Second Session - Fortieth Legislature

of the

Legislative Assembly of Manitoba

Standing Committee
on
Public Accounts

Chairperson
Mr. Reg Helwer
Constituency of Brandon West

Vol. LXV No. 5 - 7 p.m., Thursday, August 8, 2013

ISSN 0713-9462

MANITOBA LEGISLATIVE ASSEMBLY
Fortieth Legislature

Member	Constituency	Political Affiliation
ALLAN, Nancy, Hon.	St. Vital	NDP
ALLUM, James	Fort Garry-Riverview	NDP
ALTEMEYER, Rob	Wolseley	NDP
ASHTON, Steve, Hon.	Thompson	NDP
BJORNSON, Peter, Hon.	Gimli	NDP
BLADY, Sharon	Kirkfield Park	NDP
BRAUN, Erna	Rossmere	NDP
BRIESE, Stuart	Agassiz	PC
CALDWELL, Drew	Brandon East	NDP
CHIEF, Kevin, Hon.	Point Douglas	NDP
CHOMIAK, Dave, Hon.	Kildonan	NDP
CROTHERS, Deanne	St. James	NDP
CULLEN, Cliff	Spruce Woods	PC
DEWAR, Gregory	Selkirk	NDP
DRIEDGER, Myrna	Charleswood	PC
EICHLER, Ralph	Lakeside	PC
EWASKO, Wayne	Lac du Bonnet	PC
FRIESEN, Cameron	Morden-Winkler	PC
GAUDREAU, Dave	St. Norbert	NDP
GERRARD, Jon, Hon.	River Heights	Liberal
GOERTZEN, Kelvin	Steinbach	PC
GRAYDON, Cliff	Emerson	PC
HELWER, Reg	Brandon West	PC
HOWARD, Jennifer, Hon.	Fort Rouge	NDP
IRVIN-ROSS, Kerri, Hon.	Fort Richmond	NDP
JHA, Bidhu	Radisson	NDP
KOSTYSHYN, Ron, Hon.	Swan River	NDP
LEMIEUX, Ron, Hon.	Dawson Trail	NDP
MACKINTOSH, Gord, Hon.	St. Johns	NDP
MAGUIRE, Larry	Arthur-Virden	PC
MALOWAY, Jim	Elmwood	NDP
MARCELINO, Flor, Hon.	Logan	NDP
MARCELINO, Ted	Tyndall Park	NDP
MELNICK, Christine, Hon.	Riel	NDP
MITCHELSON, Bonnie	River East	PC
NEVAKSHONOFF, Tom	Interlake	NDP
OSWALD, Theresa, Hon.	Seine River	NDP
PALLISTER, Brian	Fort Whyte	PC
PEDERSEN, Blaine	Midland	PC
PETTERSEN, Clarence	Flin Flon	NDP
REID, Daryl, Hon.	Transcona	NDP
ROBINSON, Eric, Hon.	Kewatinook	NDP
RONDEAU, Jim, Hon.	Assiniboia	NDP
ROWAT, Leanne	Riding Mountain	PC
SARAN, Mohinder	The Maples	NDP
SCHULER, Ron	St. Paul	PC
SELBY, Erin, Hon.	Southdale	NDP
SELINGER, Greg, Hon.	St. Boniface	NDP
SMOOK, Dennis	La Verendrye	PC
STEFANSON, Heather	Tuxedo	PC
STRUTHERS, Stan, Hon.	Dauphin	NDP
SWAN, Andrew, Hon.	Minto	NDP
WHITEHEAD, Frank	The Pas	NDP
WIEBE, Matt	Concordia	NDP
WIGHT, Melanie	Burrows	NDP
WISHART, Ian	Portage la Prairie	PC
Vacant	Morris	

LEGISLATIVE ASSEMBLY OF MANITOBA

THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

Thursday, August 8, 2013

TIME – 7 p.m.

LOCATION – Winnipeg, Manitoba

CHAIRPERSON – Mr. Reg Helwer (Brandon West)

VICE-CHAIRPERSON – Mr. Gregory Dewar (Selkirk)

ATTENDANCE – 11   QUORUM – 6

Members of the Committee present:

Hon. Messrs. Gerrard, Struthers

Mr. Allum, Ms. Braun, Messrs. Cullen, Dewar, Mrs. Driedger, Messrs. Gaudreau, Helwer, Jha, Pedersen

Substitutions:

Mr. Gaudreau for Mr. Whitehead

APPEARING:

Mrs. Leanne Rowat, MLA for Riding Mountain

Ms. Carol Bellringer, Auditor General
Mr. Doug Harold, Audit Principal, Office of the Auditor General
Mr. Fraser McLean, Audit Principal, Office of the Auditor General

