HANSARD

NOVA SCOTIA HOUSE OF ASSEMBLY

COMMITTEE

ON

PUBLIC ACCOUNTS

Wednesday, March 25, 2015

LEGISLATIVE CHAMBER

Department of Internal Services
Governance of Information Technology Operations

Printed and Published by Nova Scotia Hansard Reporting Services

Public Accounts Committee

Mr. Allan MacMaster, Chairman
Mr. Iain Rankin, Vice-Chairman
Ms. Margaret Miller
Ms. Suzanne Lohnes-Croft
Mr. Brendan Maguire
Mr. Joachim Stroink
Mr. Tim Houston
Hon. Maureen MacDonald
Hon. David Wilson

[Mr. Terry Farrell replaced Mr. Brendan Maguire]

In Attendance:

Ms. Kim Langille
Legislative Committee Clerk

Mr. Gordon Hebb
Chief Legislative Counsel

Ms. Ann McDonald
Assistant Auditor General

Ms. Janet White
Audit Principal

WITNESSES

Department of Internal Services
Information, Communications & Technology Services

Ms. Sandra Cascadden, Chief Information Officer
Ms. Carolyn McKenzie, Acting Executive Director, Infrastructure Services
Mr. Glenn Bishop, Executive Director, Corporate Information Strategies

House of Assembly
Nova Scotia

HALIFAX, WEDNESDAY, MARCH 25, 2015

STANDING COMMITTEE ON PUBLIC ACCOUNTS

9:00 A.M.

CHAIRMAN
Mr. Allan MacMaster

VICE-CHAIRMAN
Mr. Iain Rankin

MR. CHAIRMAN: Good morning everyone, I call this meeting to order. I would ask you to please turn your phones to silent so we don't have any disturbances. I'd like to begin with introduction of committee members.

[The committee members introduced themselves.]

MR. CHAIRMAN: Today we have with us the Information, Communications and Technology Services Branch of the Department of Internal Services. Ms. Cascadden, would you begin with an introduction of yourself and your colleagues and also some opening remarks.

MS. SANDRA CASCADDEN: Mr. Chairman, good morning. My name is Sandra Cascadden, I am the Chief Information Officer for Information, Communications and Technology Services at the Province of Nova Scotia. I'd like to introduce my colleagues with me today: Ms. Carolyn McKenzie, the Acting Executive Director of Infrastructure Service Management; and Mr. Glenn Bishop, the Executive Director of Corporate Information Strategies.

Good morning and thank you for the opportunity to be here today to discuss the governance of information technology and operations. My opening comments will focus on what we do in the Information, Communications and Technology Services branch, part of the Internal Services Department, to enable government to deliver programs and services to Nova Scotians.

I'd like to begin with a brief overview of how government has evolved its IT management policies and practices in recent years. In 2009 the Chief Information Office was created with a mandate to plan, organize, and direct efficient use of information, communications and technology, and to manage the government information IT assets. Before that time there was significant investment spent on IT with no single accountability or method for measuring progress or sharing successes. Bringing everyone together was a significant change, it allowed us to better coordinate IT infrastructure activities within the province and create a stronger governance model that enabled the IT community to better support the strategic direction of government.

Our model has evolved. Last year the Chief Information Office became the Information, Communications and Technology Services Division of the Internal Services Department. This move was made to reflect our new focus on effective and efficient service delivery to the provincial government and other public sector organizations. This move also brought together the Nova Scotia SAP service management group, as well as the information access and privacy group which is responsible for FOIPOP, all within ICT Services.

On April 1st of this year our mandate will evolve yet again, as the first wave of a new shared service delivery model kicks into place across the public sector. In addition to the government departments that will become part of Information, Communications and Technology Services, the provincial health authorities, with the exception of clinical applications, school board IT and some Crown corporations, will also become part of and will get services delivered from ICT Services. This is the first time the government has consolidated many of the corporate administrative services into one body.

This first step in consolidating IT that took place in 2009 laid the foundation that supports this next major step forming a fully functional IT services group that not only supports infrastructure but supports business applications, corporate applications, technical infrastructure, information records management, access and privacy. This gives us a unique and exciting opportunity to form a longer term vision and mission for IT operations and IT information management.

We're making excellent progress as we prepare for this change. We expect that streamlining and modernization of many of our processes and tools will result in improved service delivery and capacity for Internal Services and our client departments as well, and support the long-term sustainability goals of government.

We are in the early days but this model is already working and we're seeing many differences with things that we're doing with our partners. For example, recently we've worked very collaboratively with the health sector in the purchase of software that will go across the health sector and the province. This will provide cost-avoidance savings of $3 million in three years and up to $5 million between four and five years. This represents a 59 per cent discount because of the volume that we create across multiple entities.

I'd like to share some more details around the operations within the provincial government. We underpin most of the government business. In some way we manage nearly 11,400 desktop computers and laptops; we manage 3,700 mobile and wireless devices; we host over 1,000 servers and 600 business applications. We are involved in everything from online vehicle registration with Service Nova Scotia to working with the Health Information Technology Services group (HITS), providing levels of support to them so they can manage health care records and information with the Department of Health and Wellness, district health authorities and the IWK.

We are also responsible for providing daily IT support to government employees as they deliver services to citizens. We manage an average of 390 contacts per day at our service desk and we support many client department projects and changes in our environment. We have a portfolio and project management office that is now in place and that effectively manages the larger IT projects, which deliver a broad range of services to government.

We operate in a safe and secure environment through security committees and processes that had been established to manage risks across projects, applications and the government infrastructure. The security of our data and infrastructure is critical. We're working closely with the Emergency Management Office to ensure business continuity. The departments have business continuity plans and disaster plans so that the government is resilient should anything happen.

We are leading key components of open government - initiatives like open data, access, and e-government - which will transform the way Nova Scotians connect and receive services. It's a very exciting time for information management and technology in the public sector as we bring about the next generation of service to Nova Scotians.

I must say that the invitation today to discuss the overall broad context of governance and information technology and operations in the departments was rather broad. We did our best to further clarify what the request was and we have absolutely done our best to prepare for today. We look forward to receiving the committee's questions about the operations and governance of IT.

MR. CHAIRMAN: Thank you. We'll begin with Mr. Houston of the PC caucus, for 20 minutes.

MR. TIM HOUSTON: Thank you for those introductory comments. Just to give me some perspective of your team and your group, how big is the team and what type of budget do you run that team with?

MS. CASCADDEN: We currently have a team of approximately 238 IT professionals and our budget is around $36 million. As of April 1st, that team will expand by another 237 people as we bring in the other IT departments across government and the budget will increase to approximately $95 million.

MR. HOUSTON: I noticed in your comments you were talking about changing the way that government connects with Nova Scotians and the way that it offers services to Nova Scotians. I did see in some of the pre-reading that I was doing that it was a goal of the group to move the province toward a single window to government for citizens. That's an important goal. I know that I've come across a lot of things in my constituency - you might have one citizen, a youth, who is interacting with Education and Early Childhood Development, also Health and Wellness, and maybe Justice. They're touching many parts of the government and they're all in separate silos. So I'm just wondering about that particular goal of moving the province toward a single window to government for citizens - how that goal is progressing from the IT perspective.

MS. CASCADDEN: The goal of a single window is important and as the IT group, we support the various government departments in their vision of delivering their services that way.

One of the big departments that we are working with as it pertains to this is Service Nova Scotia. They certainly, being front-facing to the government, really want to make sure that the way that citizens and businesses interact is very, very easy. So in the back end, from a pure IT perspective, what we're doing is we're preparing, through a major project that we have - and the project name is called Signet, which is the way to identify someone who is requesting services. The biggest thing we have to do is we have to make sure that when someone is requesting a service, they are who they say they are and they have the right to access the services and get the services that they are requesting. Also, that identity carries them through the request for multiple services from multiple departments.

The Signet project is a project that is really around identity management and that will give you your own identity to get to the services. We have completed Phase 0 and Phase I of that project, we are moving into Phase II of the project and we've recently put some RFPs out on the street. We're moving very successfully in creating that back-end support for all the government departments to deliver their services.

I'd like to hand over the rest of this question to Glenn Bishop because he can talk in a little bit more detail about that particular mission.

MR. HOUSTON: Okay, I appreciate that. Glenn, just a couple of very specific questions as to, is it a 10-year project, a five-year project? Then the second part of the question is, would that enable an employee of the government to just pull up a citizen's record once they're properly identified and see all the places they're touching government - is that the goal? When would that be ready?

