HANSARD

NOVA SCOTIA HOUSE OF ASSEMBLY

COMMITTEE

ON

PUBLIC ACCOUNTS

Wednesday, March 19, 2014

LEGISLATIVE CHAMBER

Chief Information Office

Printed and Published by Nova Scotia Hansard Reporting Services

Public Accounts Committee

Mr. Allan MacMaster, Chairman
Mr. Iain Rankin, Vice-Chairman
Mr. Bill Horne
Ms. Suzanne Lohnes-Croft
Mr. Brendan Maguire
Mr. Joachim Stroink
Mr. Chuck Porter
Hon. Maureen MacDonald
Hon. David Wilson

[Ms. Suzanne Lohnes-Croft was replaced by Mr. Stephen Gough]
[Mr. Brendan Maguire was replaced by Ms. Joyce Treen]
[Hon. David Wilson was replaced by Hon. Sterling Belliveau]

In Attendance:

Mrs. Darlene Henry
Legislative Committee Clerk

Mr. Gordon Hebb
Chief Legislative Counsel

Mr. Alan Horgan
Acting Auditor General

Ms. Janet White
Audit Principal

WITNESSES

Chief Information Office

Ms. Sandra Cascadden, Associate Deputy Minister
Ms. Carolyn McKenzie, Director, Client Services
Mr. Blaine Maxwell, Director, Service Management

House of Assembly
Nova Scotia

HALIFAX, WEDNESDAY, MARCH 19, 2014

STANDING COMMITTEE ON PUBLIC ACCOUNTS

9:00 A.M.

CHAIRMAN
Mr. Allan MacMaster

VICE-CHAIRMAN
Mr. Iain Rankin

MR. CHAIRMAN: Good morning. I call this meeting to order. I'd like to begin with introductions. I'd like to begin with Ms. Treen - just introduce yourself and the constituency you are from.

[The committee members introduced themselves.]

MR. CHAIRMAN: Thank you everybody. Today we have the Chief Information Office with us. We're going to be discussing controls over the disposal of IT assets. This was reported in the November 2013 Report of the Auditor General.

I would like our guests to begin with an introduction and then we'll follow up with questions.

[The witnesses introduced themselves.]

MR. CHAIRMAN: You may begin with your introduction for the day.

MS. SANDRA CASCADDEN: Thank you, Mr. Chairman. Good morning and thank you very much for the opportunity to be here today to discuss the disposal of government IT assets. With me this morning, as we've already introduced, is Blaine Maxwell, the Director of Service Management for the Chief Information Office (CIO); and Carolyn McKenzie, the Director of Client Services.

My opening comments this morning will focus on what we do at the CIO and the results we are delivering for clients and citizens. The office has the mandate to plan, organize and direct the strategic direction and leadership for information management and information technology across government. Our job is to protect information, to secure the infrastructure, to ensure that IT investments and resources are used to their full capacity in order to get the most value for taxpayers' dollars. Most simply, our job is to ensure that we are doing the right things, doing them the right way, doing them well and getting benefits.

The office was created in April 2009. I joined the office in September 2013. Our current operating budget is $31.76 million for the 2013-14 fiscal year. We also spent about $11 million this year on capital projects and improving our infrastructure. To give you a flavour of that work, one of the key capital projects for this year was the rollout of Microsoft to all government computers, at a cost of about $1 million. We also made $2 million worth of improvements to the provincial data network this year and that will continue into the next fiscal year. Finally, we invested about $2 million this year in the planning and development of a project called Signet, which will improve the government's ability to deliver on-line transactions for citizens, in a secure and private way.

The Chief Information Office plays an important role in supporting government's overall goals and priorities by setting IT strategies, policies, standards, frameworks, and solutions that support and enable the government efforts. Our vision on how we deliver on our mandate as corporate service revolves around three drivers: information, mobility, and connectivity.

Currently the office has 223 staff who work from five locations in Halifax and from a number of regional locations throughout the province to support the technology needs of thousands of government employees. The office manages about 10,900 desktops and laptops, 5,300 mobile phones and 15,000 phone lines. Those are just some of the metrics of our infrastructure.

We are currently managing over 37 IT projects at various stages, various levels of complexity for various government departments. Our service desk manages about 400 calls per day and we flow information through over 16,000 e-mail boxes. The services we provide allow citizens to do everything from renewing your vehicle permit on-line to finding out how to access the numerous services that government provides citizens and businesses. We make it possible for them to register a birth or a business, and we make it possible to get the latest provincial road report.

The services and the role the office plays have changed over the short time it has been in existence. In particular, the way we deliver our services changed substantially in the recent years as we have implemented efforts to be more client-focused and better coordinated across all of government.

We live in a world today where technology improves and changes so fast it can be a challenge to keep up. Citizens and other stakeholders have come to expect government to be open and sharing of some information. At the same time, they rely on us to be diligent and protective of other information. You seldom see staff of the Chief Information Office, but they're always behind the scenes working to meet the client demands through the support and the expansion of government-wide infrastructure systems and policies.

Within government, our clients want to be able to work on the move. They want technology that they can depend on and that will work in the office and on the road. It has to be dependable and easy to use, and it has to make their jobs easier so they in turn can deliver programs and services on which Nova Scotians have come to depend.

The office, in partnership with information technology colleagues in the other departments through government, provides corporate service designed to help government clients attain their business goals. The office will continue to focus on broad public sector collaboration, standardization, and consolidation of information in the technology environments.

In addition to the ongoing work, this year the office is focused on achieving three major outcomes: a transformed Chief Information Office with a new organization structure that is better positioned to offer corporate services that focus on the government clients; an enabled workforce supporting our workforce by leveraging mobile, social, information, and cloud technologies; and advancing tools and services to allow better accessibility, information service solutions that ensure security of the information and infrastructure at a cost-effective delivery method.

I'd like to touch briefly on today's topic of IT asset management and disposal in particular - one of the more important services we provide government-wide. The Chief Information Office is committed to supporting the Auditor General's recommendations in the 2013 report on the controls over disposal of assets. This will be achieved by adopting best practice of continual service improvement, which will standardize and provide consistency to many of the processes required to deliver asset management service to our clients.

We have prioritized all of the Auditor General's recommendations from the recent audit and we have started with the most significant actions that would have the greatest impact, and we have already completed a number of these recommendations. We have made substantial efforts creating and applying standards to ensure that data is wiped from computers before we dispose of them, and the government turns over about 25 per cent of

its total supply of desktops and laptops each year. On that point I'm pleased to note that 90 per cent of our used computers are actually transferred to the Computers for Schools program, going to students and schools across the province who can continue to make good use of these tools.

We have initiated improved tracking systems to allow us to quickly and easily determine if a computer is cleaned and ready to be transferred. We manage the service in collaboration with the corporate service units, who are the IT people in the other departments, and we work directly with them in each department. These folks are responsible for the hands-on management of each of the department technologies. It's a strong and successful working relationship and we continue to improve our supports to the CSUs through the ongoing development and the delivery of standards from the Chief Information Office, allowing increased consistency and quality in securing and managing the disposal of assets.

It's a time of great change and an opportunity for the government's information technology community. The goal is to work collaboratively to meet the challenges and ensure opportunities are realized to the benefit of Nova Scotians. I am privileged to be in this position to provide leadership and direction to achieve an important mandate of the Chief Information Office. With those comments, I thank you for your attention and I welcome your questions.

MR. CHAIRMAN: Thank you, Ms. Cascadden. We'll begin with Mr. Porter for 20 minutes.

MR. CHUCK PORTER: Thank you, Mr. Chairman. Welcome to our meeting this morning, thank you for being here. It's always an interesting topic; we've discussed this over the years, at least in my time on this committee, which I guess is now going on eight years, believe it or not, that we've had IT before us a few times. It always ends up being a fairly interesting topic for us.