WITNESSES:

Hon. David Chomiak, Minister of Innovation, Energy and Mines
Mr. Grant Doak, Deputy Minister of Innovation, Energy and Mines
Hon. Stan Struthers, Minister of Finance
Mr. John Clarkson, Deputy Minister of Finance

MATTERS UNDER CONSIDERATION:

Auditor General's Report–Follow-Up of Previously Issued Recommendations, dated January 2012

Auditor General's Report–Follow-Up of Previously Issued Recommendations, dated January 2013

Section 9–Public Sector Compensation Disclosure Reporting

Auditor General's Report–Annual Report to the Legislature, dated January 2013

Chapter 2–Citizen Concerns–"Part 1–Business Transformation and Technology (BTT)"

Chapter 3–Information Technology (IT) Security Management

Chapter 8–Senior Management Expense Policies

* * *

Mr. Chairperson: Good evening. Will the Standing Committee on Public Accounts please come to order.

This meeting has been called to consider the following reports: Auditor General's Report–Follow-Up of Previously Issued Recommendations–dated January 2012; Auditor General's Report–Follow-Up of Previously Issued Recommendations–dated January 2013, Section 9–Public Sector Compensation Disclosure Reporting; Auditor General's Report–Annual Report to the Legislature–dated January 2013, Chapter 2–Citizen Concerns–"Part 1–Business Transformation and Technology (BTT)", Chapter 3–Information Technology (IT) Security Management, Chapter 8–Senior Management Expense Policies.

Are there any suggestions from the committee on how long we should sit this evening?

Mr. Blaine Pedersen (Midland): I would suggest we sit 'til 9 p.m., and then review if there's more time required or we run out of questions before then.

Mr. Chairperson: Is the will of the committee? *[Agreed]*

Are there any suggestions as to the order in which we should consider these reports?

I have the suggestion that we first consider the items for Innovation, Energy and Mines, followed by Finance. And, therefore, the committee agree to proceed by considering Chapter 2 and Chapter 3, followed by Chapter 8 of the 2013 Annual Report to the Legislature and Section 9 of the 2013 follow-up, keeping the 2012 follow-up report as the last item? *[Agreed]*

Okay. So we–all right. Would the minister for energy and mines bring–come forward and bring his staff and introduce them, please.

Welcome.

Hon. Dave Chomiak (Minister of Innovation, Energy and Mines): It's nice to be here again. I'm with–here with the deputy minister, Grant Doak, and the head of our IT section, Gisela Rempel.

Mr. Chairperson: Okay. Thank you.

Does the Auditor General wish to make an opening statement?

***** (19:10)

Ms. Carol Bellringer (Auditor General): I'll start by introducing my staff that are here tonight. Fraser McLean and Doug Harold are sitting behind me, and they worked on the audit of the–of security management. And I see a few staff members hiding at the back there. Ryan Riddell is going to wave. He works on our citizen concern area. And Tyson Shtykalo, who's going–he's here for the second part, for the finance reports, and is responsible for our financial statement audit team. And Maria Capozzi, who helps us all with getting ready for the Public Accounts Committee, and did a–is in from vacation today, I'm reminded. She was happy to join us.

So I'll do the summary on the two–for the two BTT reports only. So for the citizen concern area, issues are brought to our attention throughout the year by concerned members of the public, the Legislature or government employees. Our act does not include a complaint mechanism and we're not obliged to follow up these issues. However, we've chosen to do so. When the issue falls within our mandate and there's enough information to proceed, we initiate limited scope audits.

In the case of the Business Transformation and Technology branch of the Department of Innovation, Energy and Mines, we are provided with information suggesting favouritism and inappropriate tendering practices. We reviewed a sample of 10 human resource files, found that the files contained appropriate documentation to support the hiring and promotions of the respective employees.

We did note an unusual circumstance involving an individual who was hired and promoted two times within a one year period, with all promotions made through the direct appointment process with no competition being held. The file did contain appropriate documentation and approvals. However, such a rapid progression by an individual through the organization could reasonably cause a perception of favouritism by others in the organization.

We also selected the files of four vendors that were awarded contracts between 2008 and 2011. Three contracts were appropriately tendered and 15 were untendered. Treasury Board approval was appropriately obtained for all of these contracts. Only eight were recorded on the public registry of untendered contracts. And that registry is an important mechanism that supports public transparency in the vendor selection process, and it's a requirement for all government departments to record all untendered contracts in excess of $1,000 on the registry.

So that's–that was it on that chap–that part of the chapter 2. And the–we'll also, I'm assuming, go into chapter 3?

