR. CHAIRMAN: Ms. Lohnes-Croft, three minutes.

MS. SUZANNE LOHNES-CROFT: This was discovered in April, and when you went in to do your audit, the department had already started implementing some risk

assessment. Can you tell us how far they had gone or what they were doing in that risk assessment?

MS. WHITE: At the time that we were . . .

MS. LOHNES-CROFT: They had already determined the 20 risks, did they not, and up to seven critical ones when you went into the department? Was that already done? How far into that had they implemented?

MS. WHITE: By the time that we had come in, the vendor as well as the department had already contracted out and had some results reported back to them on the vulnerabilities that were in the system.

MS. LOHNES-CROFT: So that's where they found the seven highly critical ones as well?

MS. WHITE: Correct.

MS. LOHNES-CROFT: So was that completed by the time you were in there? That was done?

MS. WHITE: Correct.

MS. LOHNES-CROFT: What had they started implementing when you came in for the audit?

MS. WHITE: At that time, we knew they had already plugged the vulnerability that had been the cause of the breach, and the system was already down.

MS. LOHNES-CROFT: What was that plug?

MS. WHITE: Coding.

MS. LOHNES-CROFT: It was all coding, okay. I don't understand coding that well, sorry.

MS. WHITE: In the process of putting in that plug, if you will, it broke the system in other parts, so they just could not bring it back live. It was decided just to keep it offline.

MS. LOHNES-CROFT: So that's what caused the delay in getting this site up and running?

MS. WHITE: Yes.

MS. LOHNES-CROFT: Okay, I didn't understand that. When you went in there, who did you interview in the management of this? The vendor, of course, you would have interviewed.

MS. WHITE: No.

MS. LOHNES-CROFT: Just people from the department?

MS. WHITE: Correct. We talked to the CIO, chief information officer. We talked to the project sponsor. We interviewed members of the project team. We interviewed the project manager for the second half of the implementation. We did sit down with the Halifax Regional Police as well to get their feedback on the breach. We had discussions with Architecture Review Board members as well.

MR. CHAIRMAN: Order, please. That concludes the time for the Liberal caucus. We'll move back now to the PC caucus. Mr. Halman.

MR. HALMAN: Just a point of clarification, how much time?

MR. CHAIRMAN: We're going to do 14 minutes.

MR. HALMAN: Thank you. Just going within the context of taking ownership and accountability, nowhere in the response to the report is anyone or any group held responsible. In order to move forward, do you think there has to be more specific accountability? Fundamentally that's what we're talking about here today - the best way to move forward to ensure the protection and privacy of Nova Scotians' personal information. Do you think there has to be more specific accountability built into this process?

MR. PICKUP: I think with accountability - I have to respect my role and mandate here. My job is to report to the Legislature on the results of these audits, make clear conclusions, make key recommendations, and give members of the Legislature the responses. Then in terms of what accountability means - in terms of discussion with the organizations audited by members of the Legislature with monitoring to see what happens with these types of things, notwithstanding what we do on follow-up - much of what happens in terms of accountability is really up to the members of the Legislature.

It's not really for me to say what I think MLAs should do with this report. I do believe though that as Auditor General, I hope this will be a useful tool obviously to hold the government and the department to account to say we're going to monitor, we're going to see that these things are being done, and we want to have a discussion - some of which has happened today - about how reasonable, how outraged, how concerned people are with those results.

It's not for me to answer some of those things. It's really for me to give you the tool for you then to ask those questions and to hold the government accountable.

MR. HALMAN: Certainly, appreciating your role - the role that you see for the Legislature, the role you see for this committee and our process. In following up on your recommendations, if a department or minister was taking privacy seriously, in your opinion, would they wait to hear from the committee - hear from us - before actioning these recommendations? Something doesn't line up for me here.

MR. PICKUP: Based on my discussions - not only with the team, but also my discussions with the senior folks at the department - I believe that action is under way. People aren't sitting by waiting to come to a committee or for members of the House to ask them questions. I certainly would never want to leave the impression that folks didn't take this seriously within the department, but I think now in terms of that accountability structure, I think answering to a group like elected officials gives that added accountability.

I believe that when we do audits, people act upon the recommendations based on the responses they give. Firstly because they believe it's the right thing to do. Secondly, I think part of the accountability and the encouragement for organizations to act upon our recommendations is the accountability process, but I don't believe that is the one and only driving force. I believe when people respond to our recommendations as they do, I believe they wholeheartedly mean what they say, and they do see the need to change. I do believe that.