I've got a number of questions; I'll probably bounce around a little bit from one thing to the other. I want to start with the Auditor General's recommendations. Can you update us where the department is right now, where your office is with regard to those recommendations?

MS. CASCADDEN: Certainly. There were a number of recommendations specifically directed to the Chief Information Office, as well as recommendations that were directed to each of the individual departments. I'll go through each one of the recommendations from the Chief Information Office.

On Recommendation 2.1, which asks - recommends actually - that we start encrypting data on computers, I'm very, very pleased to say that we've actually started our encryption program. Again, because there are a number of recommendations here, we took

the opportunity to prioritize which one of these various recommendations we'd work on. This one was prioritized very high, just from a risk perspective. What we did is we prioritized moving laptops and putting encryption on laptops first because, of course, they're a high-risk device, they move around. We have approximately 2,000 laptops that we are targeting to have encryption on. We currently have 851 of those laptops encrypted, as of yesterday, so we're moving very, very quickly to encrypt those kinds of high-risk, mobile devices. We prioritized laptops first, desktops second, based on a risk analysis. So that's where we are on Recommendation 2.1.

With regard to Recommendation 2.7, that recommendation was to update the standards for the wide area network policy, and categories of information technology and assets covered by this policy. We have created a new and updated policy. Those policies go through multiple committees within the Chief Information Office in order to garner approval. That policy went to the Standards Committee on February 24th, so that means the policy is actually written and it was tabled in front of our Standards Committee which is made up of multiple representatives from different IT groups.

That particular policy, unfortunately, wasn't approved by the Standards Committee. The Standards Committee asked for a couple of other changes and refinements to that particular policy, so the Standards Committee is doing what it is supposed to do, by looking at the policy. It will be going back to our Standards Committee, so we'll have Recommendation 2.7 covered off very shortly, as well.

Recommendation 2.8**,** in which the Chief Information Office should document the information technology disposal of assets process, there was a supplemental piece of information that was attached to the documents you received today. Inside that document it actually shows a number of new processes and procedures that we have actually documented. Those would be some of the flow charts inside that package. Again, I am very happy to say that we are moving forward with our documentation, and the supplemental information that you received today actually demonstrates the documentation that we have moved forward with.

Recommendation 2.9, "The Chief Information Office should use sanitization (secure wiping) software that records and reports on wipe processes and results." We are currently looking at a number of different tools and we have to assess those tools, based on our environment, so we have not procured a tool yet, but we are actively looking at a tool.

In order to make sure that we do document the process, we've actually put a number of manual processes in place. So we have a manual process until the time that we get a tool, which will automate the process a whole lot more.

Recommendation 2.10, "The Chief Information Office should implement a standard procedure that provides a visual identification of whether information technology assets have been wiped." Again, in your supplementary documentation there is a page that

has different coloured labels on it so when assets come in to be disposed we actually put one of those very large labels on the front of each of those assets and it will tell the status of the asset at a very quick visual inspection. We have completed Recommendation 2.10 that we do have a reference label scheme for the disposal of assets.

Recommendation 2.11, "The Chief Information Office should periodically verify that computers sent for disposal were wiped." We put together a process for which we will do our own audits of devices after they've come out of the wiping process. So we put together the process, we put together the documentation - we have developed a check list associated with those processes and we actually did our first trial run of that self-audit. We picked 21 computers that went through the whole process and we were very pleased to say all those 21 computers had been appropriately wiped.

The audit document that we are using is also part of the supplementary documentation that you received today. The documentation is actually on the last page of the documents you received today, so we have a process that is actually fully documented and forms that we are using.

Recommendation 2.12, "The Chief Information Office should develop a process to ensure all the information technology asset disposals it performs are recorded in a centralized tracking system." The IT assets are considered an asset just like a desk or a chair is considered an asset, and the Department of Transportation and Infrastructure Renewal is responsible for collecting and managing all assets, so we actually use the Department of Transportation and Infrastructure Renewal's database. So we're making some changes and they're making some upgrades to their system as well. We believe that we may need to procure another tool that will automate the front end of our process that is very specific for IT and then we will bolt it onto the database that TIR has.

With regard to Recommendation 2.13 for the Chief Information Office where the Chief Information Office should retain specific disposal details for each asset it services that it is sanitized, the dates of the disposals - basically he was looking for a more detailed report - we have implemented a manual tracking system so for all of the assets that we are disposing of, we have a manual tracking system for us in the CIO and then we manually link that to the system in TIR.

When we are looking at a tool to automate the IT side of the process, this manual process that we put in place will go away and will be a much more automated and much smoother process. So that's where we stand on each one of the recommendations.

MR. PORTER: Thank you for a very detailed answer, and that's okay though because there were a few recommendations in there that were quite important and people were wondering where they're at, including us.

You talked about 2,000 laptops being your first priority - 851 of those complete. When did you start that process and how long has it taken to get those 851 done?

MS. CASCADDEN: Well, the process actually starts well before the first device is encrypted because we have to make sure that we select an encryption technology. We know the implications of encrypting; we know which assets we can actually encrypt. Just because you have a laptop doesn't necessarily mean that that laptop can be encrypted because some of the older laptops actually cannot be encrypted, it's just the newer ones. The first devices we touched were about two and a half weeks ago and we've been able to move forward with 851.

MR. PORTER: So that's moving rather rapidly. Just picked up on a piece - some of them can't be encrypted. So of the 2,000, those 851 have the ability to be encrypted then at this point, but how many of the 2,000 do you know won't?

MS. CASCADDEN: So 2,000 of the 2,000 we know can be encrypted.

MR. PORTER: Oh, can be encrypted, thanks for that clarity.

MS. CASCADDEN: Any new computer that's purchased will have newer technology; we know those can also be encrypted.

MR. PORTER: What's our total - just of assets - with regard to desktops, laptops, et cetera, that are needing to meet this requirement overall, do you know?

MS. CASCADDEN: We would like to, and our target would be, to have encryption on 100 per cent of the devices, so that would be the 10,900 I mentioned that are on our inventory. As I mentioned before, we really need to prioritize our process because we can't kind of do everything all at the same time, so we looked at the high risk, which was laptops. We looked at those laptops which we can encrypt and moved those forward. Those ones that cannot be encrypted will be coming through a replacement cycle, so we will replace those; everything that's newly procured from April 1st onward, we will encrypt before it ever reaches the client's desk. We'll then start looking backwards in time for all of the newer assets that have been procured over the last six or eight months and we will start to encrypt those. We won't attempt to encrypt older devices because we know they're going to be recycled at a certain period of time. That's the kind of risk/benefit analysis that we do.

MR. PORTER: A lot of us carry mobile devices, as you know - what is the status with regard to those? BlackBerrys, can they be encrypted, as an example?

MS. CASCADDEN: Yes, BlackBerrys themselves are already encrypted. The other devices that we're also supporting, like iPhones, the way that we're rolling them out - you work in a very secure container and if anything happens to that device, we turn the

container off and we turn off access to that device immediately, so we have a lot of control over those mobile devices.

MR. PORTER: That's good, thank you. Like I said, it's always an interesting topic. I think about "significant departments" - I'll call them - like Justice, Community Services, and Health and Wellness, and we've heard in the past how some health records have been accessed by people who shouldn't have had access to them. That has been discussed in this very Chamber, in this very Public Accounts Committee setting in the past. Have we had any significant breaches in the last while that you're aware of? Can you talk about that a bit?