Mr. Chairperson: I think we'll deal with chapter 2 first because it's a separate item, and then we'll come into chapter 3.

So, chapter 2, the citizen concerns, part 1 of the business transformation and technology, BTT.

Does the deputy minister wish to make an opening statement?

Mr. Grant Doak (Deputy Minister of Innovation, Energy and Mines): No opening statement except to say thank you for inviting me tonight. I hope I can answer the questions that you have and I look forward to the discussion.

Mr. Chairperson: Thank you, Mr. Doak.

All right. The floor is open for questions. But the–before we get there, I would like to remind members that questions of administrative nature are placed to the deputy minister and that policy questions will not be entertained and are better left for another forum. However, if there is a question that borders on policy and the minister would like to answer that question or the deputy minister wants to defer it to the minister to respond to, that is something we would consider.

So the floor is now open for questions.

Mr. Cliff Cullen (Spruce Woods): Welcome tonight.

The auditor, in her report on this particular chapter, made four specific recommendations. Chapter–or pardon me, page 54 of the report. I just wondered if you could take us through those four recommendations and outline where the department is at in terms of those four specific recommendations.

Mr. Chairperson: I'm sorry, Mr. Cullen, I–

Floor Comment: I'm sorry, but I believe that that deals with other issues. And related to this section, there were no recommendations.

Mr. Cullen: Okay. And the auditor mentioned the untendered contracts. Could you outline your current policy for untendered contracts?

Mr. Doak: There's a standard procedure for untendered contracts. All untendered contracts must be approved by the deputy or by the minister or by Treasury Board, and there's certain thresholds for them.

Typically, particularly in the ICT information and communication technology environment, untendered contracts are awarded when there's a sole supplier. So, for example, if proprietary software is created for a specific application like tracking road maintenance, there's only one supplier who can maintain the system so a sole-source contract will be awarded to them.

Those contracts, as the Auditor General noted, are to be reported on a public registry. We've gone back through all of our untendered contracts to ensure that they're all registered, and we have processes in place now to make sure that in the future none are missed.

Mr. Cullen: So, in terms of the policy, then, is that a written policy the department has?

Mr. Doak: It's a written policy that government has.

Mr. Cullen: Could you–can you outline, then, the–you talked about the various parameters that were in place. Is there a dollar specific figures in regard to that policy?

Mr. Doak: Thank you. There are specific dollar limitations. Deputy ministers can sign to a certain level, and it depends on the type of contract as well. For a services contract, where someone is providing consultant services, the limits are lower than, say, procurement of other types of services. I don't have the specific limits, but we can take that under advisement, if you'd like to know.

And, then, as I mentioned, there are specific approval processes in place which require the deputy, the minister or treasury board to approve untendered contracts.

Mr. Cullen: So this policy, then, you said it's a government policy. Is this policy pertain to all departments across government?

Mr. Doak: Yes, it does.

Mr. Cullen: The auditor referenced untendered contracts over a thousand dollars had to be listed. What's the policy that you have in terms of making sure that all of those untendered contracts are listed?

Mr. Doak: We have procedures in place to ensure that all untendered contracts are reported. They're monitored centrally by our finance and administration department. ADMs and executive directors are responsible for ensuring that they're reported through administration and finance and then to the central registry. As I mentioned, we also went back through all of our untendered contracts in recent years to make sure that they were all in the registry, and they all are now. And we put in additional due diligence to make sure that none were overlooked as they were, that the Auditor General pointed out in her report.

Mr. Cullen: Would the deputy have any idea how many untendered contracts you would have over a thousand dollars on a given year?

Mr. Doak: I can certainly take that under advisement. I would say it's not a rare occurrence, particularly in ICT where we have many sole-source contracts with vendors who created the software, have the rights to the software and, therefore, the only ones who can maintain it. I would say it's, you know, more than a handful and probably in the dozens of range.

Mr. Cullen: So, in terms of public access to those untendered contracts, where does the public go to find that list?

Mr. Doak: I can only speculate, but I understand there's a public registry that's available for people to look at. Maybe others know more specifically.

Mr. Cullen: I'd like to ask the auditor that question, too, if the auditor could share that information with us?

Ms. Bellringer: So I'm pretty sure it's just down the hall, in the library; and I'm looking–yes, I'm seeing lots of nods from my staff at the back.

Mrs. Myrna Driedger (Charleswood): Can the deputy indicate of the contracts that have been untendered, what are the general amounts of those contracts? Are some of them like multi-million-dollar contracts, or is there a cap on, you know, how much you can spend on an untendered contract?