To summarize, I believe the department realizes how serious this is and that they are now working on it, and now we all have to watch and hold them accountable to make the changes.

MR. HALMAN: "Accountable" is a theme we come back to time and time again. Most Nova Scotians in their jobs are certainly held accountable day in and day out.

My understanding is that the minister's mandate letter states that, "Internal Services should continue to implement robust cybersecurity and privacy programs that protect Nova Scotians . . ." Did the minister fulfill her mandate?

MR. PICKUP: I can talk to the audit findings. Did the Department of Internal Services, led by the minister, effectively risk-manage and project-manage these two projects? The answer was quite clearly no, and there is no disagreement or argument from the department with that conclusion.

MR. HALMAN: My understanding is that there were two recommendations in that 2016 report. One is to better manage the AMANDA contract and reassess terms before 2018. The second was to assess value, the cost of the contract before the 2018 renewal.

Again, with these two recommendations, which had a 2018 deadline - was there any indication that there was an action plan, that this was actioned?

MR. PICKUP: As part of our normal process, we follow up on all of the audit recommendations that we do so that we can answer the number one question I get asked on the street - what happens after you folks leave and what happens to the recommendations? The answer is, two years later we come back and we will tell you.

For the 2016 audits, we will be reporting in March of this year as to whether those recommendations have been implemented or not. Outside of that, given that we, over a two-year period, have up to 20 audits that we're following up - in that short window, we are not following up. I believe when I looked last night, I don't think the AMANDA audit came to the Public Accounts Committee so there probably wasn't an action plan or a follow-up timeline given to the Public Accounts Committee as to what was happening.

MR. HALMAN: I would like to direct some questions with respect to the rushing of AccessPro. Certainly, what I'm understanding is clear lack of oversight and risk management. You've indicated that there was no government project manager for the AccessPro project, which is quite alarming. I think any project you want to have that oversight. As you've indicated, these things are just standard operating procedure, so it is quite alarming.

In Paragraph 11, you stated that components that did not impact the government network were not assessed by the Architecture Review Board - the ARB. Did your audit come across any other instances or applications where information is being housed outside the government network and therefore not assessed by the Architecture Review Board?

MS. WHITE: That's not something that was part of our objective or criteria to look at for this particular audit.

MR. PICKUP: I will just add this quickly - somewhat related, but not to the ARB. This is something that will always stay with me from this audit as well, and that's in Paragraph 7. This was going to use cloud computing. The department developed a strategy in 2013 that included questions to ask around risks related to cloud computing, but those resources weren't used here so those questions weren't asked. That really concerns me.

Cloud computing is a reality, right? We're not suggesting that people shouldn't be using cloud computing, but when you have a strategy and you identify risks and questions, you want to make sure you use them. So that was another area that we haven't talked about, but I quickly wanted to get that point in there because it stays with me.

MR. HALMAN: Are you aware of any other instances or applications where information is being housed outside the government network and therefore not assessed by the ARB?

MS. WHITE: I don't know the specific applications and information that's being housed out there, but there are - I would rather not say. I'm not sure. The department should be able to tell you for sure.

MR. HALMAN: There just seems to have been this absolute rush to push this website to get it up and running. I think we've established that due diligence was not followed. Certainly, your report outlines that very methodically.

Did your audit find any indication that there was a conscious effort within the Department of Internal Services to push this project forward regardless of the usual procedural obstacles?

MR. PICKUP: What we really focused on here is what should have been done, ought to have been done, reasonably expected to be done, so that even if somebody did give us that, that might be part of a story. I'm not saying it was, but it wouldn't be acceptable. These are things that are a reasonable bar as to what should have been done and weren't.

MR. HALMAN: Paragraph 16 refers to the fact that the Freedom of Information website wasn't submitted to the Architecture Review Board because it was - to quote from your report - "a change, not a new application." You used the word "Currently" to begin that statement. From that, can we infer that if this whole process was to start again today, it would still not be submitted to the ARB?

[10:15 a.m.]

MS. WHITE: That is correct.