MS. CASCADDEN: From an access to information perspective, there are multiple different types of ways breaches can happen. One is that somebody leaves a device somewhere and somebody picks it up and then looks at that device. The encryption and the other methods that we're taking to secure those devices, the fact that they have to have a user name and password on them when you open them up, we can manage those devices that way.

There are other breaches that are more - people already have access to an information system and they're just going places they should not be going, based on what their access is. That's a different type of breach which we're not controlling. That's controlled by the lines of business that own those particular applications.

Some of the breaches that have been discussed before are really about people who have had access to a system but are going places and looking at information they shouldn't be looking at because they don't need to look at that information for their own job. Those we don't have any insight into because we're managing the physical assets, we're not actually managing the access associated with the system.

MR. PORTER: So you're not doing anything with regard to the actual passwords themselves, you make your recommendations with regard to it being safe or difficult, or whatever the right terminology is for having a password as secure as you can possibly make it, changing them on a regular basis and so on. But you really don't have anything past that - is that correct?

MS. CASCADDEN: That's correct. We set the standards and the policies and the best practices to say, your password has to be greater than eight characters long, numbers and capitals. We would hope that each one of the various departments that owns the information system will adhere to that.

There are certain corporate assets that we do manage directly as the CIO. That is the e-mail system, so that's where we have direct command and control over that particular asset, but an asset like a hospital information system, we don't have any - it's completely separate.

MR. PORTER: I want to get to the assets in general - a little more specific. There are many, as we know, there are multiple departments. Just as an example, does your department, your office, purchase all of the assets? The Department of Health and Wellness or the Department of Justice or the Department of Community Services or anyone, for that matter, any department or others, does that all go through one purchasing or does each department do their own thing? How does that work?

MS. CASCADDEN: I'll start with just a little bit of an explanation of what happened pre the creation of the Chief Information Office. Before the CIO was in place, each department, each entity procured all of their own assets, so they could choose which assets they wanted. When the CIO was formed and we did a whole asset inventory, there were multiple different types of assets everywhere. So over the last couple of years, we have been working diligently to create standards and we have been successful in creating a single standard around desktops and laptops, which is HP. That now makes our environment much more manageable as we do those standards.

MR. PORTER: Sorry to interrupt, but just on that, is the bulk of that now done or are we still a long way from the bulk being HP as a standard, as an example?

MS. CASCADDEN: The HP started about two years ago and what happens is it will take us four years to get to a homogenous environment just because of the length of the refresh strategy. Most government departments are actually procuring through the CIO process because we have an on-line process that makes it really easy for people to procure their computers. When they procure it through the CIO process, we actually then can manage that asset all the way from procurement through disposition.

MR. PORTER: Is that a requirement now?

MS. CASCADDEN: It is not a requirement that people actually use the CIO process. There are some entities that don't use the CIO process at this point.

MR. PORTER: Why would that be?

MS. CASCADDEN: I think this one I may pass to Carolyn because she works directly with this.

MS. CAROLYN MCKENZIE: Essentially the majority of our government departments use our processes. We do have some arm's-length organizations that receive service from the CIO. One good example would be the Auditor General, Utility and Review Board, the judiciary, which falls under the Department of Justice. They use some of our processes, but not completely - where they are arm's-length organizations, they kind of pick and choose which ones fit their business requirements. A good example would be: the Office of the Auditor General purchases Toshibas versus HP, so that would be a good

example of someone who would use the process. We support them; we kind of do some management on them, but the full cycle isn't followed under our process.

In advance as well, the Department of Community Services was following our processes, but actually doing their own procurement, and we've been working closely with them where actually our office will start to do their procurement and have worked through a transition plan. That's one good example of a government department that was retaining the procurement process on laptops and desktops, but has recently now been working closely with Blaine's team on bringing their process into ours.

MR. PORTER: Why the HP as the standard, versus something else?

MS. MCKENZIE: When we did HP that was part of a strategic procurement initiative that was led through the Treasury Board and really it was a cross-sector initiative where school boards, the Department of Health and Wellness, and government basically went through a process to say, if we increase our purchasing volume, can we get a lower price? So through a process that was led through government procurement, you know a cross-sector evaluation panel, we landed on HP as our standard. Prior to this HP contract, we would have had about 25 different models where we basically had Dell, HP, and then potentially a third contender on our standing offer for purchase.

MR. PORTER: Thanks very much.

MR. CHARMAN: Thank you. We'll now move to Ms. MacDonald and the NDP caucus.

HON. MAUREEN MACDONALD: Thank you very much. Good morning, this is very interesting and such an important topic. I think people in the province, in the community that I represent certainly are always really concerned about identity theft and privacy, confidentiality. Increasingly, so much information about ourselves is contained in all kinds of places so I don't have to tell you the heavy burden of responsibility you have in terms of protecting the public, in the public interest and individuals.

This is an area that for most laypeople - and I put myself in that category - is quite mind-boggling in terms of what would be required to protect people's privacy and confidentiality. As I listened, as I was reading the Auditor General's Report, I was thinking probably in very simplistic terms, just from my own common-sense understanding of computers and the experience I've had as an MLA, getting new IT in my office and having to dispose of the old IT, it was my understanding that a hard drive can really never be wiped and that the information continues to be on that hard drive, even if it's encrypted, and that some computer genius someplace, theoretically, could undo the encryption.

Can you explain this to us - what is encryption, what forms are you adopting and how secure actually is that in the long term?

MS. CASCADDEN: Certainly. I'll start talking about this and I'll try to keep it as non-technical as possible. I may hand it over to Carolyn as well.

First, there are different types of hard drives. For example, hard drives that are in servers and those servers would contain, I would say, highly personal information because we are conducting many different types of transactions within government. So when it comes to a server hard drive, they're actually pulled out of the servers and they're taken to a disposal site where they're cut in half or three pieces or shredded. We handle different devices differently, depending on the risk associated with those devices.

Then when it comes to personal computers, when the computer is operational and you're carrying it around, the best thing we can do is to actually encrypt that hard drive. Somebody would have to really know how to break into a hard drive and kind of decrypt it - you would need keys. Nothing is impossible but what we do is we make it as difficult as humanly possible.

There are bad guys out there all the time, looking at devious ways of doing everything and anything. What we have to do is - what can we do that's the best thing in order to protect the devices and the information on those devices?

There are also times when we get devices back and it's a laptop that hasn't been used for two or three years and the hard disk is suspect, so even if we try to turn the device on, it really doesn't turn on. Those hard drives are immediately removed and they're sliced, as well, because we actually can't take them through a process to clean them that we're comfortable with. That's a slightly different process, depending on the situation.

The other thing we do with hard drives is not only is it encrypted during its life but when it comes in from a disposal perspective, we believe that we can wipe the hard drive so it can be reused. Wiping is I'll say a bit of a physical process in that we degauss it, which is basically taking magnets - really, really strong magnets - and rolling them over the hard drives. Then what you do is write ones and zeroes over every part of the hard drive, to overwrite the data. We do that process at least three times.

With the original encryption, with the degaussing, with the overwriting of the hard drive multiple times, we're following what we believe are best industry practices so that the hard drives can be reused.

There are a number of devices that, depending on where they come from and the risk of the type of information on them, we just pull the hard drives out but for other devices we will wipe the hard drive and we will go through that very, very detailed process, based on what cyber-security folks are saying is the best process. We follow RCMP processes for wiping hard drives as well. If we believe and feel that we've done the due diligence, then these devices actually can be reused somewhere else in the system.

MS. MACDONALD: The scope of your mandate, does it extend to the district health authorities and the school boards or are you confined to government departments? Can you give me an idea of the breadth of your responsibilities?