Mr. Doak: There are caps that a deputy can approve and a minister can approve and then treasury board approval is required. Generally, the contracts are not worth millions of dollars because there's economic risk associated with untendered contracts of that size. They're often 10, 20, 30 thousand. For the most part, I would speculate to say they're under a hundred thousand usually. It would be rare that they'd be hundreds of thousands of dollars simply because of the economic risk associated with–on such an untendered contract.

***** (19:20)

Mrs. Driedger: Can the deputy indicate what percentage of employees are hired or promoted without competitions being held?

Mr. Doak: Can I just ask clarification. Are you asking specifically to Innovation, Energy and Mines or the Province as an entity?

Mrs. Driedger: Well, if you're able to specifically indicate for the Province that would be certainly what I would be most interested in.

Mr. Doak: If I could take that under advisement, we can seek to find an answer.

Many of the competitions–and I've been in government 31 years–are through a competitive process. There are occasions when we promote people internally, as per the civil service guidelines.

And I can certainly get that information on behalf of this.

Mrs. Driedger: So the deputy has indicated that there are specific guidelines. Are those guidelines a document that is public so that the public would know when, you know, when the government has chosen to bypass the competitive process?

Mr. Doak: Thank you. There are specific, written guidelines that are available through the Civil Service Commission which stem from the act and then devolve into regulation and policy as well, and I believe all of that information is publicly available on the Civil Service Commission website.

Mrs. Leanne Rowat (Riding Mountain): I'm wondering if the Auditor General would–could share with us does she have any of the records with regard to percentage of employees that are hired or promoted without competition being held?

Ms. Bellringer: No, we didn't do an audit of it across the board.

You know, and I'll, I'll just throw this out as a bit of a caution. It's not that easy to figure–like, for the public to know when it has occurred, that information is not made available.

Mrs. Driedger: I do have a question. I'm not sure if the deputy minister would have an answer to it, but we certainly know of a number of occasions where political staff that have worked for a government–for the government over any number of years end up being then employed within the civil service.

Does the deputy have any indication as to how many of those get jobs by direct appointment or how many of them get jobs through competition?

Mr. Doak: No, I'm sorry, I do not have that information.

Mr. James Allum (Fort Garry-Riverview): I just wonder if I could ask the auditor about their approach to citizen concerns in general. Your report suggests that–or says–our act does not include a complaint mechanism and we are not obliged to follow up on these issues, however, we choose to do so.

So–but many of these things that are outlined in this chapter–not all, some of the tendering issues seems inappropriate–but many of these items in this chapter suggest to me that they're not value-for-money exercises but they're an unfairness issue instead.

Wouldn't it be appropriate for your office to refer all citizen complaints to the Ombudsman to decide which is a value-for-money issue and which is an unfairness issue?

Ms. Bellringer: Quite often the issues that come to us are more appropriately followed up by the Ombudsman and we do suggest to citizens coming to us that that's where they should go.

There are occasions when they say they don't want to go there. And so we take that into account and say it still may be an issue we think that should be followed up and we might, in that case, do it ourselves.

They–it tends to be, you know, I wouldn't actually make the distinction between this and a value-for-money audit, but rather it is a much more limited review. And so it is only looking at the negative because it, you know, having said that, if we find that there is nothing wrong we report the positive, but we're not doing it in an extensive way.

So it doesn't give you a full picture of exactly what's going on within an area and it shouldn't be used to suggest that it is any way reflective of the overall management of an area or anything like that. But, rather, how else is someone going to get an answer to their question if they feel frustrated with the system, for example.

So we do them, but we are really emphasizing the fact that they're very limited in nature, they're very narrow and they are very specific to what's brought to us, and we rarely go beyond that. But, having said that, we bring a little bit of context around it so we didn't look at one human resource file; we looked at 10. We looked at the process around the recording of the untendered contracts in this situation as opposed to just one. So a little bit bigger, but it really can't be looked at in the same way as a large-performance audit where we're looking at a number of aspects to reach a conclusion. We're just checking for evidence against one particular thing.

Mrs. Driedger: A question for the auditor. In the report it indicated that you found one contract on the registry that was not provided to you when you asked for it. Can the Auditor General tell us what that contract might have been about, why it was not given when requested and if the auditor's office ever did get a copy?

Ms. Bellringer: My recollection–and I'll just get confirmation from the staff who worked on that is it appeared to be purely an oversight that the list given to us just omitted it. *[interjection]* And my staff just confirmed, yes, it did appear to be an oversight and it was around $50,000, and it–we don't have all of the information about it with us.

Mr. Cullen: Follow up with that–I don't know if you've done any follow-up with the department in terms of, you know, their process now in place. Some of these untendered won't be missed. Have you gone through and reviewed their existing process now since your report?