MR. HALMAN: Let's talk a little bit about oversight and the reliance on the vendor. I'm reading a lot about assessments and penetration tests, in a number of points throughout your report, and how they could have possibly helped point out the inherent weaknesses in the projects and the obvious oversight and the carelessness. Clearly there was no testing. There were signs while doing your audit report to suggest that at least someone had voiced that such a thing should be done.

In your investigation, in your audit, did you come across that other perspective that these things should have happened? Did anyone voice that to you?

MS. WHITE: Throughout the process, there were areas where it wasn't clear whose responsibilities, what they were responsible for. It stemmed from this reorganization of Internal Services.

MR. HALMAN: In sociology, that's known as diffusion of responsibility, where no one is taking ownership, where no one is stepping up and saying, I'm accountable. It

sort of comes back to that theme I have been talking about. I certainly appreciate the recommendations you have put forward, but it seems like there is that gap. Who or what group was fundamentally responsible? Why didn't anyone in this situation step up and say, look, we should be doing these things?

Am I correct in saying that there was no one who voiced to you in this investigation that maybe we should have done X, Y, and Z?

MS. WHITE: The chief information officer indicated to us that she has ultimate responsibility.

MR. HALMAN: With respect to the question I asked regarding the mandate letter, I would like to table that mandate letter.

MR. CHAIRMAN: I was going to ask, if you quoted from a letter, to table it, please.

MR. HALMAN: Yes, and I have that here.

MR. CHAIRMAN: There's 45 seconds if you have a quick short snapper.

MR. HALMAN: No, I think that concludes my questioning. Again, I have grave concerns that an ingredient is missing here with respect to accountability and taking ownership. Certainly, action plans are important, but I also think that moving forward, we have to make sure that the right people are in place to ensure that these changes that Nova Scotians expect - the protection of their privacy - are utilized to the utmost.

MR. CHAIRMAN: We'll move now to the NDP caucus. Ms. Leblanc.

MS. SUSAN LEBLANC: Thank you all for being here. Mr. Pickup, I just wanted to say that I really appreciate the work that was done here, in particular your comments about giving a real-life picture to the implications of this situation and what you described as an utterly preventable disaster.

I think that with a lot of things technical possibly, or just generally in government, we as everyday Nova Scotians sometimes don't understand the implication of a decision or a mistake until it actually affects us. Hearing these heartbreaking stories - in particular the one about the woman and her child's identities being revealed - I hope it gives all Nova Scotians pause to consider how government and the decisions made in government affect our daily lives. I want to thank you in particular for highlighting that.

Based on your comments, I'm wondering if you can comment on your concern or if you are concerned about the 600 missing documents that are still out there. Also, given the fact that we don't know if there were or could have been other breaches, I'm wondering if you can speak a little bit about that and the department's pace at which they are working

to contain those missing documents and looking to see if there's a way to detect other breaches.

MR. PICKUP: The aspect of containment, which is a critical part of this as well, was not something that was part of our audit work. That was something that the Privacy Commissioner did as part of her work and that she reported on yesterday. In terms of what is happening with that, I will leave that to the department if you call them in as a witness and let them explain to you what they are doing with containments since it wasn't part of our direct audit work.

MS. LEBLANC: You've mentioned before that the general practice for your office after you do an audit is to check back two years later. Earlier in this session, you said that you would be keeping a closer eye on the department's implementation of your recommendations. I'm wondering if you can clarify that and if you have a plan laid out to alter your regular practice. Are you going to come back in six months or a year? Do you have a codified plan for that?

MR. PICKUP: You're right, our plan for that is a little abnormal. It's a little unusual and I think it recognizes that this audit includes such important information and the privacy of information in people's lives.

What I've agreed with the minister and the deputy minister is that we've agreed on getting quarterly updates as to what is happening with the recommendations so that we have a sense of what is happening. Both from the perspective of this audit, but also from the larger risk understanding in government to say, for example, if this is uncovering other issues. Are there other audit areas that we should be considering? Are there issues preventing them from doing this more quickly or doing this as quickly as they planned? It's that kind of awareness.

Because we're 35 people and we have to watch what we're all doing, we're not intending to start doing quarterly public reporting on that. We're not going to do reporting to the House on that. This really is an agreement between me, the minister and deputy minister to say we all acknowledge that this is a really sensitive issue - we better stay close to it to give us the sense. Of course, that doesn't stop the committee from doing whatever they want in relation to following up with the department.