MS. CASCADDEN: We're responsible directly for government departments. We do work in collaboration and very, very closely with the district health authorities and the school boards. For example, a lot of the health information systems reside within our government data centre and a number of the contacts that we negotiate from a volume perspective involve both Education and Early Childhood Development and Health and Wellness. In fact, in some instances involves Dalhousie and HRM, from a whole volume buying perspective. So our direct scope of control is really from a provincial government perspective but we actually open up to engage others and invite them in, hopefully to the benefit of their clients as well.

MS. MACDONALD: Thank you. A few years ago I remember either at this committee or during the Budget Estimates, there was a report that floored me. It talked about the number of laptops that went missing on an annual basis and it was pretty high. I'm wondering how many laptops have gone missing, let's say in the prior 12 months, and how is that dealt with? What is the process used, first of all, to try to prevent the disappearance of laptops and then, if a laptop goes missing, what procedure is in place to look at what information was on that laptop, the risk and the security implications?

MS. CASCADDEN: I'll just start with responding to this question and then I'll hand it over to Carolyn McKenzie for some other details. Laptops are highly mobile and that's good, and laptops are highly mobile and that can be a detriment to having a laptop.

Certainly one of the first things we do is encourage people to not leave their laptops in cars because lots of times laptops are left in cars, cars are broken into because it's a nice, shiny device and it can garner enough money on the market. So first we do an education.

We also have the ability to physically secure the asset to a desk. Even in an office situation, depending on how open your office is, there could be the risk of somebody walking in the door who is uninvited, just kind of walking by a desk and scooping up a laptop. So we actually have - and all laptops have it - the ability to have a cable and a lock put on the laptop, which is a combination lock so it's kind of like a bicycle lock that you undo and you can take it away. So there are multiple different things we can do to secure the physical asset and we do encourage and supply those types of things to our clients. With regard to the numbers and the process, I'll let Carolyn McKenzie take that.

MS. MCKENZIE: Essentially it's not a high volume that come in and report directly to us as the Chief Information Office. In the last 12 months I'm aware of two situations that have been directly reported to our office. The process really is - if a laptop is stolen, we treat it almost as a potential privacy breach so the process that's documented is it needs to be - and our service desk would inform a client, you need to talk to your privacy

person and report it; you need to inventory what potential data may have been on that laptop. Then there's the process that's really from a privacy perspective that's launched within each department.

From my perspective, we haven't really seen a high volume, but whether or not they come in and report or just deal with it as a breach and then purchase a new laptop. So depending on the scenario and how educated the person is, the process may be different, but there are two that I'm aware of in the last year.

MS. MACDONALD: In other words you're saying it's not a requirement right now that if I were an assessor for home care - I think that's out in the district now - but when it was in the Department of Health and Wellness, if that laptop went missing there wasn't a requirement that it be reported to you?

MS. MCKENZIE: There's a requirement to be reported to Privacy, but we don't have a current process in place to report to CIO.

MS. MACDONALD: So you would have no way of knowing?

MS. MCKENZIE: Running a report to give you information at this point.

MS. MACDONALD: Is that something that you might address in the future? It seems to me that it would go very well with the standardization that you're attempting to get.

MS. MCKENZIE: We're working on an IT asset management policy, as well, so through that there are considerations about various scenarios that would happen. Through that process I would expect that we would be able to address that because a requirement would be to have the life cycle of the device managed through a system so if it was lost, if it was reallocated to a different person, some of the tracking of the asset is made throughout the life cycle. In the future, through continuous improvement, I would expect that we would have that addressed.

MS. MACDONALD: One of the things that strikes me as being really important is securing the data that MLAs have in their constituency offices. I'm being fairly self-interested here in some ways, but it's the work I know best and many constituents come to us and they bring all kinds of personal information and we are in communication with government departments and agencies.

Often we have a lot of very sensitive information in our databases, yet I'm not very sure, I guess, that we have the support or the training, the direction, to help us secure that information. It's something that my colleagues and I are always very aware of and very concerned about - the trust that's placed in us by our constituents and the confidentiality that they require, but the limited capacity, I suppose, in some ways we have to deliver that

to them in kind of a technical way. We personally can do the best we can to ensure that we're not sharing documents inappropriately or whatever.

I'm wondering about the relationship of your office to the MLA offices and whether or not this is something you've considered as part of your mandate. I particularly wonder about that since you've indicated that the Auditor General's Office, for example, is arm's length - I suppose we'd be a little arm's length as well - and have capacity to act independently. It's still highly problematic, from my perspective.

MS. CASCADDEN: An interesting opportunity and a learning experience presented itself in the October time frame with the change of government, when we were trying to deploy different technologies and connect different people differently. It was an incredible learning opportunity for me because it was the first time I went through this process as the CIO. Many people actually reached out to us and asked us questions about how can we do this, how can we get everything from wireless connectivity through to sharing files, what types of devices can we use, what types of devices can't we use?

My answer to the question - I would say that we probably haven't had the focus for these offices that we can, should and are willing to have. So if these offices are interested in learning more about the technology and about what we can supply them to secure information and/or even just to enable seamless movement of information, we are more than willing to work with people. We've actually had a number of those conversations already but they have been one-on-one conversations.

MS. MACDONALD: Mr. Chairman, how much time do I have?

MR. CHAIRMAN: You have approximately four minutes left.

MS. MACDONALD: Good, thank you. I actually have one very specific kind of irritant to raise with you in a very polite way. It's about my old BlackBerry number; I had it from the time I was elected but I took it with me when we were in government and when I no longer was in government and returned my BlackBerry, I also lost that number, which is fine. However, that phone and that number is still active and people are still calling a number that I had from the time I was first elected in 1998, so it's almost 16 years. They still get my voice message but I no longer have that phone or that number because it was turned in.

In checking with some of my other colleagues, they have indeed had the same experience; I think Mr. Corbett, for example, is in the same boat. Somewhere out there today in cyberspace there is this phone number still active, still with my voice message that was on it two years ago, getting messages that I can't get. I have no idea, unless somebody runs into me and is irate because I haven't returned their call. What can we do to fix that? How is it possible that that occurred?

MS. CASCADDEN: We try to manage all those assets and when we're given those assets and we're asked to turn them off, we have a process that we take them through. When we're engaged in that process early and in the right place, then we have a higher success rate of actually getting things turned off. If others are engaged in that process and don't pull us in, we actually don't know what should be turned off and what shouldn't be turned off. I would say it's a process issue between the other people who are engaged in it and then us, who at the very tail end are actually managing the process.

Certainly in your very specific instance we will look into it. In fact, what we'll do is we'll look into all of the transition phones over the next couple of weeks and deal with this issue specifically.

MS. MACDONALD: Thanks. It seems - oh, my time is up.

MR. CHAIRMAN: Order. I'm sorry I have to call order, but you can continue in the next round.

I will now move to the Liberal caucus and Mr. Rowe is beginning.

MR. ALLAN ROWE: Thanks very much for your presentation this morning. I just have a couple of questions, actually, and most of them are primarily for clarification. In speaking about the phones, I'm curious about the passwords on the smartphones and when it became mandatory that there would be a password on the smartphone. That's my first question.

MS. CASCADDEN: I'll talk about the smartphones and the passwords and the why, and maybe Carolyn can answer exactly when - I'll take a stab at when too. From a device perspective, if it's a BlackBerry that you're using, the passwords go on at the very front of the BlackBerry because what we've done is we then have granted you access to the e-mail system and to the calendaring system for which, after you put the BlackBerry password in, you don't have to put a password in for that. So we have to have one password somewhere and the password for the BlackBerry, based on how we manage the BlackBerry system, is at the very top level, which is access to the entire BlackBerry.