MR. GLENN BISHOP: I appreciate the question. First to your question in length of this project, Phase II that Sandra just talked about is going to conclude at the end of March 2016. As you can appreciate, these kinds of efforts are very incremental in length. What the effort will do up to March 2016 is put us in a base system that allows us to get to where we need to be, in terms of making sure we have what we call levels of authentication that are appropriate for the first sets of transactions that will be coming on board.

Once we get to that point we're going to move to a state of operation. Then this becomes a regular operation in which we will continue to add more and more services as the piece matures.

The second question you ask is about accessibility. This is one of the most important things about this particular project, it ensures privacy and this is one of the very important things that we've talked about right from the beginning of this initiative, to ensure privacy for the citizenry. This does this in two ways: specifically, we have an internal approach which is for employees only, that allows accessibility to only what employees should be seeing, not personal information for the citizenry; then there's an external view, an external accessibility which is for the citizens themselves. It's allowing the citizen to set up an account to be authenticated as to who they really are so they can then go in and access only what they should see and have controls over whoever sees their information. It's used only to what they consented it to be used for.

MR. HOUSTON: Thank you. It sounds like a long-term goal and certainly it sounds like maybe the first couple of years are all to do with security and making sure that the right people are seeing the right information.

In terms of security, security of data - and I know some of the mandates of the team are to provide efficient, effective and secure services to the province so there's lots of moving parts there - where does security rank in terms of your priorities of your job?

MS. CASCADDEN: Security ranks extremely high when we're considering everything from the implementation of a new system through to the operations of our existing systems. When we start, and we start with the implementation of an information system, we go through many steps before we actually implement the system. One of those steps is a privacy impact analysis. In that privacy impact analysis we go through a detailed checklist around the security side of the system. Even before a new information system is contemplated, even before an RFP hits the street, we start the privacy impact analysis work.

MR. HOUSTON: So in terms of security it should obviously be very high, it's probably the most important aspect I can see of what the group does. I appreciate the strategy for all projects going forward.

We do have a bunch of legacy systems that are in use and have been in use for quite some time and I have a few questions about the security of those systems. Specifically, do you have information on the number of security attacks against the provincial network in 2014?

MS. CASCADDEN: We do track the number of attempts to get into the infrastructure of the network, I'll say, because there are many doors to our house. One of the front doors is through the Internet pipe and that Internet pipe is guarded by very traditional software and hardware that most organizations have; they have multiple firewalls. Those firewalls have rules and those rules stop certain things that are known to be threats. We have rules on the firewall that very specifically . . .

MR. HOUSTON: So would you be willing to say how many attempts there have been?

MS. CASCADDEN: There are thousands of attempts pounding on the front door of every organization, but those attempts are stopped at the front door through the security policies, the tools and the technology that we have.

MR. HOUSTON: That's the goal, anyway. So there was a CBC news story that said, I think it was in December maybe, the story that said that there were five successful attempts in 2012-13. I don't know if you're familiar with that story but it said, "Hackers hit Nova Scotia computer network 5 times last year." So those would be attacks that actually were more significant than an attempt that actually had an impact in some way on the government, and there were five of them. Are you familiar with that?

MS. CASCADDEN: Security is very complex. There are hacking attempts, there are just malicious attempts and they're all very, very different. Hacking into the network is very different than someone who opens up an email that may have a virus attached to it. There have been a number of things that have happened where somebody has opened up an attachment in an email and a virus has happened. That is very, very different than a hack into the network.

MR. HOUSTON: These five instances, I believe, were hacks.

MS. CASCADDEN: I'm just going to pull up my files.

MR. HOUSTON: This was 2012-13, there were five and I'm just wondering, my first question on that was is five a lot?

MS. CASCADDEN: The nature of the five that we had, the first was a web server. A web server itself can be attacked in multiple different ways. The first thing is, if a web server is outside of our network, it could be attacked and we have nothing to do with that; that's one scenario. Another scenario is a web server that's inside of our network, but has been built by another company who hasn't kept their software up to date; that would be another type of attack.

On January 17th, that particular attack was on a web server. It wasn't a personal attack on a person, it wasn't an attack on an information system that contains personal information - it was a web server that was hacked into. Usually what happens in these things is they put up advertising for performance-enhancing drugs, with a number of those web server attacks.

On January 30th, we had a similar attack . . .

MR. HOUSTON: Just in the interest of time, without going through the five different attacks and types of attacks, my general question to you is, in your capacity, is five a lot?

MS. CASCADDEN: No, five is not a lot.

MR. HOUSTON: Five is not a lot?

MS. CASCADDEN: No.

MR. HOUSTON: That was for 2012-13. Do you have the corresponding number for the next year, like how many attacks there were in the next year?

MS. CASCADDEN: We have a number of different ones that we have tracked and what we would consider how we would respond to it under our risk security response. We've had a couple of web servers that have been attacked. They've just been compromised in the same way, somebody puts up a message that doesn't belong on a government web server. There are two of those that we've had.

We also have had a number of email malware. What has happened with those is someone has opened up an email that has an attachment that actually is infected. Now it's very interesting that the email account they used to open up the attachment was not a government email account, it was a private email account - so it was like Gmail or Hotmail - because inside government you can access your normal email accounts plus you can access any private accounts. It was the private account that was actually hacked. The virus was put in the private account but when the private account is opened up on the government network, it then has access to your contact list and then starts rolling out other emails.

MR. HOUSTON: So all those instances would be reported.

MS. CASCADDEN: All those instances are reported.

MR. HOUSTON: How many of those would there have been?

MS. CASCADDEN: We had six instances of those particular email events. The majority of them ranged from December 17th to January 28th. During those events, as soon as we find out an event happened we then track it. We take the computer, we isolate the computer, take it off the network and get the user to turn the computer off so the virus doesn't continue to move through the system. Those particular events ranging from December 17th to January 28th, there were about between 100 and 120 computers that were infected at that particular time.

MR. HOUSTON: Is there a point in time when there's a security attack against the government that it should be disclosed to the public that this has happened? I know in these types of instances you're talking about here - and I assume you have other categories and other numbers for them - we did do a FOIPOP request to find the number and the request was denied so we know there were attacks.

I'm just wondering at what point in your mind would it be important for the government to disclose to the citizens that their network has been breached in some manner? Right now there has never been a disclosure, I don't think, of any type of attack against the province, right?

MS. CASCADDEN: To decide which ones you would disclose or which ones you wouldn't disclose, certainly if we disclosed the email virus, those are so commonplace that that's probably not newsworthy. There has been no breach of information, like information did not move outside of our network, it was really more of a nuisance because it's malware, malicious intent, just to bog down your network. Certainly we can disclose if any of our websites happen to be compromised.

MR. HOUSTON: But should you disclose if something has happened that has made you believe that people's personal information is at risk? Would you feel that would be something the province should be disclosing to people?

MS. CASCADDEN: We actually have one piece of legislation on the Personal Health Information Act that states that if an information system on the Health side of the house is breached and a person's personal information is actually viewed or moved or seen by those who shouldn't see it, we do disclose. We assess the situation and we disclose.

MR. HOUSTON: So you'd contact those people individually, presumably, and say hey, something may have happened to your data here?

MS. CASCADDEN: Yes, that's right.

MR. HOUSTON: And that's limited to Health? That doesn't extend to Community Services?

MS. CASCADDEN: At this time it is limited to Health, because of that Health piece of legislation. The advantage of the formation of the Information Access and Privacy

Services group within the ICT group is that it's one area that we're going to look at because the FOIPOP does not cover the disclosure of a breach. It's only that Personal Health Information Act that does. One of this group's mandates will be to look at that for the broader government.

MR. HOUSTON: That certainly sounds like a useful exercise to look at that. I want to talk about the Community Services thing a little because the Auditor General released his report reviewing the security of the Integrated Case Management System. In his report, the Auditor General found that there were "significant weaknesses" in the IT security of systems. Those were his words, not mine.

The first question on that is, I'm just wondering - without going into specific detail of actual things you might do - how often does your team search for security holes and vulnerabilities. In the Auditor General's Report, they said they tried to hack into the system and were able to hack into the system with what they described as kind of unsophisticated tactics. I'm wondering, do you do any of that type of stuff across your systems yourself?