MS. LEBLANC: I'll just ask one more question before I hand it back over to my colleague. I just wanted to ask about the finding that there was a lack of documentation. Your audit found that when the FOIA website was implemented, there was no amendment or change order or new contract created. Can you explain how it is that a project would be able to move forward without a new contract in place?

MR. PICKUP: Sure. I will give the first part of the answer and if Ms. White wants to add to it, that's fine, and if you want even more detail, you can look to the department.

I think the easy answer is - or the quick answer is - there was this long-standing relationship there that already existed. I alluded earlier to how much money had been spent on this in the past, so I think that probably contributed to it - we already know these folks, therefore we'll get them to do it.

I'll just double-check to see if Ms. White wants to add anything to that.

MS. WHITE: Just that they were in the process of doing a change request to incorporate the new pieces, but they couldn't agree to the terms so it was never signed.

MS. LEBLANC: I just have a B part. Are you aware of any other instances where government has implemented a project without a contract or any definition of roles and responsibilities or financial obligations?

MR. PICKUP: You mean in relation to this or government-wide?

MS. LEBLANC: Government-wide.

MR. PICKUP: I'm going to say that is a big question - one to which I cannot give an answer because, again, we would have to do audit work on specific areas to be able to really answer that. So I can't say yes and I can't say no.

MS. LEBLANC: Thank you.

MR. CHAIRMAN: Ms. Roberts.

MS. ROBERTS: I do want to acknowledge that for many of us, though our lives involve using a lot of technology and also probably sharing some of our personal information online, many of us aren't aware of the specific safeguards that we are counting on various entities, both public and private, to put in place to make sure our information is safe.

There is a fundamental difference between a privacy breach at a Facebook or some large private-sector entity and a privacy breach with the Government of Nova Scotia, in that citizens are obliged to share their information with government. We're not obliged to share our information with those private-sector companies.

I do think about the cases of child protection, for example. There isn't an element of choice where you're choosing to do a transaction. It is the job of government - sometimes in extremely difficult and painful circumstances - to intervene in our lives. That is why that information is there.

Given that, what ought the bar for risk and the test for risk be and how ought that be perhaps different for the Government of Nova Scotia, versus a private-sector entity that is working to safeguard my credit card information, for example?

MR. PICKUP: Without disagreeing with anything you said - I wouldn't want to suggest that those factors contributed to us holding the government to a higher standard than a basic standard. I think the things we're looking at would be basic things, even if it was just transactional information.

Now, recognizing that these are the privacy folks that we are talking about, these are the folks who should know about privacy. These are the folks who clearly knew what type of information they were dealing with. How they could have assessed this as low risk is just very confusing to me to understand how that could be. I think in looking back now probably, when all this is laid out, they would agree.

MS. ROBERTS: I wonder, is there anything further that Ms. White would want to add in terms of what the bar should be? Should the test be a more stringent test because of the nature of information that is held by government?

MR. PICKUP: We both want to say something. I will speak as a non-IT technical person and then Ms. White can add her part.

I think it's incumbent on government to do the triage of that, if you will, to say okay, what is the impact if this type of information is disclosed? You do some sort of assessment to say okay, this is health information, this is family information, probably high risk to an individual if this type of stuff gets exposed versus something that might be lower risk. As a non-technical person, I would say I would expect the people who are responsible for the privacy of this information to be able to do that and to say okay, go through it and triage.

Now I'll turn to Ms. White to add her part.

MS. WHITE: There's really not a technical piece to that. The reality is it was private information that was being stored and potentially could be accessed. My comments were actually a mirror of Mr. Pickup's.

MS. ROBERTS: I want to go back to the Architecture Review Board because I believe I heard in a comment from Ms. White, a reference to the office of the Privacy Commissioner as participating on the Architecture Review Board. Can I confirm that? Is that correct?

MS. WHITE: The member on the Architecture Review Board is from the division with Internal Services, not the office of the Privacy Commissioner.

MS. ROBERTS: Thank you, so I misheard. I wonder if you would comment on the suitability of, or I guess on whether it would be advisable for that committee to tap into the resources and I guess the particular sensibility of the office of the Privacy Commissioner. Would that be a good step moving forward as we seek to regain public confidence in the province's ability to safeguard our information?

[10:30 a.m.]

MR. PICKUP: Part of the point of this ARB is, the government needs to figure out what they want them to do. It's not necessarily for us to say, these are all the things they should do, and here's what this should encompass. It's up to them to figure out what all of this means and to do it in an efficient and effective way, as well, without creating an overly cumbersome process.