Ms. Bellringer: No, we haven't on this one. It would–it'll fall into a regular follow-up process, but we didn't have any recommendations so we probably wouldn't be looking at this one specifically. We did decide to do a much larger audit across government on the waiving of competitive bids, and so we felt that it was more important that there be a strong process right across the board. We weren't particularly concerned with this department once it was drawn to their attention. We believe that they have indeed updated the information on the system but it does concern me to get a little bit more information about how well the system's running right across government.

Mr. Cullen: That leads to my next question. In terms of the government policy on tendered contracts, have you had a chance to look at that in depth and are you satisfied with the existing policy or have you made recommendations to revise that policy?

Ms. Bellringer: That audit's still in progress. It's getting nearing completion so it'll be out within–with the next 2014 report. So I don't have any overall recommendations to make quite yet. I have looked at it and we looked at it when we were also doing the eHealth audit, and some of the procurement that we had seen there, you know, I will make a general comment that when you have policies that have some general application that require a lot of subjective ways of applying it, you're going to get an application that varies across government. So the more precise it can be, the better, and I would say it has–it's a fairly general-type policy that would permit quite a few things to be not tendered.

Hon. Jon Gerrard (River Heights): You know, first of all, to the Auditor General. What in the 18 contracts that you looked at–15 which were not tendered, three which were–what was the range of the size of the contracts?

Ms. Bellringer: The smallest contract was $13,000 and the largest was $500,000.

Mr. Gerrard: Can you tell us what the largest untendered contract was?

Ms. Bellringer: Two hundred thousand.

***** (19:30)

Mr. Gerrard: My question–one of the problems that I have seen in the years that I've been an MLA is that they have people in government who say, well, there's no one else who can provide it, and then I end up with people in my office who say, well, we could've done it; they just never tendered it.

How do you know that there isn't somebody out there if you don't tender a contract of $200,000, for example?

Mr. Doak: That's a fair question. I have heard that criticism as well.

When we look to renew or to enter into a contract with a supplier, we look carefully to see, in the market, is there someone else who could effectively provide this service, and if that's the case, we will go to market because it's in our interest to do that. In the case where it's proprietary software, where someone's developed it from the ground up and they've maintained it for years, it's more likely that we'll do that.

Often people will say that they can do it, but I think when you look with an unbiased eye, it's often the case they simply don't have the expertise. It may be more costly. They don't have the right to maintain the software, and that's why we would award a sole-source contract.

Mr. Gerrard: I mean, it–what concerns me is that 80 per cent of these contracts were untendered, or roughly, and that seems like a pretty high proportion. And it seems to me that, particularly when you're dealing with, you know, $200,000 contracts that, in fact, you should be tendering it as a general rule. I mean, even if your initial perception is that there may not necessarily be somebody out there who can do this because–I mean, I've had complaints in other areas which are non-IT, but I've certainly had people complain in the IT area that they've been inappropriately excluded.

Mr. Doak: Thank you for that comment and question.

What I would say is we do carefully look at the situation. I see most of the untendered contracts and I ask the same questions that you're asking, and I'm assured that due diligence is applied to make sure that this tender–that this contract is most effectively awarded as a sole supplier. But, certainly, we'll take those comments back to the department and ensure that we have the proper processes in place.

If there are ever any specific concerns that the member has, we're happy to look at the situation and provide advice and assistance on it.

Mr. Gerrard: I just–thank you. The problem is that most of the time when somebody comes to me, it's after the contract has been awarded and they're upset. And so it would seem to me that it would be sensible, when you've got large contracts, to be proactive and tender them, and I'd just pass that on.

Mr. Chairperson: Any further questions on this section? Seeing none, we will then move on to Chapter 3, Information Technology (IT) Security Management.

Does the deputy minister–well, does the Auditor General, sorry, wish to make an opening statement?

Ms. Bellringer: Our objective with this audit was to determine whether BTT designed and implemented adequate IT security management practices and controls.

We concluded that BTT needs to significantly improve its IT security management practices and controls to properly secure information. The lack of IT security risk assessments, IT security plans and a data classification system means that the rationale for the design and implementation of IT security practices and controls is not well-supported. As such, we cannot comment on the completeness, relevance and effectiveness of the practices in place to secure systems in network operations.

Our audit criteria was based on the control objectives for information technology, better known as COBIT, developed by the Information Systems Audit and Control Association, better known as ISACA, and the IT Governance Institute, as well as standards developed by the International Organization for Standardization and the International Electrotechnical Commission.

Our report summarized our findings against these extensive, generally accepted standards. Many of the findings are long-standing problems going back eight years and persist despite repeated recommendations to remedy the situation.