MS. CASCADDEN: Yes, we actually look at our systems. First we monitor the systems on a daily basis and we monitor any abnormal activity either going into a system or out of a system because that might be an indicator something is going on. We also do tests on a number of the systems. The configurations on the systems today - as technology progresses, the configurations may change. We will go back and change those configurations to increase the security side.

MR. HOUSTON: I have heard this term - white-hat hackers, which are friendlies that you engage to hack into your system to find vulnerabilities. Is that a tool you use to protect data?

MS. CASCADDEN: Our last cyber assessment was in May 2014. We had that assessment and then once those things are found, we then work our way through to clean them up. So yes, we do use organizations to do that.

MR. HOUSTON: So those are third parties? Do you have people on staff whose job it would be to just constantly search for vulnerabilities?

MS. CASCADDEN: We do have some people on staff who do make sure our systems are secure as well as engaging other companies and organizations to assist us in doing that because it's a very complex . . .

MR. CHAIRMAN: Order. We will now move to the NDP caucus, and Mr. Wilson.

HON. DAVID WILSON: Thank you for being here today. I know when you first hear about this topic, I think most people would think, oh well, it's just dealing with the IT stuff, but it is an important area of government to ensure the privacy of information that is gathered is protected. So you have an important role to play, especially as we see your branch expand over the next coming months.

I'm just going to go back a little bit to what my colleague was asking about around the hacking of the system and back to the same report he mentioned. In 2013 we had five computer networks that would be considered hacked and at that time I believe you had mentioned that on a scale of one to 10, those hacks were about a level or range five, which is kind of in the middle. So we shouldn't be overly concerned, but we should be concerned.

The hacks that you've mentioned in your response earlier, so far for last year, what would you range those attacks? Am I correct that there were about eight attempts last year? Five the year previous, but about eight last year?

MS. CASCADDEN: Certainly the website hacks - and I'll just use that term, it's kind of an invasion of the website - those are really about your reputation. Something appears on your website that shouldn't be on your website so there's a bit of a reputational risk associated with that.

The challenges with malware and the things happening in the email where you get a corrupted email and then that starts sending out more and more emails, that's more of an issue of what will it do to the performance of your system, how does it block people's inboxes and things like that? The websites, again, I would rank as low, so it would be the four or five type of thing because nothing has really happened, it's just somebody posting something. The email side of the house can be more of a nuisance and if left unchecked it could block your network, so I would rank those between the five and the six, but I think we're in exactly the same place because it's basically the same types of things that have happened this year that happened last year.

MR. DAVID WILSON: I know in 2014, the Auditor General, Jacques Lapointe recommended that the chief information officer should ensure all computers are configured to encrypt their data and this would involve, from my understanding, two levels of security: a password and a random code. I believe at the time the recommendation was accepted, so how close is government to meeting this recommendation from the AG's Report?

MS. CASCADDEN: When we came in about this time last year and were talking about the IT asset management, we actually made some really good inroads even at that time and we have continued to progress significantly as well. Every device is required to have a password so a BlackBerry device, a tablet device, laptops, computers - that's kind of your first line of defence. The second line of defence that we did put in is the encryption of devices. At the time we were here last year we concentrated primarily on laptops because of their mobility and we made significant inroads; in fact, at that point every new device that was purchased since April of last year was purchased with encryption software. Everything new that came in the door had the encryption software on it.

What we've then done once we worked on all the new devices, we then started to go backward, so we went into the existing devices and we're moving the encryption software on those existing devices. We're about 60 per cent complete on the existing devices so, again, we continue to make really good inroads on that.

For us we're really not protecting the really hard-core asset like the laptop or the iPhone, that's just a device, we're really protecting the information that's on those devices or access to the information that those devices may have, so that's what we're really protecting when we do this.

MR. DAVID WILSON: So you're at about 60 per cent. Have you given yourself a timeline on when you would maybe be at - I don't know if you'll ever be at 100 per cent but close to it, I would assume, is your goal. Is there a timeline that you foresee knowing that as you grow it's going to make it more difficult?

MS. CASCADDEN: I'll say 99.9 per cent. What happens is we have a refreshment rate of four years, so in theory, after four years every device will have been refreshed which means it would have to be procured with this technology. In about four years we will be at 99.9 per cent, and I would say it's actually going to be sooner than that because we're already a year in so we're probably between two and a half or three years before we would actually get all the devices protected because of the refreshment. But we're going to go backward as quickly as we can.

MR. DAVID WILSON: Also, I'll kind of piggyback on some of the questions on disclosure, knowing under the Health and Wellness Department there is legislation that covers that - do you have a timeline? I think you indicated that there's a group looking at departments across government that would, I assume, include Community Services. Is there a timeline with recommendations that may come to the minister? I would assume that legislation would need to be brought forward to the Legislature so is there a timeline, and on top of that, would we foresee seeing something in the upcoming session that would involve covering the rest of the departments under the disclosure Act, I would say?

MS. CASCADDEN: We don't have a timeline right now, we're just forming this group as of April 1st. We recognize there is a bit of a gap on the disclosure of information or a privacy breach. That has been noted and that will be one of the things this group will work on. It has been noted as something to do but at this point we don't have a timeline for that.

MR. DAVID WILSON: Because of the concerns we've heard not only from the Auditor General, would it be worthwhile to maybe bring in temporary legislation that would cover sensitive information in Community Services, for example, to get us through? I would assume it might be a couple of years before we see legislation that will cover every department in government.

Would it be beneficial, in your opinion, to bring legislation in maybe temporarily, to cover off the concerns that were noted by the Auditor General?

MS. CASCADDEN: That will be one of the things that we will consider as part of going through this process. Certainly we'll be working with not only the Information Access and Privacy group, working with the various departments, but we'll also be working with the Review Officer on this as well. We will consider all options here, especially as it pertains to personal information and the fact that we need to make sure people are comfortable that we are managing personal information properly.

MR. DAVID WILSON: Thank you. Just going to the wrongdoing Act - and I know now, if my memory serves me correctly, that it covers only government employees, not employees of the district health authorities or school board. I believe you mentioned you're taking on the responsibility of the Nova Scotia Health Authority, I guess, once it's amalgamated. Do you foresee an amendment coming to encompass those employees also, under the wrongdoing Act, so that your responsibility in the yearly accountability report will cover off really what your work does and what you oversee within your branch?

MS. CASCADDEN: When the sectors come in and become part of the IT shared services group, all the employees coming in will actually be employees of government. So in the way that we deliver services, we will be covered and they will be covered under all the Acts that we have.

There will be other things that we have to do in consideration when we are delivering services to the sectors. Those types of things we are working our way through as we create shared services. But from an employee perspective and our branch perspective, all the people who are delivering services into the sectors will be government employees.

MR. DAVID WILSON: I know in last year's report, the fiscal year 2013-14, there was nothing to report. Not to pre-empt, and I don't know if it's in June that you disclose this, but have there been any reports in the last fiscal year that you would be required by legislation to acknowledge in your accountability report?

MS. CASCADDEN: We're gathering the information. At this point there is nothing to my knowledge that we'll be reporting but we will be going over all the information from the previous year just to make sure we're reporting the right things and not missing anything.

MR. DAVID WILSON: I just want to go quickly to something that I wasn't anticipating talking about but you mentioned it in your opening comments. It was around the work you do for Access Nova Scotia on the online vehicle registration. I would take it that you oversee that component of Access Nova Scotia - is that correct?

MS. CASCADDEN: We will. We don't at this point and we're only doing it from an information management and information technology service. We support the application and the technology behind the application. We don't make any of the business decisions around that application.

MR. DAVID WILSON: The reason I go there, which I know more recently the minister has indicated a possibility of government looking at outsourcing those types of services so how is it that you're not taking it over yet - you're going to take it over. Has there been any discussion with you and your minister and the other departments that are working on what that would mean for you and your branch if they're looking at potentially outsourcing registration for vehicles, for example?

MS. CASCADDEN: With regard to the RMV system and the activities that are happening in Service Nova Scotia, I have been in contact with Service Nova Scotia. They are in the very, very preliminary days of looking at the various options. It's only once they start looking at the options and figuring out which ones are viable, they will then bring us in to have conversations on how it may impact how we deliver services and how we interconnect with whatever their decision will be.

They have a fair bit of work they need to do on their side to figure out which is the best model and the best option for them to consider. That was the conversation that I've had with Service Nova Scotia so we will be engaged in that conversation.