I won't talk about the privacy report, but I would indicate that in that report yesterday, the Privacy Commissioner did mention that she was consulted in the days before and made some suggestions that weren't acted upon.

MS. ROBERTS: In one of my lives before being an MLA, I was a journalist. Certainly, as a journalist, I was party to many conversations about the frustration of long delays and cumbersome processes for accessing government information. Of course, that was one of the functions of this public-facing portal of the FOIPOP website.

It strikes me that the range of information that was accessible through that same portal, with the same lack of security, is really quite dramatic. We're talking about information that government is releasing to the public intentionally because it has been deemed to be public information. Then we're talking about some of the most intimate, personal, possibly damaging, information about private citizens.

Did you come across any analysis, or can you offer any of your own analysis, about whether it was even possible to do a risk assessment of that piece of Internet architecture given the range of information that was going to be accessed through it? It strikes me that we ought to have been talking about two very different doorways . . .

MR. CHAIRMAN: Order, please. That ends the questioning for the NDP caucus. Maybe we can get that in writing afterwards to you, about that question.

I'll turn it over now to the Liberal caucus and Mr. Wilson.

MR. GORDON WILSON: I certainly don't mind having him answer that question if that's possible.

MR. PICKUP: Sure, and I'm not going to use a lot of your time because the answer is quick. It sounds like you're looking to some of the design-phase-type work, which really

would be better suited to the department to ask them in terms of the design, why it was this broad.

MR. WILSON: I also want to thank you and your staff for this report, on my behalf and I think all my colleagues - it's been echoed it a bit that this is going to be taken very seriously by the government. We want to thank you and the privacy review officer for the thoroughness of those two reports, and the recommendations are going to be followed up on. I will touch on that a little later.

To start with, you had mentioned in your opening statements that this will only help repair - I think was the quote that you had - and only if recommendations are followed through on will we see some fruit from this. Can you explain the importance of follow-up in respect to this one report specifically?

MR. PICKUP: Sure, since I'm asked the question - Mr. Chairman, I respect the member for asking me the question, so I will give the answer. I do believe it's very important that the Public Accounts Committee follow up with the department on their action plan and ensure that it's being done on a timely basis. As I said earlier, we can't be everywhere every day following up on everything, but we will come back in two years.

I believe that the commitment to us through this audit is real, but let's say, for example, if there are challenges in implementing the recommendations, we will only know that really through follow-up. So follow-up is not just to make sure things are getting done, but it's also to understand the complexities that may be involved, the challenges that may be involved and new risks that may be exposed in doing things.

I would also link in with that - since you asked - the question on the AMANDA audit, for example. That one was done in 2016 with a similar issue to what we see here and really - to put it fairly bluntly, I guess - there was no follow-up done outside of us. As I said, our process that we can reasonably handle with the resources we have is a two-year follow-up so that will be in March. So follow-up, I think, is critical.

I will say though quickly that in fairness to the Public Service, to the people that we audit, I believe that when they commit to responding to the recommendations and they're doing something, they believe it. I do also believe that accountability, including the Public Accounts Committee, is an added element to encourage them.

While it's often not reported, probably the number one question I get at the Superstore or Costco is - or people start with the assumption, you make all these recommendations and nobody ever does anything with them. I tell people that's not true. When we followed up in early 2018, 75 per cent of the recommendations were implemented within two years.

So I need to be hopeful, but I think hope has to just be a foundation over which follow-up occurs. I thank you very much for the opportunity to talk about the importance of follow-up.

MR. WILSON: You didn't have to link in that second part because I was going to ask you specifically about the AMANDA report also. I was going to ask you a little later, but I'll go into it right now, seeing that we're there.

You noted several times that that report you tabled in this House did not have subsequent witnesses brought in after the fact to talk to that. Can you speak to that?

MR. PICKUP: Sure. We did that audit in Fall 2016. We made a number of recommendations, including a couple of which parallel to this report. I have to believe as Auditor General that it is important that when we do these audits and report to the House that members of the Legislature use those reports as a way to hold the government accountable. That may be things like the Public Accounts Committee calling in the department as a witness. This is one of those audits.