Mr. Chairperson: Thank you.

Does the deputy minister wish to make an opening statement?

Mr. Doak: The Auditor General's findings relate to the responsibility under Innovation, Energy and Mines as well as the Department of Finance, Treasury Board Secretariat and the Civil Service Commission.

IEM, Finance and Treasury Board Secretariat and the Civil Service Commission have accepted all of the Auditor General's recommendations and are currently focusing efforts to make progress in implementing measures to improve our security further.

We recognize that ICT security touches all aspects of the organization, and the world is increasingly connected through technology, thereby exposing information assets to a wide range of threats as reflected in the OAG report.

As a result, Manitoba is not alone in needing to constantly monitor the environment and improve ICT security. This is an ongoing challenge with new threats emerging regularly, and as indicated by the OAG, this requires both a lot of time, resources and money to successfully prevent such attacks.

Manitoba has invested significantly in ICT security and a number of initiatives are already under way and will address many of the main recommendations.

In addition, an independent third-party expert has been engaged to conduct an information security risk assessment associated with the OAG recommendations, and to develop a roadmap which will expand on the work currently under way and prioritize activities to ensure the most crucial issues are dealt with first.

With the protections currently in place, Manitoba's fortunately not had a serious breach to our systems that has resulted in compromised data. However, we must continue to be 'viligent'–vigilant.

Thank you.

Mr. Chairperson: Thank you, Mr. Deputy.

Are there any questions?

Mrs. Rowat: The comment made at the end of your presentation here, indicated that there's no breaches that have occurred within the computer system–security management system. How do you know that for sure?

Mr. Doak: We have fairly advanced monitoring systems that indicate when servers have been compromised or the systems have been accessed, and those have happened. The proper alerts have occurred. And we often will shut down a server or shut down applications, do a full investigation, usually the servers are completely wiped and reloaded. And we know if data has been accessed and we know if data has been removed. And my understanding is that–but we have had intrusions into the system, data itself hasn't been compromised or downloaded.

Mrs. Rowat: Compromised or downloaded. From the discussions we had earlier today with regard to a trend that individuals may keep it or use it, outside of the examples you used, the concern I have is with regard to the child registry–Child Abuse Registry. I have some serious concerns with breaches in that regard.

Have there been any indication that there have been breaches to the Child Abuse Registry, and have you had to follow the process as you've just outlined a few minutes ago?

Mr. Doak: My understanding is that there's been no breach of the Child and Family Services Child Abuse Registry system.

Mrs. Rowat: Another area of concern would be the witness protection program? Could you indicate to me if there's been any breaches or concerns raised with regard to trying to access information through that program?

Mr. Doak: My understanding is that there's been no such breach of that data where someone from the outside has been able to access it inappropriately.

Mrs. Rowat: You've indicated no outside breach. Can you indicate to me if there have been breaches within the inside of government with regard to–

Mr. Doak: Not that I'm aware of, no.

Mrs. Rowat: I'm just wanting you to clarify, why would you then indicate that, inside and not outside? What would be the reason for that?

Mr. Doak: The reason I indicated that, is our ICT is responsible for protecting the system from outside users. So for–departments are responsible for maintaining the system and ensuring that people have access. So it's just really the distinction that, you know, we're trying to protect it from the outside world. It's not to say that there aren't protections in place to protect the system inside as well.

***** (19:40)

Mrs. Rowat: Thank you for that.

I'd like to ask the Auditor General, she'd identified the two areas that I have just asked about as areas of concern, and witness protection program is obviously something that we would be very concerned that there would have been information shared, and we know how that would have been used. And it would definitely put not only an individual at risk, it would put a family at risk or–and also with the Child Abuse Registry, we're very concerned with that aspect as well and if there were concerns raised.

Could you just share with us what you've found and whether you're comfortable with the outcomes of how they're planning to address that type of issue?

Ms. Bellringer: I'll share a couple of general comments and then I'll ask my staff if they'd like to add something to it. While we did note that there were some processes in place that were going to detect such things as the deputy minister described, you actually have to basically go through the whole report and see. In total, we still saw some gaps in the system; that does mean that there are risks. And there are–the risks are because of the number of items that we've brought forward; they're significant. So we would not agree that you can be absolutely sure that there have been no breaches.

Mr. Chairperson: Ms. Bellringer, could you introduce who we have at the table now, please?

Ms. Bellringer: Yes, this is Doug Harold, who's one of our IT specialists that works within our office–

Mr. Chairperson: Thank you.

Ms. Bellringer: –and who conducted most of the audit.

Mr. Chairperson: Thank you.