My understanding would be we put passwords on BlackBerrys almost from day one, but I'll get clarification. It's a little different when we're dealing with the iPhone application; iPhones have a password for the iPhone itself, which you can turn on or you can turn off. The way we're delivering services on an iPhone is we actually have a secure container. It looks like an app for your iPhone. That secure container requires a password and then you get into the e-mail system. You're getting into e-mail at a different level when you're using an iPhone. You could actually take off your password for your full iPhone so if somebody picked it up they could see all your pictures and they could see all your apps, but as soon as they saw the government container there, if they clicked on that, we put a

password on that to protect the information contained within your e-mail, your calendar and the e-mail system. So different devices we actually manage differently.

On the iPhone, if you wanted a password for your iPhone you'd have password number one for the full phone, and then password number two would be for your container. For the BlackBerry, it's password for the BlackBerry, and we open up the e-mail after that BlackBerry password.

MR. ROWE: Perhaps I misunderstood then. Has that always been the case - that was my question - like five years ago, for example, eight years ago? I guess my concern is, are there potentially phones out there that are not password protected? Maybe that's a simpler way of putting the question.

MS. CASCADDEN: I would like to hand this over to Blaine.

MR. BLAINE MAXWELL: No, actually - now, when you say phones, we have to be careful because there are non-smartphones as well, but the smartphones that would contain data, which would be the BlackBerrys, no, they've always had the passwords on them. Actually, it has been enhanced, the password, so now you will notice it times out a little quicker and things like that. In fact, those who would have had the old BlackBerrys would notice that, I should say. No, that security has always been on there and, in fact, the BlackBerrys, if you lose them, they'll be wiped automatically.

In fact, the advantage of a BlackBerry over a laptop is the fact that because they're on the network, because they are that type of device, they can be wiped immediately, as soon as they're reported lost.

MR. ROWE: Can I go back to wiping hard drives? I think, if I recall, in the AG's Report there were some indications of the software that's used to actually wipe the hard drive and there were some deficiencies there that the software was really not geared for business use. Has that been addressed, and if so, how? Could you shed a little bit more light on that, please?

MS. CASCADDEN: The software that we are using is a smaller type of application but it does do the job. It was actually sanctioned by the RCMP a number of years ago so it meets a certain CEA standard - don't ask me what those numbers are. So it does meet those standards that the RCMP had at the time.

Because we have been prioritizing all the other activities we actually have not procured a corporate level application yet but we are looking at the various types of applications that are out there that we could procure and we could bring into the government. That would be our system solution.

What we have to do when we are looking at procuring a piece of software like this, we have to say exactly what we want this software to do, so not only would we want it to wipe the devices, we would also want it to record its success rate of wiping. We would want it to be able to record the serial number of the machine from that hard drive. We want it to record the date it did the wipe, we would want to record the person who did the wipe and the verification.

The software we're looking for is not just a wiping software; we'd actually like it to have a front-end process to collect information so that we actually have it in an inventory and have records to prove that we wiped the hard drive. Then all of that information we'd like to connect it to the Archibus system, which is the TIR asset management system, so that when that device is wiped it actually goes into the asset system and says that this asset has been disposed of and this asset was wiped on this date by this person, so carrying that information across.

It takes a while to put together all of those functional requirements of what we're looking for in an application. That's what we're doing now and we're looking in the market to see what the best application is for us, so we are looking at replacing what we have.

MR. ROWE: One more, Mr. Chairman? Thanks very much. My last question may be a little more difficult to answer. I'm trying to look to the future - like many of my colleagues I am hardly an expert. I do not envy your job at all and what you have to do so it's out of my field. What we do hear all the time is that what you own today is already out of date and what you're about to buy next week is probably out of date as well.

My concern is, how proactive are we being about looking to these issues down the road, as the technology changes, as the people who are out there who are looking to be a little nefarious in their activities, their activities are also changing, they're becoming more educated and so on. How proactive are we in looking at new methods of controlling our equipment?

MS. CASCADDEN: We are being as proactive as we can, and I'll give you some examples of how we're doing that. One thing we're doing is we subscribe to cybersecurity forums and we have communications with cybersecurity experts from a pan-Canadian perspective. We look to understand the trends in the industry: should we be focusing on anti-virus software or is it malware that we should be focusing on, from a securing of our asset perspective?

We're watching the industry, we're watching the trends, and we're getting that information from the experts, including CSIS and other organizations. That gives us a sense of kind of what we should be focusing on in the future.

The other thing we're doing is we also really understand industry trends of what's called BYOD, which is "bring your own device". Instead of having your own personal

cellphone and getting a government cellphone and then you have your own personal iPad and getting a government iPad and getting a government desktop, there's a huge trend in the industry to bring your own device. We have to look at what that means for our ability to manage your device, as you're using it to conduct our business. That's the future stuff we're looking at and we're taking all of that into consideration now.

The way we actually set up the iPhones takes into consideration the fact that you would, based on how we've configured those devices today, actually bring your own device and we could put that container on your device. We are very actively looking at where the industry is going and trying to get out ahead of it. It's really tough because it's moving really quickly but we are taking all those types of things into consideration, to the best of our ability.

MR. ROWE: Excellent, thank you very much. Thank you, Mr. Chairman.

MR. CHAIRMAN: Do we have any other questions from the Liberal caucus? Ms. Treen.

MS. JOYCE TREEN: Sorry, I have a cold, I don't hear very well today - I'm clogged. I just have a couple of questions. In the report it indicated that the inventory asset list was lacking, on Page 3. I'm just wondering, is there a plan put in place for stronger inventory tracking process? Is there something being put in place for that?

MS. CASCADDEN: I will start with a response and then hand it over to Blaine Maxwell. When each government department was doing their own individual procurements, the asset being tracked starting from procurement was probably a bit hit and miss. As the CIO formed, and as we started putting standards and processes together, as more and more government departments have been utilizing our processes to procure assets - and we know when those assets are coming in the door - we actually can update that database and that database is much more robust and accurate than it was in the past. That's the high level explanation of that so I will hand it over to Blaine for the details.

MR. MAXWELL: Actually Sandra started that off very well. Basically when a PC or laptop or actually a Blackberry is first brought into the government - going forward from about a year and a half ago, we actually record every single device. So the tracking of that, because we now have mostly a central control - and I say mostly because actually from a departmental perspective there is still the Department of Community Services who will be bringing in their procurement over to our group effective April 1st and at that point we will have all the government departments proper - we will track all that inventory and assets as they come in.

That goes out to departments and that is still a little bit of the weakness that we have. When a department gets it, if they decide to move it to somebody else's desk or unplug it or somebody actually steals it from there - unless they notify us, we don't always

have information on that. When the refresh takes place and that device is replaced, that is another opportunity for us to dispose of it and sort of tie the two records together.

One of the things that we have most recently looked into and I think we're going to pursue - there is a tool that is being used, it's actually out of Vancouver - called Computrace which goes right on the BIOS. I don't want to get too technical about it, but it goes right at the lowest level so people can't turn it off, that's the important part. That will actually track your device down to a geographical region. As long as that device is connected to the network - the Internet or our network, which is basically all devices nowadays - they can actually track it right down to where it is, whether it gets stolen, whether it gets moved, and we'll have that information all on-line so we won't be relying on the departments necessarily to tell us where that information is. We'll be able to do that automatically.

That will be a big step forward because that tool is actually being used by - it's something to be quite proud of on a Canadian front as it's the only company in the world that does this. They've actually made deals with all of the major manufacturers of PCs, so this is incorporated into their PCs. They're also working with handhelds such as your Samsung, iPhones, et cetera. They're actually putting it on those devices. They are actually looking forward to the mobility issues that may happen.