I remember at the time when I was here talking about AMANDA - because I did talk about that in terms of my report day - and saying, this is one of those areas that is important. It may not get a lot of public and media attention on that day because it is just some government system that does A, B and C. I think I even recall saying, unless something happens, that's when you're going to hear about AMANDA. That doesn't diminish the need for follow-up because we pick these audits to do areas that are important. They're important and hopefully they work well. In this case, we see an example of something that didn't work so well.

I think follow-up would help and we certainly wouldn't then be having the discussion today as to whatever happened with those recommendations from the AMANDA audit because probably we would all be aware of that already.

MR. WILSON: Do you know any specific recommendations that were in that report that could have impacted outcomes?

MR. PICKUP: Sure. Now I do have to be fair. There were recommendations in that AMANDA audit that are similar to here, but we do have to remember the timing. That audit we produced in 2016. While we're reporting on this breach this week, a number of the things that were occurring on this were taking place at the same time. So whether or not the timing would have lined up probably would depend where and when the questions would have occurred.

I think I have to be fair on that and not opportunistic in saying, had you done everything in AMANDA audit, maybe you wouldn't be in this. The timing was a bit of an issue here when you look at the Appendix 2 time frame.

MR. WILSON: I guess you know what I'm getting at here. The importance of having all the Auditor General Reports come before this House is significant. The importance of having witnesses subsequent to those chapters is significant. The importance of follow-up for each and every recommendations is significant for the future moving forward of our province. I hope, I really do hope, that we as a committee, and I do believe that we are moving in that direction.

I will assure you that on our side - I have heard it from my colleagues, but they never mentioned us when they said it - I will guarantee you from our side that we will follow up and we will track those follow-ups. I will give each and every one of you my commitment on that. That's key. I don't want to harp on that much more, but it is important to note that.

It was a complicated read quickly yesterday and a busy day that we had, to understand all of the underlying implications of a series of things that failed to protect this data. I am curious about one aspect of Recommendation 3 that was made. I don't believe I have heard this asked, about project management expertise. How would the lack of expertise in that area have contributed, just in project management of the data breach?

MS. WHITE: It depends on which project.

MR. WILSON: The portal, for example. Am I wrong in saying that if the portal was secured, if there had been a real gate key there, this might not have happened? Is that too simplistic?

MS. WHITE: The portal project had a project manager who was experienced in project management and actually is from the project management office of the province. She followed the procedures from a project management framework perspective that the province uses. The project sponsor should have been able to provide some more of the documents that were requested by the project manager throughout the process for the portal side of things.

MR. WILSON: Okay, that's helpful in understanding that.

I do also, Mr. Pickup, enjoy the five or six questions that you always give us. There are a couple - I don't know if I can squeeze them in quickly here - that didn't get asked also. What role will the expert in-house group play in going forward in the assessment of the new IT systems or changes to the existing IT systems, in your estimation?

MR. PICKUP: We made the recommendation as you allude to in Recommendation 2, that they should look to define the scope of responsibilities of that ARB. In the response, the department said that they are currently reviewing the scope, mandate, and processes being performed, and they will determine what improvements and enhancements need to be done. At the point of the audit, they weren't in the position to tell us exactly what those

were going to be, that they were going to be working on those things. Perhaps in follow-up, they can then decide.

To me, it's very much the difference between the auditor and management. It's not for the auditor to figure out what you want that ARB to do. It really is for management to say, here's what we want the ARB to do.

MR. WILSON: Just quickly, what is the department doing now to ensure the safety and security of data, that you know of at this moment?

MR. PICKUP: I think one of the big things that they did was recognizing back in April, when this breach occurred, that the threat assessment had to be done. They did that threat assessment working with the vendor, and they identified a number of vulnerabilities that had to be dealt with. I think reacting quickly like that - I certainly have said more than once that that should have been done from the get-go, but I think then recognizing that they had a problem and they had to do something was a big first step at that time.

MR. WILSON: I believe I only have two minutes left here. I am curious also - in your report, you mentioned that there were some problems with the tender contracts. I didn't hear any details. Do you have any details on what - or can you explain a little bit about what happened there with the tender contracts?

[10:45 a.m.]

MS. WHITE: The software is proprietary and specific to this vendor, so in order to issue a tender for a new application, they would have had to start all over again because there are no other vendors that could support the application that was coming forward. Does that make sense?

MR. WILSON: Is there another way you could explain it?