Mr. Doug Harold (Audit Principal, Office of the Auditor General): I call your attention to 7.3.3 in the report. In 7.3.3 in the report, normally a network is set up with a variety of different levels of security. But what concerned us greatly was the fact that there is a high-security zone within the provincial setup. And, really, only Vital Statistics and a few financial servers were placed in that high-security zone. And those controls are thought to be higher security, obviously. And so the concern for us was, given that the Province is handling other sensitive data, our request was basically to look at the rest of the sensitive data that we know that is out there and to–perhaps it should be placed in a higher security zone.

Mrs. Rowat: Was there any indication or was there any push back with regard to the areas that are identified on page 100 under 7.3.3?

Ms. Bellringer: No. No, there wasn't.

Mrs. Rowat: And was there some assurance that they would be moving those areas that are identified here as high risk or high 'sensitivid'–highly sensitive information pieces will be put forward into sensitive area?

Ms. Bellringer: We don't know what's been done since the report was issued.

Mrs. Rowat: With regard to Child and Family Services, and today we had a really interesting day with regard to questions with regard to security of files, electronically or paper. And I'm just wanting to know if you can give us some insight into how Child and Family Services have been progressing with regard to, you know, information gathering in–and how well they are moving forward with making sure that documents are entered properly and that the–that everybody is–everybody's files that are connected with Child and Family Services are being taken care of in the proper manner.

Ms. Bellringer: I'm assuming this question is quite outside of this audit in the–well, and I'm not to suggest I won't answer it, but just the–I'm not looking at it just from a security perspective. We haven't done a recent audit of the actual information technology systems at Child and Family Services. We have been, obviously, through a number of reports, been watching a lot of change going on there, including whether or not there's been a new system, which at the time of the most recent follow-up audit was not the case. We had noted over the last few audits that we did in that area that there have been significant improvements in the way that data's being collected and entered into the system. But we haven't done a full audit to determine just how well that's being done.

Mr. Dave Gaudreau (St. Norbert): Yes, I wanted to ask, in terms of the risk assessment team and all the contractors they use, how do you make sure that they have adequate security? Like, do you do checks on them? Like, when they're looking at the data for all the databases that we have, do we know that they're a secure team?

Mr. Doak: Thank you for that question. That actually was subject to an Auditor General recommendation that we do a better job on ensuring that there is appropriate processes in place for third party contractors.

We've recently renewed several contracts, including our desktop or workplace technology agreement, and built more stringent security requirements and checks in that agreement.

Mr. Chairperson: Mr. Doak, I have a question for you, following up on Mrs. Rowat's question on the internal security. Obviously hard drives are getting smaller and more–harder to see. There's lots of high capacity thumb drives, zip drives–that type of thing. How do you ensure that internal information is not accessed and exported by foot?

Mr. Doak: Excellent question–and technology is evolving every day and there's risks as a result. Often the data you have is in the cloud; often some server may be in Toronto or elsewhere. And so we have procedures in place and policies in place with regard with mobile media–so the sticks that people use or the removal of laptops or tablets from the office.

We've done some outreach and training, and the Auditor General indicates that we need to do more, and we'll do that with employees. We really have to build a culture of security. The data that we have–and members have mentioned it–is the most sensitive data that the public can have–the Child Abuse Registry, for example, or Child and Family Services data–and it's our duty to protect that. We do have processes in place to help protect it.

As technology evolves, we need to involve–evolve as well, and we need to train employees to make sure that the people on the front line with this data take seriously, protections measures that need to be in place.

Mr. Chairperson: Thank you for that, Mr. Doak. And further to that then, a culture of security that you need to build, obviously, the Auditor General addressed that in great detail. And are you comfortable that you are there now, or is this a work-in-progress? And, obviously, there's no end to it, but where will you be at the point where you will be comfortable enough to say that you do have that culture of security?

Mr. Doak: I think that we have a very professional civil service. I've been in civil service for 30 years now, and I've spent a great deal of time in Family Services and I've found people to be quite cognizant of the data that they're–that they take care of–the paper files and then evolving into electronic files.

I would say, no, we're not there yet, and we'll never be there. As technology advances, we need to advance. We have to do that through proper policy and proper systems. Most importantly, it's really proper training, because it's–you can have all the systems, all the procedures in place, but unless you have that culture and appropriate training and so that it's not just additional work for people to do but they understand that our credibility really hinges on the protection of individuals' privacy. And once that trust–if that trust is ever breached, it's very difficult to get back.

Fortunately, as I've said, we have not had a significant breach of data, and we're going to ensure that we don't. We accept the Auditor General's recommendations which indicate that we have more to do, and I commit to the committee that we're going to do that work.