It's actually a relatively cost-effective solution and it's being used by large organizations such as the Los Angeles School Board - I think they have 600,000 PCs - and they also have a recovery. You can actually buy an additional service where if it gets stolen, they'll actually recover it. In fact, in some of the larger cities in the U.S., this is the only tool they will recognize if you go to the police force - do you have this on there? If you do, they'll pursue it; if you don't, they won't pursue it. That tool is actually very powerful and it's something we're looking at. I just wanted to make sure that we mentioned that as well.

MS. TREEN: Very interesting - it can track our phones and computers - I like that. The other question is unrelated to that - when you read the Auditor General's Report, was there anything that surprised you regarding the disposal in the past, for computers? Was there anything surprising in that report?

MS. CASCADDEN: I don't think there was anything surprising in the report. We always look to the Auditor General's Report as tools we can use in order to better what we do. When I looked at this report, that's what it actually pointed out: so you do have a piece of software, but you should have a stronger one; you look after assets, but maybe you should tighten up that process; departments do their own thing, maybe you and the department should work together a little bit more to tighten up that whole process.

They hold up the mirror and really help you look at what you're doing and you say, okay, we need to enhance what we've been doing. I actually welcome this report and it

does help us move the yardstick forward when reports like this are public. Then it helps us get support in other areas.

MR. CHAIRMAN: Thank you, Ms. Treen. Mr. Gough.

MR. STEPHEN GOUGH: I'm just wondering if there are measures in place to prevent hacking of the government devices, either at home or if someone is travelling abroad?

MS. CASCADDEN: From a hacking perspective - it's a tough one. When you think of your computer being hacked or the government system potentially being hacked, what it means is you actually have to be attached to the Internet for that to happen. So if you're sitting at home and your computer is not attached to the Internet and you're not doing any Internet activity, then the probability of you being hacked is slim to nil.

If you happen to have a little wireless device at home and you don't put a password on it and you don't have protections on your own home PC, anybody driving by in a car can stop in front of your house, climb on your wireless network and they are with you and your entire family.

From a government perspective, when people who have a government asset are in their homes or abroad, and they are connecting to the networks, the way they connect to the networks is through our own VPN tunnel - it's things like that that actually mitigate the risk when you're out there.

The bigger risk from a hack perspective is the outside world to the whole government network, because they're not really looking at individual computers. When it's an individual computer, it's really more about a virus coming on from the Internet, which really isn't a hack, it's a virus issue or malware. Some malware would be a hack, and how that would come in is if your computer does not have the most up-to-date profiles on it, from the anti-virus software perspective. So if some of you have your home computers it will say that you need to update your anti-virus now and you click "Yes", it puts down a whole bunch of new signatures so that when you're on the Internet and somebody tries to do something bad to your machine, your machine says, oh, that name is a bad file name, I'm not letting that in.

One of the things we do is we make sure those signature files are up to date on every one of the government machines. So there are some mornings you come in and you see the little blue wheel rolling a little bit and your system is saying, don't shut off your system, we're doing updates, or an update is coming through and you have to push "Yes", those signature files are getting updated at that point.

With those signature files being updated, the personal computer is protected. When we look at the whole government network and we think of the government network as an

enclosed circle and the rest of the world outside that circle, the way we connect to the rest of the world is through that Internet connection.

There are a number of things that are between us in the circle and them in the outside world which actually block bad things from coming in. Those things are firewalls, so we have a major firewall for the government. We also have part of processes which would be standard security processes. We know where the bad guys are, we know what countries they're coming from. We know the IP addresses, we block those IP addresses, so we know a lot of that activity and, again, we work with other cybersecurity people so that if you know there are things coming in from Asia or South Africa, we all have those blocked, but all of a sudden if something pops up from the Ukraine, that information is shared amongst the cybersecurity community and then we put IP addresses on our own firewalls.

We also have opportunities to work with our Internet provider, so not only do we block it, the Internet provider that connects us to the world also has a level of blocking at that Internet provider. So there are multiple different filters here, both from a whole government perspective and from your own individual PC perspective.

MR. CHAIRMAN: Order, please. I don't like to interrupt you because it's interesting to hear what you have to say, but we'll move back to the PC caucus now for 12 minutes of questioning.

MR. PORTER: I want to talk a bit about the disposal piece of things in the few minutes I have. We've heard a bit about the hard drives and whether they're wipeable or not, and you've explained to some degree that they are. This committee always takes the stance of looking back at what costs are associated with doing things and so on. Has it ever been costed out because obviously there's a cost with doing this procedure of wiping and somebody spending time on that or you have a specialist that does that, or two or three or whatever it might be?

Has a cost analysis ever been done to compare the cost of just replacing the hard drive and throwing it away, smashing it, whatever you would do with it as opposed to wiping them? When you disposed of the asset, if someone went to surplus and picked it up, the deal would be you would put your own hard drive in it, but here's the box and everything else - have we done that?

MS. CASCADDEN: I will hand this over to Blaine because he has all of the detail around the hard drive disposal.

MR. MAXWELL: Yes, actually we have looked at that, in fact, especially the cost of the drive. The other factor that probably is expensive is the labour that's involved in removing a drive. When you do a wipe, it's actually much less labour intensive. That's why we actually prefer the wipe method if it will get rid of the data.

One of the things that I don't think was mentioned is the RCMP actually has done forensic studies on these drives afterwards, and the recovery rate of the data is basically impossible to get the data so we are very confident in the wipe. The problem with our wipe is it just doesn't have reporting tools, so just to go back to that, that's a little bit of the reason why the Auditor General picked up on that. What we now do is we actually manually record those, and that has actually added to our labour costs obviously, so we have found that we've probably increased a half an FTE, basically, based on some of these. So we know we've increased our costs, but we also realize that's very important.

To take out a drive, for example, you're talking a significant amount plus the cost of the drive, and because 90 per cent of these go to Computers for Schools, there is a value that they get out of them as well. It would actually almost be double exercise - it would be us taking them out, taking the labour, and then actually them putting another one in. The cost of the drives is coming down and that actually has been considered.

MR. PORTER: What's the turnover, what's the age of a computer when you're turning it over and replacing it?

MR. MAXWELL: Basically it's what we call a four- or five-year cycle. After four years we start looking at it for refreshment, and depending on where we are at that time, we won't let them go any longer than five years.

MR. PORTER: What does "refreshment" mean?

MR. MAXWELL: Refreshment is basically the point where we determine that the machine should be replaced, so we maintain that and inventory the age. In fact, with our new inventory, keeping track of all the devices, we'll know exactly when the devices are coming due.

In fact, it's one of the areas - when we talked about going with IMP and HP, they actually - IMP is the vendor that sells this locally, they actually work very closely with us on that process and that has been an improved process. At one time you probably heard of a lot of PCs getting purchased at the end of the year as budgets were - people wanted to make sure they got their budgets. We now have that so we don't have that big - because for us it wasn't the budget issue; it was the fact that we had 2,000 PCs coming in within the last three months of the year and trying to roll those out. What we now do is we forecast that out throughout the year and that is actually how that would all be managed.

MR. PORTER: I see. So you're on the four or five year and things wouldn't go any longer than that.

MR. MAXWELL: That's correct.

MR. PORTER: Okay, a little bit about the hard drive question I had, obviously you're fairly confident that the wiping is working well. It has had some audit done on it by professional people. Generally speaking, the average person couldn't get anything off it. Maybe the expert couldn't get anything off it, I don't know, somebody who is really tech savvy couldn't get anything off it. So there obviously is a low risk; knowing a lot of them go to the school or something, it's highly unlikely that anything would happen there anyway, you're obviously quite confident in that.

MR. MAXWELL: That's correct, yes.

MR. PORTER: In my office, just as an example, for the last three years - I think we're in year three - in an effort to get rid of paper, if you will, although it was once upon a time thought that was going to happen with the world of technology but I believe it has increased, we actually built a database for constituency business. If somebody calls my office it's recorded electronically versus a paper file. We haven't done that - I think we're in year three now of doing that.