MS. WHITE: The vendor that the contract is with outsourced the application to a subcontractor, but that subcontractor can't provide the services that the province needs to support the application overall. That's the main vendor that the province has the contract with, so no one else can sort of come in and take over for that.

MR. WILSON: Is this a common problem with other large applications that we might have that you would know of?

MS. WHITE: That I don't know.

MR. CHAIRMAN: Thank you. If the Auditor General's Office would like to have some final comments - Mr. Pickup.

MR. PICKUP: My final comments will be brief. One, I very much want to thank you for the questions today. It certainly is one of the things that makes doing this job worthwhile and interesting to see ultimately the people we report to - members of the Legislature - interested in our work and engaged in our work.

I'm really pleased that this is a very clear example where everybody agrees, whether they're elected folks or whether they're us or the people in government, that this has to be fixed for the protection of all Nova Scotians. We're all individuals - we all have a story. We all have families that have stories and we expect that information to be held private where government has it, so it's in all our interests to see these recommendations implemented.

I also want to thank the people at the Department of Internal Services. This was a tough audit for them. There are some tough messages here. Yes, they didn't do the job that they should have done, but I respect that we can sit down with those folks and they can acknowledge that, and they can say, yes, you got it right, we've got to do better. We can stand up and shake hands at the end of it and say, okay, we're all in this for the betterment of the people of Nova Scotia, now let's move forward.

There's no time wasted in playing games and wasting energies, nobody ever reports that. But for that I do have respect for the public servants and for the people we deal with and who the team deals with - acknowledging, to somebody's point earlier, that these are people and people who ultimately want to do a good job.

My final thanks would be - this was unusual for us to do an audit with another organization, so my respect goes to the Privacy Commissioner and her folks as well. We ended it yesterday, but I think it was a very good process. We got to use our efficiencies. We looked at different things, and ultimately, I think the day served Nova Scotians well in terms of getting the full story and full picture. We're still talking at the end of it, so that's probably a good sign as well.

I will end on that and thank the people in my office. One quick reminder without sounding self-serving is to remind you that this is our third report in four months, and for that I say thanks to the people in my office. We're only 35 people, and for the folks who those reports go through, all of us, that is a big accomplishment vis-à-vis other audit offices. It's not me to thank - it's the two people with me and the 32 other people who are across the street working on the March report. Thank you.

MR. CHAIRMAN: Thank you. We just have some short committee business to do. If you want to refer to the correspondence that we've had sent back to us from the Nova Scotia Gaming Corporation, we have a response to the December 12, 2018 motion. Are there any comments, questions, or concerns?

Hearing none, we also have a letter from the Department of Communities, Culture and Heritage on information requested from the January 9th meeting. Any comments or concerns about that? Does that letter answer the question that was posed of the grants? I believe the cost of those grants might have been included in that question but I'm not sure. (Interruption) It wasn't, okay.

As we have adopted endorsement of the Auditor General's Reports, the committee has adopted the practice of endorsing those recommendations. The Auditor General has now presented his January report to the committee today. Can I have a motion put forward to endorse those recommendations? Ms. Lohnes-Croft.

MS. LOHNES-CROFT: Yes, Mr. Chairman, and we thank the Auditor General and the Privacy Review Officer for their investigation and report. This was a very serious breach.

That being said, I move that the Public Accounts Committee formally accept and endorse the recommendations contained in the January 2019 Report of the Auditor General that have been accepted by the audited departments or agencies. I ask those departments and agencies commit to and take responsibility for full and timely implementation of the recommendations accepted by those departments and agencies.

MR. CHAIRMAN: Would all those in favour of the motion please say Aye. Contrary minded, Nay.

The motion is carried. Mr. Halman.

MR. HALMAN: I'd also like to put forward a motion that along with endorsing the Auditor General's recommendations, this committee should also endorse the recommendations of the Privacy Commissioner.

MR. CHAIRMAN: Would all those in favour of the motion please say Aye. Contrary minded, Nay.

The motion is carried. Thank you, Mr. Halman.

There being no further business, our next meeting will be on January 30, 2019, here in the Chamber, when we have officials from the Nova Scotia Teachers' Pension Plan, the Nova Scotia Health Employees Pension Plan and the Public Service Superannuation Plan about public sector pensions, Chapter 3 of the October 2018 Report of the Auditor General.

There being no further business, the meeting is adjourned.

[The committee adjourned at 10:52 a.m.]