MR. DAVID WILSON: Are you confident though that you could manage the online component of registering the vehicle and the work that you foresee that you should be doing, or will be doing, unless they change course down the road?

MS. CASCADDEN: With regard to the RMV system, when the information technology staff comes into the shared services group, we get all of the people who are currently managing that system coming in to us and they will continue to manage that system the same way that they have managed it up to this point and they will stay together as a cohesive group in order to do that.

It's only once that Service Nova Scotia makes a decision that we all have to work together to figure out how that might change, but the creation of shared services really is bringing people together to afford different opportunities, but when they come together they're still going to support the system as it exists today, the same way that they're supporting it today. So I'm confident we can support the system into the future as it stands today.

MR. DAVID WILSON: You had mentioned also in your comments that there will be an additional 237 IT individuals coming over as of April 1st, I believe is what you said. Going through some of the material, we noticed that there are, in the structure - and I would assume it's the management operation, service transition, service manager structure - that there are some vacancies.

One of the vacancies we noted was the manager of business continuity. Could you maybe elaborate what the role of that position is and - there are a number of vacancies - why is there a hold on filling those positions until you transition the other 237 over? So maybe just on that one position, could you elaborate on what that position is and then maybe elaborate a little bit more on why there seems to be quite a few vacancies in the organizing structure, which I would call management structure of your branch?

MS. CASCADDEN: With regard to vacancies, we have actually been holding vacancies and we've been doing that very strategically. The holding of vacancies will allow us a greater flexibility when we start pulling ourselves together in the shared services organization, which means we'll be able to move people around, or when we bring in people we may have more directors than we require and we would be able to take these vacancies and reassign them to different areas.

Specifically around the manager of business continuity, we actually had a director position around risk management and business continuity. The person who was the manager is currently in the director role so we have the person who was in the manager position performing a director-level function, but we have kept the manager position vacant, again just to give us the flexibility as we move into the new organization so that we can put the resources where we need to put them in growing our new organization.

MR. DAVID WILSON: I know a lot of the transition is to try to streamline and look for savings. I know the Minister of Internal Services has indicated the potential of roughly around $60 million in savings through shared services over two years and that Internal Services through procurement, IT and Telecom, will account for half of these savings, so roughly about $30 million. Is that an achievable goal and can you support that idea of the savings being about $30 million over the next two years?

MS. CASCADDEN: There has been extensive work done on the shared services initiative. We've been engaged with consultants over the last little while. In fact in the last year we have worked very diligently on the business case associated with shared services.

As part of that business case, we've identified where there are key areas of opportunities. One of the opportunity is very, very significant when we're together as a single group. Those areas are areas of infrastructure, especially when we bring in the health sector there's a lot of duplication from the infrastructure side of the House. Again, in my opening remarks I made a comment about the Province of Nova Scotia and the health sector working together and we actually saved $3 million as a result of a contract.

So there are some very real savings associated with infrastructure and greater volume purchases. There are also very real savings around what we call application consolidation. That means we have a multiple number of applications and what we'll do is we'll streamline the number of applications so we don't have the duplication. There are opportunities around that as well.

The next level of opportunity is, we'll move to things more like self-service where we don't have to have a warm body going to a place or people answering the phones all the time; we'll actually serve up more things electronically. There are some opportunities around there as well.

MR. DAVID WILSON: Similar to what our parks will have soon, a self-serve entry. I guess I'm out of time so I'll leave that and I'll come back the next round.

MR. CHAIRMAN: Thank you, Mr. Wilson. We'll now move to the Liberal caucus and Mr. Stroink.

MR. JOACHIM STROINK: Thank you very much for your presentation today. I guess I want to expand a little bit more on the shared services. It is a huge project that you guys are undertaking and the cost savings, as you spoke to, are about $30 million to $60 million. Can you walk us through where you guys are with that whole process and what needs to still happen to ensure that we get a complete working system?

MS. CASCADDEN: Absolutely. Shared services is a big initiative. It's a lot of change, it's people changes as well as technology changes and process change.

What we have been doing over the last year is we have been finalizing the business case associated with shared services. That business case is - I'll say the hard core business case, which is the financials, but it's also putting together the operational model: what will we look like as part of shared services, how will we operate, what services will we be delivering, how will we be delivering those services, what structure do we need to put in place to deliver those services. All of those things that we have been working on over the last year.

When we look at what the scope and the magnitude of shared services is, certainly we start with the CIO office, about 237 or 238 people, our first group that we are bringing into the shared services organization is the government IT people. In the government it is called the IT CSUs and that is around the 338, 337 FTEs, plus all of their applications. That's happening in wave one on April 1st.

The second wave for shared services to bring into shared services is actually the health sector. The health sector will be bringing another 200 people into the shared services organization so by the time you are through the health sector, the ICT Services will be around 600 to 650 people, and then the budget and the responsibility that comes with that.

The third major wave will be the education sector which we are targeting for April 2016. That will bring in between another 130 and 150 people. At the end of the day we'll be an organization that has around 858 IT professionals providing services to all the government departments, the education sector, the health sector, and as well we've also identified five Crown corporations that we'll be providing IT services to as well. We're working our way through those various waves.

What we have to do is collect a lot of information from each of those entities about who is doing what from an IT role perspective, what services they are providing, what applications they are supporting and how they are supporting them, what issues and concerns they have about moving the yardstick forward. We've just concluded the information gathering, the budget transfers, and the people transfers for government departments for April 1st and then next year we'll start having our conversations with Health, Education, and the Crown corporations.

MR. STROINK: By doing this now you've created a more insular group of people and a more streamlined business. How does that affect the security? I'm assuming the security would be way stronger now with this new program in place.

MS. CASCADDEN: Bringing groups of people together, actually bringing a larger number of subject matter experts together so Health, for example, has a very, very strong security group because of the nature of the type of information they deal with in their information systems. That group plus the government group, plus the Education group, we will build a really strong security group as well as building a strong client services group, and a business and corporate applications group. The more people we have the better we'll be able to service our customers. It also creates a really nice environment for IT professionals to work in because it will give people an opportunity that if they've always worked in the Education sector but would like to work in the Health sector or with Community Services, they can move across the various departments if they so choose.

The other thing I have done from an organization structure perspective is I've actually created a chief security officer position and we are putting additional resources on the security side of the house.

MR. STROINK: What would be some of those securities that you're going to implement?

MS. CASCADDEN: We'll be moving people over and what we'll be doing inside that organization structure for the chief security officer is we'll be creating positions that will drive more policy, more monitoring, we'll engage with other entities. There is a lot of pan-Canadian and jurisdictional support on the security side of the house. We have to beef up this area because the more services we put online, the more we have to track and the more we have to monitor. We'll be looking at are there additional tools that we should be procuring to automate processes and to track. We have tools already, but we can always augment our tool sets, so those are the types of things people will be doing. They will be looking at kind of the rules we have on our various pieces of equipment and making sure that they're standardized, so we're just going to up the game.

MR. STROINK: That sounds great. I also kind of want to touch on the data centre. You had a tender out there for a new data centre for Nova Scotia, to create a better, secure environment and then you pulled it back. Where are we now with that?

MS. CASCADDEN: Over the last year we actually recently worked with a consulting company and it took us through a new strategy as it pertains to data centres, so we're very pleased to say that we do have a strategy, we will be moving the secondary data centre forward. That secondary data centre actually provides us business continuity and business resiliency, but during that time we weren't just at a standstill, we were actually doing extra work on the back end to ensure our key systems were backed up and we had an alternate site for key systems. So even though it took us about a year to get through to the strategy that we're now comfortable with, we have made moves where we have invested in technology and we have invested in a second location to provide the redundancy on some very, very key systems.

MR. STROINK: Is that second location in Nova Scotia or is it out of Nova Scotia?

MS. CASCADDEN: The second location is in Nova Scotia.

MR. STROINK: Great, thank you very much.

MR. CHAIRMAN: We'll now move to Ms. Miller.

MS. MARGARET MILLER: Thank you for your presentation and all the information. I know when I started university and people were getting involved with computers - that was the early 1970s - there wasn't a whole lot of people. So you hear all of this now and to hear about everything that you're doing, the value of information and especially to hear about the amount of savings that this merger is going to bring about is really great.