I back those up on an external hard drive, obviously, for obvious reasons and so on. I replaced a computer that was quite a few years old just recently, through your process. I haven't disposed of that yet, it's in the process. How should that be wiped? I mean obviously there's a fair bit of significant information on there which I'm not even allowed to pass on to the member down the road who will replace me. As it stands, due to confidentiality and so on, should that go through a certain procedure through your department or should that be . . .

MR. MAXWELL: It absolutely should because we do this regularly so we have all the processes and policies in place to do this. We would gladly take that on, in fact - again, when you get into the arm's length it has been a little bit less clear but I would encourage that. In fact, I was glad to hear you say you're backing it up because actually now, all of a sudden, you have to consider that backup drive as well.

One of the things that hasn't been mentioned is we actually discourage people from storing things on their hard drives. Everything really should be stored on a server so that's actually part of an education process as well. So if you took the actual proper use of a computer, really the only private information would basically be e-mails and it would be stored on the corporate system. Yes, we would willingly take that on, but absolutely, that should be destroyed.

MR. PORTER: I agree and we're moving to that, as well, sort of everything going to the backup or the external hard drive, whatever you want to call it, versus hanging around on the main desktop or something.

That being said, I don't know if you can buy anything anymore that's not 50 gig or 100 gig or whatever they come in now. I mean I don't know what people do with all this

space. I guess if you're recording or you're doing something, maybe there's obviously a use - you know, somebody a lot more tech-savvy than myself. I mean it's just in excess now, an Excel database, it doesn't take up a lot of space so they're very easily moved about and backed up and so on. I'm very curious about that. I couldn't get my local IT folks who have done work for me in the past - I've got a local company down there, too, that does work. Would they be of that level or again, I just want to stress this because I'm in the process now of getting rid of that - you would recommend through you?

MR. MAXWELL: I would recommend through us because I know our processes. Local companies probably would have various standards. I would hope they would recognize the importance and what to do. At the very least you could ask for any certifications they may have or what their processes are and whether they're certified. But I'd highly recommend it coming through us. If you wish, you can call me directly or we can get in touch with you and provide you with a contact.

MR. PORTER: That's great, I appreciate that very much. Mr. Chairman, those are my questions, thanks.

MR. CHAIRMAN: Thank you, Mr. Porter. We can now move to the NDP caucus and Ms. MacDonald.

MS. MACDONALD: Thank you very much, Mr. Chairman. I want to go back to the computers that you know of that have gone missing and just ask a bit more about that. I'm wondering if those computers were encrypted or not and what departments those computers were from.

MS. CASCADDEN: On this one I'd like to hand it over to Carolyn.

MS. MCKENZIE: They were not encrypted, as we just recently started the encryption process on March 4th of this year. The two departments that had reported them, one was from TIR and one was from Community Services. They both followed the process of reporting through their privacy group to do an assessment of risk. At that point they would have assessed within their department. We wouldn't have had an outcome of that assessment of risk, but I do know that the Department of Community Services, for example, does have a departmental policy not to store local data on their hard drive due to the nature of their data, so it would be deemed - without knowing the details of the device that was stolen.

MS. MACDONALD: I want to ask you about the recommendations from the AG. At the outset you said you had prioritized them and you gave us kind of an update of what you intend to do and where you're at in the process, but I didn't actually catch the priority in which you've ordered the recommendations. I wonder if you could give us some clarity around that. I know you did indicate that the first priority was encryption, starting with the

mobile devices, but can you just tell us the priority in which you've ordered them and then how long will it be before they're fully implemented?

MS. CASCADDEN: From a priority perspective, there are priorities and then sub-priorities, and we can actually work on multiple things at different times because different groups are responsible for these. The ones that we have worked on that I commented on today, those ones were put in kind of the priority-one bucket. So instead of saying, this is priority one, two and three, I'll put them in a bucket.

The ones that were left to a little bit later because it's going to take longer to do them is the procurement of the software, for example, because we have to go through a longer process. What we did is we assessed the risk associated with not having that software. Well, we actually have software that wipes and that software wipes well. It isn't a fully automated process, we have to put manual processes around that. Are we willing to do that at this time? Yes, we are because what has a higher priority is the encryption and we need to put those same resources that would be having those conversations about the software, we actually need to put them on the encryption project.

When I was going through each one of these - we've actually tackled each one because different groups can do it, so it's more of a prioritization bucketing because even inside the encryption, we prioritize laptops, not desktops. It's kind of a roundabout way of answering your question, but it's really not Recommendation 2.1 was number one, Recommendation 2.8 was number two. We looked across all of these to see which parts of those that we could move the yardstick forward on.

MS. MACDONALD: What is the objective for the goal in terms of time frame to implement the recommendations?

MS. CASCADDEN: With these different types of recommendations, some of them are relatively easy to say, check, we've done. We have purchased a piece of software, okay, we can check that off, but does that actually address the recommendation of completing the documentation, tying it into the TIR application? So the procurement of the software - even though it takes a while to get it, from a functional perspective - we could procure it, but we still, from an Auditor General's perspective, haven't fulfilled the whole intent of the recommendation until it's a completely automated process and tied into Archibus. That could take two years.

Some of these could take two years, others, for example, even though we put a priority on encryption, it actually will take a four-year cycle to complete because first we're doing laptops that are capable of being encrypted, then we're doing everything that is purchased from April 1st on a go-forward basis. If our computers are being updated every four years and into the fifth year, we will have completely gone through a cycle of new computers in four years, so it will be that four-year/five-year mark before we can say all the computers are encrypted.

Some of them are longer term. So the Auditor General may say, well, great, you started encryption, but until every single asset is encrypted, you're not finished this one. So it all depends on what parameters we put on "done" or "complete". It could be up to four years, if you look at one of the longest cycles here.

MS. MACDONALD: It's hard to envision what the world could be like as well - that world in four years. I'm wondering, do you provide verification to the client that the asset has been securely disposed of so the departments or whatever the client groups are - do you provide any written reassurance to them that their asset has been adequately dealt with?

MS. CASCADDEN: That was one of the recommendations in the Auditor General's Report: that we actually communicate back to the departments, so as we're building our process, we're building that communications plan back to them. Up to this point, I would say we don't have a robust process communicating back to the departments. The robust process is more about: we're in replacing your old asset, how do you get your old asset to us?

We've strengthened the process of our own internal processes; now we have to look externally to say, are we educating each one of the leads in the various departments about what their role and responsibility is in asset management because they have a role in this? Do we communicate back with them that the asset has been disposed of and what direction we took on the disposal of that asset, at what time? Those are areas where we have to strengthen our processes and they're being looked at.

MR. CHAIRMAN: Thank you, Ms. MacDonald. We'll move on to the Liberal caucus. Mr. Irving, please go ahead.

MR. KEITH IRVING: Thank you, Ms. Cascadden and colleagues, for all the work you've done on this. This is clearly extremely important and it appears you've made significant progress. I guess my first question is, through the work that you've done so far and then also looking forward, have there been - I think you mentioned a half FTE, but are there other staff or budget implications that have come out of this Auditor General's Report up to this point and in terms of additional resources going forward to complete the recommendations?

MS. CASCADDEN: Certainly when we start to look at procuring anything new from a financial perspective that will be a plus from a budget perspective. At this point, until we have actually decided the functionality of the new secure wiping software and what we're looking for, we don't have a cost associated with that yet from just a straight procurement perspective.