I did have something though that gave me a little bit of concern when you were talking about the self-serve option, that things would eventually go to a self-serve option. At this point I already hear a lot from seniors who are having issues because they're not computer literate and wondering if there's always going to be a warm body there somewhere that's going to be able to help those people.

MS. CASCADDEN: When I talked and referenced self-service, my primary reference was internal - how we deliver services internally. So instead of having to call the service desk to have your password reset, you can actually go on one of our websites and have a password reset very easily.

We will always have the backup of a warm body - internally for sure. I'm sure if you talk with the other government departments that are delivering the services directly to their clients, they will feel that way as well.

I think it's very interesting in today's generation that people are starting to get more comfortable with requesting services and getting services electronically. It's actually becoming an inconvenience to have to pick up a phone and place a call at a certain time and make sure you place that call during operating hours. So it's very interesting how we see the shift happening and it's across generations. It's very interesting when we talk about seniors and embracing technology. Seniors are really starting to embrace technology much more, especially if there are grandchildren involved. They're Skyping with grandchildren and emailing and things like that, but we certainly recognize that not only would it be seniors, it would be multiple different types of populations that we would have to ensure that we deliver services differently.

Really it's about shifting how you deliver services so instead of by the phone or on a counter, which is the most expensive way, can you reduce that and increase the electronic means? That really just shifts the dollar value and the cost of delivering a service, so there are some significant opportunities for the various government departments because they're the ones that really have to make that decision on how they deliver their services. We provide the infrastructure and the capabilities for them to do that.

MS. MILLER: I do agree that seniors are learning very quickly and I've witnessed some of the programs at the libraries for seniors, which are really great because it gets them out and doing different things and really opens up their social life in a lot of cases where they've been sitting home and now they're doing more things and engaging more people.

I have one more question about the FOIPOP sector and the information technology involved with that. How is that changing compared to what there is now with FOIPOP and what you're going to be seeing after April 1st?

MS. CASCADDEN: I think it's really exciting actually, what we're doing in the area of Information Access and Privacy. FOIPOP is one part of that group. Currently what's happening on the FOIPOP side of the house and the structure that we have within government, very similar to information technology, it's very disparate and pulling it together will actually give us greater opportunities.

Some of the things we're seeing is there's an increase of FOIPOP requests. There's an increase in the sophistication of those requests. We're seeing that because of that sophistication and the increase in requests, it's really putting pressure on the single individuals that are out there in departments, which is usually how it has been supported. So pulling people together as a group will really support better coordination of the requests and better consistency about how those requests are responded to because there will be standards associated with building that as an entity.

The other thing that we're also doing - and it's probably a bit of an advantage being an Information Access and Privacy group attached to a bunch of IT people - is that we're looking at information systems to support the FOIPOP requests and really make it a much more automated process, because today in Nova Scotia it's a very manual, paper-based process and there are tools available that could put the FOIPOP request and the entire process online and electronically. So we are looking at those tools to enable and support the FOIPOP team. The fact that we're bringing them together will enable them to deliver better service, more consistent service, deal with the complexity and the frequency of the requests coming in, plus we'll provide them with technology and tools that will enable them to do their jobs better and actually providing a better way for people to request FOIPOPs.

MR. CHAIRMAN: Thank you, Ms. Miller. We'll now move to Ms. Lohnes-Croft.

MS. SUZANNE LOHNES-CROFT: How much time?

MR. CHAIRMAN: You have until 10:07.

MS. LOHNES-CROFT: Okay, thank you. Wonderful to have you here today and you are very busy with your April 1st date and another April 1st date is the amalgamation of the district health authorities. I want to ask with all that, what role will you be playing in the transitioning they are going through? My understanding is that they will all be using the same system, whereas now they are all working in little silos. Could you talk to that and the efficiencies that may bring about?

MS. CASCADDEN: Certainly the consolidation of the district health authorities into the Nova Scotia Health Authority, plus the IWK - there are two entities that we will end up working with and supporting into the future. In fact we actually work with them today and support them today in many, many ways.

The creation of the single health authority is actually very beneficial from an information, technology and information management perspective. In the past when there were the 10 district health authorities each of them had their own way of doing things. In some instances they had some of their own information systems which meant that there were disconnects, certainly if a patient travelled from one area to another area.

Over the years we had worked within those information systems and we've consolidated a lot of those systems already. As the health authority pulls itself together and has an overall governance of all of the delivery of the programs in the health authority, it makes it very much an easier initiative for us to talk about information systems. For example, we work with the health authorities and we wanted to put in an emergency department information system, we'd have to talk with 10 different health authorities, 10 different emergency managers and each of them probably had 11 different ways of doing things. So when it comes to configuring an information system it made it very difficult for us.

When we have a single health authority plus the IWK, they're going to streamline their business processes which then make it very, very easy for us to help them get to their business objectives by putting the IT system in place. The future construct of a single health authority plus the IWK will be incredibly beneficial and it will enable us to get information systems across the whole health authority.

What happens in information technology is that the business has to align and the business has to figure out how it has to run and then we come in and deliver the system to support the business. When you have 10 different businesses doing things 10 different ways, it's very, very difficult to put one system in place to do that.

We'll also be working with the health authorities on the new vision and the new direction to reduce the number of information systems. The reduction of the information systems means there will be larger systems across all the health authorities so that disconnect about information not moving from one place to another, we'll start breaking those barriers down. The change of how health authorities manage themselves will certainly provide us the opportunity to help them even more when it comes to information technology.

MS. LOHNES-CROFT: In that, when you take a collaborative practice that is using their own IT system for sharing amongst their practice, what will be the security that will keep that information there? Can a doctor in Halifax - it won't be Capital Health - would a specialist in Halifax be able to access those records or do they maintain in that one, cohesive, collaborative practice?

MS. CASCADDEN: I'll respond to your question based on the environment we have today and then I'll talk a little bit about the future of where we hope to go. We have big hospital information systems and there's a lot of patient information in hospital information systems. Then we have information systems that are in private practices - CECs or GP offices. Those smaller systems are governed by those offices. So we put in the technology in the back end and we support the technology. We make sure that the technology is locked down but the day-to-day privacy practices are the responsibilities of those physicians and the physician offices.

What we do is we make sure that information flows between those systems. In the future we're looking at how we can have a larger single system that has greater governance with regard to security and privacy, respecting the fact that for example, physicians are their own independent business people, which is a challenge on the information system side of the house, respecting that fact, look to see how we can increase that confidence that information is where it needs to be and not where it shouldn't be.

In today's environment we have, and through the IT group on the health side of the house, they have the governance over those big hospital information systems, so they have policies and practices and things that actually lock down those systems. They have tracking mechanisms to make sure that if you shouldn't have seen that record it's flagged and they can track that. We make sure that the information from those hospital information systems doesn't flow to any place it shouldn't go.

The doctors' office systems, those doctors are responsible to maintain their day-to-day security. For example, if their front office clerk leaves, they have to shut down that account and make sure that nobody else uses it. So there are different practices. The future vision is the one-person, one-record system where we have many, many less systems which then actually tighten up security because every link in the chain, if you have many links in the chain there are many places that there could be issues.

MR. CHAIRMAN: Order. Thank you, Ms. Cascadden. We'll now move to the PC caucus and Mr. Houston.

MR. HOUSTON: Thank you, Mr. Chairman, very prompt with your times today. You mentioned the creation of a new position, the chief security officer. That's a position to take effect when?

MS. CASCADDEN: We're planning to have the new organization structure early in the new fiscal year so it's on the organizational structure. Job descriptions have been written, the postings are waiting to go.

MR. HOUSTON: So you have that ready to go and you also mentioned adding additional resources to that person. Do you have any idea how big that team would be?

MS. CASCADDEN: At this time we're planning a team of between eight and 10 people directly associated with that team.

MR. HOUSTON: Do you know what type of budget range you have for that security group?

MS. CASCADDEN: I don't have it off the top of my head, I can certainly bring it in.

MR. HOUSTON: Earlier you did mention that there are some people already on staff who kind of do some white-hat hacking and you also use third-party organizations as well. The people you have on staff who do the white-hat hacking is it their full-time job or is it kind of part of their job?

MS. CASCADDEN: It would be part of their job.

MR. HOUSTON: I want to go back to the Community Services Integrated Case Management system. I do hear a lot of theoretical prospective changes and improvements that will be made to security over data. There are lots of things in the works, I guess, that are going to happen over time. Meanwhile we still have a lot of data today that's sitting in different systems and the Auditor General was able to identify pretty serious weaknesses with this one system that's used by Community Services, the Integrated Case Management system.

Now that's just one system that's used by Community Services, presumably other departments have their own systems that would have been developed over time. How many other systems would you say are out there that would be under your kind of management through your department?

MS. CASCADDEN: In my opening remarks I had mentioned that there are somewhere around 600 other applications and systems . . .

MR. HOUSTON: Most of those would be off the shelf. I'm talking about just systems that were kind of homegrown for departments that are relatively important to the management of the - the Community Services Department can't operate without this system from what I understand, presumably there are other ones for other departments that are similarly important. Would there be a half-dozen of them?

MS. CASCADDEN: There would be a number of homegrown systems, it would be under 100 across government.

MR. HOUSTON: Okay, so there's a lot of them out there. In terms of the Integrated Case Management system, was your team aware of the security weaknesses in that system before the Auditor General discovered them on his own and made them public? Were you aware of some weaknesses in that system?

MS. CASCADDEN: With regard to the ICM system, we do provide the back-end support, so the servers, for the application. Any of the items that were identified in the Auditor General's Report that were co-owned by Community Services and ICTS were identified as co-owned. A lot of the items that were brought to our attention were things that we would have been responsible for and a number of those were very, very quickly remedied even before the Auditor General left the door.

One of the things I do want to say about the work that the Auditor General did on that system, when the Auditor General did their work, what they did was they worked from within the government system to get into that system. They did not come from the outside into that system, they were already privileged users inside the government system who then tried to break into the system. What they did and how they accessed the system has to be taken into consideration when you think of what the risk is. The risk isn't at the front door because the Auditor General actually has keys to the front door and actually can get in. What the Auditor General did is came into the next room which was also locked, but because they're privileged they could get through other gates.

MR. HOUSTON: Right, understood, but still very significant nonetheless. Almost 10,000 people work for the province and that's a lot of friends, neighbours, cousins and people who could be inside the system to begin with.

MS. CASCADDEN: No. The security challenges inside the ICS system were associated with those who had privileges to the system already. For example, anyone who did not have privileges to that system would not have been able to get into the system . . .

MR. HOUSTON: So you have to work for the Department of Community Services?

MS. CASCADDEN: You would have to have had an account associated with that system to give you access to that system somewhere.

MR. HOUSTON: So it's individual user access levels.

MS. CASCADDEN: That's right.

MR. HOUSTON: In terms of that, do you have any way of knowing whether or not the Nova Scotians who had their data in that system - because when you have an interaction with the Department of Community Services you don't really have an option, they know everything about you, your SIN, whether you have children in foster care, what your income is and stuff like that, they have a lot of sensitive information in there - so do you have any way of knowing whether or not the Auditor General, if he was able to reach across and see some data that he shouldn't have seen or his team shouldn't have seen, it could have happened with other employees of Community Services, they could have breached that. Do you have any way of knowing whether or not that happened, that people actually saw information that they shouldn't have?

MS. CASCADDEN: My understanding is the capability of seeing information that shouldn't be seen could only be performed by someone who knew what they were doing, it couldn't happen accidentally. You would have to be a super user who knew what you were doing and purposefully did something that crossed the boundary of the access to information that you shouldn't have access to. It's not like if I were a user of that system I could go in and see everything and anything that I wanted to see, that's not the case in the observations associated with that system. If I happened to know some back ways around something, which means I would have to be a very sophisticated user to do it, I could have gained Access to information that I shouldn't have access to in my role associated with my access to that system.

MR. HOUSTON: I don't want to downplay the risks though. The risk is real so I'm just wondering at what point - it seems like you believe the risk is minimum. I guess that's your assessment of it, but I'm still trying to get a sense from you as to what point would the risk be at a level that you should notify people that, hey, your personal information may have been breached?

I'm thinking in the private sector you often hear major companies - like I remember Target and one of the banks saying, your information probably wasn't breached, but it might have been so keep an eye on your transactions and stuff like that. So is there a similar line in the government? I actually feel that some of these people should have been told - your information may have been seen by people who shouldn't have seen it so keep an eye on things that are happening there. You don't think that's the case in this situation?

MS. CASCADDEN: I'm actually accompanying Community Services to the Public Accounts Committee on April 1st very specifically to have this conversation. So for me, there are a couple of things where breaches should be disclosed. The first is if it's an external to internal breach, so someone who should not have access to the system - period - has accessed the system and pulled information out to take it and do something with it. That would generally be someone with evil intent in the outside world not associated with the information system.

The next level of breach is when something happens inside the system and someone looks at information or uses information that they should not have access to. Now, the question is, what did they do with that information?

MR. HOUSTON: But that could be the case here.

MS. CASCADDEN: Right, and so the question then becomes - what did they do with that information? Did they go into the system knowingly looking for something? That would, in some systems, be looking up information about your neighbour or your ex or something like that - information that you shouldn't have access to. That absolutely should be reported and there would be processes within any department or organization to deal with someone breaching that because that's just like taking a file off of a desk and going through . . .

MR. HOUSTON: But in this case you wouldn't have known. I guess my question is, do you know whether or not that happened?

MS. CASCADDEN: In this particular system, my understanding is there is no way to see if someone looked at information that they shouldn't have access to.

MR. HOUSTON: Right, so if you don't know - the discussion will continue next time, but I think to protect people you'd assume that it did, but we can have that discussion next time.

In my last three minutes and 27 seconds, I do want to switch gears a little bit. I know in B.C. there's an office that's responsible specifically for monitoring how many privacy breaches occur by a department. I think in B.C. between 2010 and 2013 there were 2,700 privacy breaches that were reported. Is that something that you're – (a) I don't think we do that here; and (b) is that something we should be doing here? This could be anything, like you sent an email with sensitive data to the wrong person or all these types of privacy breaches. Is that something that we currently track and should we?

MS. CASCADDEN: This is one of the challenges that we have with our very decentralized structure. Each department is responsible for collecting and managing any privacy breaches. They usually do that with their FOIPOP people. Usually FOIPOP and privacy are combined.

I believe that the amalgamation of that whole group coming together will actually strengthen us in this area. So if you ask today, does any one group have all of that information, the answer would be no. Do individual groups have access to that information? I would say yes. Is it managed consistently? Probably not. So the opportunities that we have in front of us, also with the new Review Officer as well as the new IAP group, will strengthen ourselves in that.

MR. HOUSTON: So as we sit today, it would be group to group or department to department, whether or not they have to even report that they sent, in my example, an email to their own recipient with sensitive data - they may not have to report that in some departments and in others they may. Is that pretty much the case today as we sit here?

MS. CASCADDEN: I would say there are different levels of the way they manage it department by department. I think the less sensitive breaches are probably managed differently. The very sensitive breaches are probably managed consistently, because of the magnitude of the breach, but I think the email sent to the wrong person may be managed differently.

MR. HOUSTON: In light of the numerous other systems that we talked about which correspond to the case management system, did you get direction from the minister after the Community Services one came to light that the minister said hey, go and check these other ones, too? Did that kind of ramp up efforts on checking the other systems for different types of vulnerabilities?

MS. CASCADDEN: The Auditor General actually comes in and does checks on various systems. The Registry of Motor Vehicle system, for example, has been checked by the Auditor General. Because the systems are currently owned and operated by the department, we're usually supporting in that audit but that audit is generally directed by the department that owns that system. There are times when . . .

MR. CHAIRMAN: Order. I'm sorry, but I must interrupt. We'll now move to the NDP caucus and Mr. David Wilson.

MR. DAVID WILSON: I just want to continue on where I left off. It was on the line of questioning around savings that we'll see through this kind of - I'll use amalgamation, I guess, but consolidation of your branch.

Forgive me if I'm not confident in the numbers that the government has provided with the potential savings of $60 million. I say that because there was a commitment from the government to save about $15 million on the amalgamation of the district health authority in the first year and we know that's not going to happen. The minister came out - and I thank him for coming out and being forthright and saying no, that saving is not there, we may see savings down the road. So when we hear the Minister of Internal Services tell Nova Scotians that there's a $60 million saving through the work you are going to be doing over the next little while, within two years, I want to be confident that is a true reflection of what's going to happen.