Certainly as we increase the robustness of our processes and we really look at doing appropriate tagging and tracking and documentation, we are concerned that the staff that

we have in this particular area will not be enough staff to actually do it to the level of due diligence which we believe, with the Auditor General, we need to do. So there are absolutely some implications to kind of stepping up our game. There's no doubt about it, both from a hard perspective that we're going to have to procure some additional tools. We can't tell you right now what those costs will be because we're just scoping out what our requirements are, but we are concerned about the number of staff that we have in this particular area and the added workload that we'll be putting on the staff because we have stepped up in our processes.

MR. IRVING: There have been some good questions here that have been insightful, but there seems to be for me still a question about responsibility. We seem to be transitioning to a more rigorous system, but you've used language such as "departments do their own thing" and "we offer our services". There remains for me a question in terms of the ABCs and their independence, yet we are building this knowledge and policy development around a more secure, more rigorous system. Whose ultimate responsibility does this issue lie with? I'm sensing that you are trying to nurture departments and ABCs. Is that the way it is and should be or do you have some suggestions in terms of policy changes?

MS. CASCADDEN: Certainly the model we have from a CIO, or Chief Information Office, perspective right now - and I'll say that because as of April 1st it's going to be slightly different with the new Internal Services Department which we are now part of - the model that was put in place when the CIO came to be in 2009, looked at all the different government departments that all had their own individual IT shops and they were all doing things differently; like I mentioned before, they were doing procurement differently, they had different standards.

When it was pulled together into the CIO, the parts taken out of the various departments were the hard stuff. If anyone was looking after a server they came over to the CIO; if anyone was doing help desk activity they came over to the CIO; if anyone was doing desktop support they came over to the CIO. That structure stopped short of other IT people who support applications that are very, very specific for that department. So there is an IT structure that still remains in each one of the government departments which gives them the latitude to do things either completely aligned with us, partially aligned with us, or not aligned with us at all.

That structure is much more of a federated model, so the Chief Information Office is not the one and only entity that has some role and responsibility and accountability for IT in the government at this point. So it is a federated model that each of the departments have autonomy to do certain activities themselves.

What we have had to do, coming together as the CIO, is we have had to demonstrate to them that we can deliver a good service to them, that we can deliver a service in a timely manner, that they can trust us in the delivery of that service, so come and

be partners with us. We do not have that dictatorial - for lack of a better word - relationship, it's much more of a collaborative relationship and it's a relationship building.

Different groups, depending on what they are and it's kind of different for each group, it's different from a government department than it would be for an agency, board or commission or for a district health authority or a regional school board. We have to work with each one of these entities, depending on what type of entity they are, respecting what their mandate is.

It is complex - if you're feeling it is complex, it is complex.

MR. IRVING: So at this time, no particular policy changes or suggestions would make your job easier, I guess?

MS. CASCADDEN: I believe there are opportunities to broach this subject with the advent of the Internal Services Department.

MR. IRVING: Okay, thank you.

MR. CHAIRMAN: Thank you, Mr. Irving. Mr. Stroink.

MR. JOACHIM STROINK: Thank you very much for coming out today. I have just one question. The question kind of relates to the chart in the report on Page 11 on application controls. Is the attempt being made to ensure things like passwords, lock screens, automatic expiry, are being implemented across all departments or is that possible?

MS. CASCADDEN: I don't have that specific one although I'll take a look at that. Certainly from our perspective, any system that is a corporate system which we manage, those types of securities are put in place on all the systems because we program them that way. If you try to put in a password that's too short it says "Try again" and it keeps saying "Try again".

Specifically this one was about, I think, the inventory management software that was in use at various entities. It kind of goes back to - the Department of Transportation and Infrastructure Renewal has the responsibility within government to manage all assets. It is their mandate to have this database to manage all assets, so all assets are in this database - chairs, desks, computers - and that is the application that the Auditor General commented on here with regard to how robust that application is.

When the Auditor General made the comments on the Archibus application - you probably saw it mentioned a couple of times - when the Auditor General did their look at this application it was at a certain revision or version number. The Department of

Transportation and Infrastructure Renewal is upgrading that application that will take care of most of the X's in the column for that application.

Both the Department of Community Services and the Department of Justice have their own inventory systems for which they were keeping their own individual inventories outside of the TIR system, but both of these groups are coming on board with the TIR system. This is one of the benefits of having an Auditor General Report that points this out and then just by having conversations with both the Department of Justice and the Department of Community Services people see the logic and the opportunity to climb on board one asset management system for government.

MR. STROINK: Thank you, that's all I had.

MR. CHAIRMAN: Mr. Gough.

MR. GOUGH: Thank you for your answer to the last question; I know we ran out of time. I have one other question here. I'm just wondering if you could tell us about the average number of computers that get disposed of on an annual basis. What happens to these computers?

MS. CASCADDEN: When you think of the fact that we have - I'll just round it up - approximately 10,000 computers; I just rounded down because we actually have 10,900, but just for the math. We recycle computers every four years, so one-quarter of those computers get recycled, so one-quarter of 10,000 - 2,500 computers - actually get recycled on an annual basis. Those are the ones that we have to document, track and everything through the process.

Out of that number, actually 90 per cent of those computers go to Computers for Schools-Nova Scotia. We are actually highly successful in the redeployment of computers to schools and places other than schools, but very similar to schools is through the Computers for Schools-Nova Scotia program, which means that they can be reused again.

The computers themselves - what happens is inside government we may buy a new application and it may require much more horsepower on that computer than that computer can provide. So as soon as we buy that application, the computers that use it have to be upgraded. It doesn't necessarily mean that that computer is bad because if those computers are too old, automatically what we do is we take out the hard drives, destroy the hard drives and we take out any other pieces that we may want in our own supply to fix other computers. Then it goes to the ACES recycling; those older computers are recycled.

We have a standard for which we will not go below when giving those computers to Computers for Schools-Nova Scotia because we actually don't want to transfer the cost of maintenance to those folks if those computers are really old.

MR. CHAIRMAN: If there are no other questions, we will give you an opportunity, Ms. Cascadden and your office, to provide some closing comments.

MS. CASCADDEN: I hope that what we have been able to communicate with you is that we too are serious about managing this process, managing the assets on behalf of our clients inside government, and that we've actually taken this audit report very seriously. We've managed to move forward on many of these recommendations in a fairly significant way when you consider that this report was actually released in November 2013.

We've actually made very good in-roads and it's kudos to the folks I have on both the left and right of me and their teams. I sincerely hope we've been able to communicate that we are moving the yardstick forward and we do truly believe this is an important thing for which we have a role and responsibility and accountability and authority to do. Thank you.

MR. CHAIRMAN: Thank you, Ms. Cascadden. With that, we do have some committee business. We do have a briefing coming up at 11:00 a.m. and that will be on Occupational Health and Safety. Before we get to that, I would like to remind members of the committee that we have meetings upcoming, including on March 26th, we have a meeting, of course, with the Department of Labour and Advanced Education.

After that we have a subcommittee meeting and we will be discussing subjects to come up at future dates for this committee and also to discuss some outstanding issues, including one on pension valuation adjustment and to discuss another recommendation put forth by the Liberal caucus with regard to the proposals of the Auditor General; specifically, we would like the Auditor General's Office to explore the idea of ranking recommendations, from the most important which should be done immediately, to items that can wait a little longer to a later date. That's something we'll discuss in our subcommittee meeting at that time.

We have also a meeting on April 2nd with the Department of Health and Wellness. That is actually going to be moved to April 9th. We won't be having a meeting on April 2nd, but we will be moving that topic ahead one week.

With that, I'd like to take a short recess and make sure everybody is back for the in camera briefing coming up at 11:00 a.m. We might even be able to get it on the way a little bit earlier, if we can. I will come and collect you if we have our presenters ready. Thank you.

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