You indicated in a response earlier a potential of about $3 million in savings that you foresee. With that $60 million, about $30 million will come through procurement, IT and Telecom - is that an achievable goal for you? Are you going to be able to deliver - and that's your role, to deliver government's policy - are you going to be able to deliver that type of savings for Nova Scotians and for the government?

MS. CASCADDEN: Out of that $30 million actually we're responsible for about half of that within ICT. It's going to be very interesting to track these savings because those savings are projected out over five years so we're going to be starting at a certain level. Over those five years we're actually going to be growing information systems and technology, so at the same time we're trying to drive savings, we actually going to be adding to information technology, both in FTEs and systems and things like that.

We're committed to keep two pieces of paper, I'll say. One piece of paper to track all of the savings that we achieved as a result of this consolidation, and another piece of paper that says at the same time we tracked savings we also had to grow ourselves because the increasing demand over those five years for information technology and information services.

Will there ever be a single piece of paper that says here's the savings? Very difficult because of that growth and decline. I think and I believe there will be certain areas where we will actually be able to run much more efficiently and there will be some really hard-core savings that we will be able to demonstrate.

One of the commitments we've made with regard to any people reductions as part of this process is that will be done through attrition. Attrition is something that we don't control. It's when people decide to retire or people decide to leave. Some of that target is a little harder to nail down because it's really going to be a result of when people actually decide to leave the organization because we've committed to do our changes in that methodology.

There are definitely savings. We can see it already, as I had mentioned, in our volume discount associated with the way that we do things. There are absolutely savings associated with not having multiple information technology systems that do the same thing.

MR. DAVID WILSON: I would agree with that, but what I'm hearing from you - and we heard this when we started to look into the savings that the government was saying they were going to save on amalgamation - it's really not going to happen. You're indicating it's very difficult at the end of the day to say, yes, the government is going to save $60 million a year once this transition is completed.

I appreciate you being up front and I think what I get from what you're saying is that commitment - I mean, the minister should not have made those types of commitments to say and put a dollar figure on the savings. That's the challenge and the concern I have, is that it's easy to say we're going to save $60 million, but you're saying here that yes, there will be savings, but you cannot commit today that the $60 million will be - here's the savings, here's the reduction in the budget. So that's interesting. That will be another debate I think we have with the minister, especially when we go back into the House on Thursday.

I want to go to FOIPOP and I know my colleague has talked about this. FOIPOP can be challenging at times and we just heard that my colleague's Party initiated a FOIPOP that was denied, but the media initiated a similar FOIPOP and they received the information. I thought maybe you would give it to the Opposition caucus because then they need to fight to get the media attention about it, but it just shows that it's a challenge. I understand that. You had indicated that you're potentially going to look at going to an automated process because it's very much a paper-driven process now and it takes a lot of time. Is there a timeline on when you would think that an automated process for FOIPOPs would be available, not only for political Opposition, but the general public, media, and those who are interested in information that the government has?

MS. CASCADDEN: I am so pleased to say that we actually have selected a system and we're starting to do testing and piloting. We've moved fairly quickly on this because we saw that there are huge benefits to automating this entire process - from the front, which is the requests of the FOIPOP will be done electronically, all the way through to the information gathering, for those of us who have to gather the information and submit it. All of that will be gathered electronically - so no more two copies, not stapled, all of that sort of good stuff that we have to go through. The assessment by the FOIPOP officers will be done electronically and the letters and all of the supporting documents will be forwarded to the group that is asking for the information, electronically. So it's a full end-to-end electronic system.

MR. DAVID WILSON: Do you have a timeline on when you would foresee that fully up and running, for the benefit of those who are requesting information?

MS. CASCADDEN: I would like to redirect to Glenn Bishop because he has been working on this particular one.

MR. CHAIRMAN: Mr. Bishop.

MR. BISHOP: Yes, we've been working on the process. Right now we're going to go into what we call a proof of concept that's going to take place over the next - we're estimating - three or so months. Once we understand how that looks and whether it's going to truly fulfill the needs of the FOIPOP group, then we'll move into a more complete implementation.

We don't have hard timelines on that because we want to find out what the outputs are from the proof of concept, but we suspect within six or so months we would have something in place.

MR. DAVID WILSON: I think that definitely will help the process and hopefully speed up the return of that information, or the actual denial if you're not going to get that information, so we look forward to that. Currently the way it works, when processing an application, the Freedom of Information administrator will ask the government employee to give them access to their computer. If it's automated, will that allow for maybe a possibility of server-side search for FOIPOP? We house all of the data so if you do a server-side search for FOIPOP, it could really alleviate some of the backlog. Is that part of this automated system?

MS. CASCADDEN: One of the pieces of functionality that this system does have associated with it is once a FOIPOP request has been fulfilled, we can actually post it and it's available to everyone. We have to work our way through what that looks like, actually posting FOIPOPs and a number of jurisdictions already do that. Once somebody has requested a FOIPOP it's basically available, that FOIPOP request and the information associated with it, is available to anyone else who is looking for that information. This system has the capability of doing that and . . .

MR. DAVID WILSON: So will it retrieve the information on the server side of things? The reason I ask and you can be up front, especially recent reports - now you go in and ask for access to that computer, emails can be deleted so that information wouldn't be covered, for example. If you do a server-side search, all of that information will be there, so would that not be beneficial? You still are able to look at the information and if it's sensitive then you omit it, that's really why you would look at the server side of things, that way you have all of the information in front of you, the professionals can siphon through it and say, is this information that we can give out? That's why I'm asking for server-side search so that all of the information, deleted emails, could potentially all be looked at under a request for FOIPOP for whatever information someone was looking for.

MS. CASCADDEN: At this time my understanding of the process that they're looking at is very similar to the paper-based process where you ask the individuals to supply the information to the FOIPOP officers. The FOIPOP officers actually don't go in and do a search themselves. I do not know whether this system would allow for a server-side search. I know that we are pretty much replicating the process that we have now where we engage the people who we believe have the information and get them to submit the information to the FOIPOP officer.

I know the system is capable of that. I'm not sure if it's capable of the next level but, as Glenn mentioned, that's why we take these through three months or six months with a pilot to see what are the pros and cons of doing things differently and what does that look like.

MR. DAVID WILSON: I noticed in your annual report that you mentioned there are nearly 11,000 desktops and laptops, 3,400 BlackBerrys, 2,000 cellphones and over 1.000 servers. I understand, I think I know the answer to this, but BlackBerrys for government employees are not FOIPOP-able, right? I mean, you can't get information off the BlackBerrys. Am I correct on that?

MS. CASCADDEN: So are you asking about BlackBerry Messenger and texting in particular?

MR. DAVID WILSON: And BBM and all that area. I know that there are more reports going on now about the use of BBM pins that aren't traceable and I know that there are policies in place, but the reality is people use them, government employees use them and that information is not being captured. Are you looking at potentially bringing that in? I say BlackBerrys, but I know now the government has opened up - I think there are some iPods now we can use, but they're capable of using BBM, I believe and similar things. Are you looking at potentially including handheld mobile devices in that coverage of what can be FOIPOP-able?

MS. CASCADDEN: From a technology perspective, we do not log the transactions associated with BlackBerry Messenger or with texting. That started back when the technology wasn't capable of doing that. As we look to our newer technology and the capabilities, we have to determine if people are conducting business in that method, then that business being conducted is actually a record of government and we need to keep it as a record.

It's part technology, are we capable of doing it. A number of years ago we couldn't because the way messaging was handled, most of those messages were transmitted through whatever carriers you were using and there's no record through our systems. Now as the technology has increased, there are capabilities of actually collecting those from a logging perspective.

MR. DAVID WILSON: So will that be a recommendation maybe that you'll go to the minister with? I think that's my last question.

MS. CASCADDEN: We're definitely looking at the possibility of collecting those.

MR. CHAIRMAN: Order, thank you. We will now move to the Liberal caucus and Mr. Farrell.

MR. TERRY FARRELL: I have a couple of fairly specific questions. One of them has to do with the effect of shared services and how it will trickle down to different organizations throughout the province, libraries in particular. How will the realignments that are coming about as a result of shared services affect, say, IT employees in libraries?

MS. CASCADDEN: With regard to the different employers involved in the creation of the shared services, one of the reasons we did the waved approach is that we did the government departments first because they were all government employees. From a labour perspective that was a relatively easy task of moving them from one department to the next.

As we move into the health sector, which is a different employer; Education and the school boards, different employers; the regional libraries, different employers - all those various situations are going to be assessed and managed by the Public Service Commission and the labour team with the Public Service Commission.

What we do as part of our process is we identify those IT professionals who are out there, who are supporting information systems that are now part of our purview. Once we identify those people we give all the names to the Public Service Commission and the labour team and they start looking at all the different things that have to be considered when those people will be transitioned over to become a provincial employee, because that's what's going to happen to the people who are deemed within the scope of the shared services objective. It will be handled through the Public Service Commission and the labour groups.

MR. FARRELL: I know that with getting back to the libraries again, the IT people in the libraries, particularly in my local library there's one person who also has some programming types of responsibilities. Are there equivalents within your - are there government employees that you're dealing with who are not just responsible for information management or IT support and service, but who also have programming responsibilities? I don't mean computer programming, I mean library programs that are offered to the public.

MS. CASCADDEN: One of the things we do when we start looking and talking with the other organizations - and it is a conversation but at some points it's a negotiation as well - when we initially identify the people who are doing things that we believe are IT in nature, who are coming over to our side of the house, we do a fairly extensive data gathering and we actually gather that information both from their management level as well as from the individuals themselves. What the individuals do is they submit their whole portfolio of activities.

What has happened on a number of occasions is you have people who are 40 per cent IT and 60 per cent non-IT. It could be anything, it could be a program, they might support a financial service or some other service. That's then when you start to enter the negotiations with the department about whether that person is best suited for the delivery of services because we're looking for the best across all of government and the entities, whether it's best to have that person move into a pure IT role or to leave that person with their skill set back in with their group.

Now we also recognize that if they had a certain percentage of IT, that system and that support would be coming to IT so that's when we start negotiating how much of the budget, how much of the FTE. If you happen to have two people - one 60 per cent IT and 40 per cent program and you have another person who's 40 per cent IT and 60 per cent program, you look at those two individuals together and between the department and the IT you say, one individual comes this way and one individual comes this way and we cross-train so the programming stuff stays back with the program and the IT comes with the IT.

It is a negotiation. It's not a case of reaching in and grabbing it, and having no respect for what that person was doing back in support of a program. It's a negotiation with the group because everything has to work at the end of the day, not just one side.

MR. CHAIRMAN: Ms. Lohnes-Croft.

MS. LOHNES-CROFT: I just want to get back to the DHAs. Were you finished with - you were sort of cut off the last time.

MS. CASCADDEN: The health system and the IT on the health side is very complex because there are many systems in play right now. What we are doing with the Department of Health and Wellness, as well as with the health authority and the IWK, is launching a new initiative called One Person-One Record, which is really an initiative to look at how we can have greater single system solutions in the health care sector, which really drives the sharing of information seamlessly amongst providers.

That initiative will start knocking down some of the barriers that we have in the provision of care, as well as the complexities that we have in the back end trying to support these multiple systems out there and then linking them with all of these fine chains; that takes a lot of effort. There are opportunities as a result of the health authorities coming together because they're going to streamline the way they do business, which will then help us put information systems in, which will further streamline the information flow and the way they do business.

MS. LOHNES-CROFT: That's supposed to all come at what date?

MS. CASCADDEN: We're saying the target is the Fall and I have kind of October 1st in my mind. The first step is with the health authorities and the IWK and the Department of Health and Wellness, and our responsibility as part of this merger of the health authorities plus the shared services because those are two things that are happening at the same time - our responsibility will be infrastructure. All of the client service, help desks, desktop support, provision of BlackBerrys, server, storage - all of what I consider hard core IT - as well as any corporate applications. So things like email, the SAP system will all be coming over to the ICT shared services within the provincial government.

What stays back in the health authority is the responsibility for the clinical applications. We left the clinical applications back with the health authority because it was so integral to their businesses. Also, the magnitude of the change that was going on within the health authorities to pull all of IT out of the health authority responsibility was making the health authorities really nervous that they were losing connect with what's really something very critical for them to be able to manage the health system itself.

So the split and the decision on the split, that the clinical systems would stay within the health authorities and that the shared services ICT would get the infrastructure side of the house - what that will mean is that we now have to work in a triad partnership with the Department of Health and Wellness, IT shared services, and the health authorities to manage those clinical systems. We'll have the back end, they'll have the front end, the Department of Health and Wellness will have the strategy.

The One Person-One Record initiative is being kicked off now with the Department of Health and Wellness leading that strategy, and both us and shared services and the health authority at the table to build out that strategy for a more streamlined information technology infrastructure across the health system.

MS. LOHNES-CROFT: How does that work? In South Shore Health, we have some collaborative practices that are run by the DHA. We have some that are private practices and then we have private doctors' offices. I know you're saying it's going to be regional, but how do you get everybody on board? How do you get a private physician to say, I'm going to purchase this system for my office?

MS. CASCADDEN: It's very complex and you are absolutely right. How do you get all these multiple stakeholders to the table and how do we make sure that the information is flowing to the benefit of patient care, right? It is very, very complex.

The vision for One Person-One Record is certainly to take the complexity out of it by reducing the number of information systems involved. It won't mean there will only be one system that will make up the information technology inside the health system. What we're really trying to make sure is that there is only one record. That means that those systems have to talk to each other so we reduce the complexity.

The way you get people involved and engaged in this really to have them part of the process and to make sure that you understand what their needs are out of the system. So even though you may have a physician out in the community or in a private practice, they need access to a lot of the information that's in the hospital information systems. They need the labs, they need the X-rays, and they need the visits to the specialists. That's the key to making sure the system actually works, making sure that information flows from one to the other.

When you hear One Person-One Record, don't necessarily think one information system to do that. It's really we need to create that one record and it is created by connecting fewer multiple systems than we have today.

MS. LOHNES-CROFT: Thank you very much.

MR. CHAIRMAN: Thank you, Ms. Lohnes-Croft. If there are no further questions, we will offer Ms. Cascadden an opportunity to provide some closing comments.

MS. CASCADDEN: Thank you very much for all your questions today and especially thank you for being interested in information technology and information management. We do support so many different things across government, yet we're in the back rooms and we're not very front-facing to a lot of the services that are provided. As the government moves into the digital area, we have to be at those tables where we have the conversations to really help the various government departments move forward and support the government departments.

There will be increasing dependency on information technology and information services, not decreasing. That means we do have to step up our game on the privacy side of the house, on the security side of the house, making sure that we are investing in sustainable solutions. Information technology is expensive; it's expensive to procure, it's expensive to maintain on a go forward basis so we take our role and responsibility very, very seriously. We understand our role in supporting the various government departments. We have a lot that we can bring to the table to help move the yardstick forward.

We are excited to be here, we are excited to do this and I think there are great opportunities for Nova Scotia as a result of the directions that we are all taking in order to make our services more available to the citizens of Nova Scotia, so I thank you very much.

MR. CHAIRMAN: Thank you, Ms. Cascadden and also to your colleagues for joining us today and for all your answers you provided to the committee.

We do have a couple of pieces of business on our agenda. One is the approval of the subcommittee's record of decision on our upcoming agenda items. I believe everyone has a copy of the record of decision from February 25th. Are there any comments on that matter?

Hearing none, may I ask for a vote in support of these topics? Would all those in favour of the motion please say Aye. Contrary minded, Nay.

That vote is carried and we'll move forward with that record of decision.

We also have a workshop which has been scheduled with the CCAF for May 20th. I believe everyone has or will receive some more correspondence on that as time goes on. As you recall, that was an offer they had made to us about giving us some training towards making our own recommendations to government departments. That's on May 20th.

In August - August 23rd to August 25th - we have the CCPAC conference. Myself, the vice-chairman and I believe a representative from the NDP caucus will be attending that conference. We also have an opportunity to put items on the agenda for that conference, so if there's anything that you're thinking about that you wish to add, contact myself and we'll certainly discuss that further.

There are two pieces of correspondence, one from the Department of Finance and one from the Department of Health and Wellness which I believe you've all received. If you have any questions on that please let me know. They were in response to questions asked during previous meetings with those departments.

To close, I just want to remind everyone that our next meeting will be April 1st with the Department of Community Services and the topic will be the Integrated Case Management system. We will now adjourn for a few moments before we continue with our briefing for that meeting.

Just one final item for our guests, there was a request for information that our clerk will follow up with you about and that was to obtain the budget for the team for the chief security officer. Thank you.

[The committee adjourned at 10:51 a.m.]