Mr. Gaudreau: Yes, I mean, it's the technology, like you were saying, it moves fast. What's the–like, what's the answer? What's the hardest thing for your department to keep up with that? I mean, as we've seen, like he was talking about jump drives and phones now and all of that stuff. What's the answer to keeping up with that?

Mr. Doak: It's a combination of things. It's having a good information protection section within our branch. It's making sure that we're aware of trends in Canada, around the world. It's making sure that we have, as I said, the proper practices in place.

And I think it is really important to emphasize to people that, you know, this is serious business of when we deal with people's data. They give us the most intimate information and their expectation, it's correct, that they–that it be protected.

There's huge evolution. Like, how many people in this room have a smart phone? It has more power than all the computers in the 1960s combined, and every day there's something new. Well, there's–you may know as near field communication where you simply hold your phone up to another one and it transfers data. And so we have to make sure that we understand what that technology is, that we have policies in place and practices in place, and, as I said, most importantly, people understand that their duty is to protect individuals' privacy and data. And it's in their own best interests because we can't do our jobs unless we have the trust of the public.

***** (19:50)

Mrs. Rowat: With regard to security awareness programs that you were talking about in ensuring that staff are trained with regard to live training workshops, the report indicates that there were only 6,000 employees since 2006 that had actually taken training in this area, and that is a fairly low number compared to the number of civil servants within the province.

And another point that was very concerning was the number of actual incidents caused by employee data loss has risen by 25 per cent in the last year, so what you've just said is relevant and very important. But what we're finding here is information is being lost, data loss is occurring and 25 per cent increase in that loss is significant, so I'm just wanting to know how you're planning to address those two points.

Mr. Doak: As I mentioned, we accept the Auditor General's recommendations, including the one to consider making mandatory the security training which would mean all employees who come through the system get that training, understand the importance. We have over 15,000 employees so it's a big task to get out there, to train people. Unfortunately, people take security for granted. All of us do. Until you have a compromise in your data, you don't realize how important that smart phone is and how much information it has. So we're going to look at the Auditor General's recommendations and ensure that we increase ICT security.

If I can just read from a memo that the secretary to Treasury Board sent out on May the 17th of this year. She indicates that information security awareness is increasingly important as technology becomes more sophisticated–I'll just give you the highlights of this–it's expected that all new and existing employees will attend information security awareness training sessions, as well as refresher courses every four to five years. Afterwards, we've developed a half-day awareness session and there's information available on the website.

I think that we have to be more proactive than simply sending out memos and sending out reminders, and to work with our BTT area to make sure that we are.

Mr. Chairperson: Mr. Doak, following on that, occurrences such as the individual who fled from the US to Russia recently with a wide variety of information in his possession have heightened people's awareness of security. Do instances like that bring it a little closer to home, or do people think that couldn't happen here?

Mr. Doak: Certainly, those incidents bring it home, and whenever there's a compromise in data, as I said, you can take it for granted and then you lose data, and you realize how devastating it is all around for the individuals whose, you know, privacy is compromised and it's a wake-up call for all of us.

You know, I won't speak to that specific situation except to say that you place trust in employees and trust in contractors, and for all the due diligence you may have in place, if there's a breach of that trust, it's hard to protect against. We do have procedures in place to make sure that, you know, we know where data is. We know where it's been stored and we know where it's been accessed, but it's still–and there's still some significant amount of trust in the system when people are inside of the system.

Mrs. Rowat: I'd like to ask the Auditor General, with regard to target training, do you–was that raised with the departments with regard to highly sensitive areas that were–like the Child Abuse Registry and the witness protection program–was that raised as something that needed to be looked at? And did you get a sense that they were actually going to be moving in that direction with regard to training their employees?

Ms. Bellringer: That wasn't an area we looked at.

I'm sorry, I've got my–I'm holding some pages open because there was one thing I did want to just go back and reference, just to–in the context of the conversation about the external contractors, to some of the specific information, I think, that you need to note through the report.

One is–figure 1 on page 63. So it just gives you a sense of the size of the contracts we're talking about that are external. So 49, 50 million in 2011, 2012. I mean, it's large amounts.

The recommendation–the main recommendation attached to that–there are several–but on page 92 we speak about incomplete assurance that contractor IT security controls operate effectively.

And to sort of simplify a lot of pages with a lot of information in it, it's a need that we feel the department has to increase the extent to which it's getting assurance that the external contractors have all of the various controls in place. They're large companies with strong reputations but that's not enough in our view. You have to still oversee it because it's protecting government information.

So that's where recommendation 26 comes from, recommending that BTT periodically obtain independent assurance that the IT security practice is used by its contractors are operating effectively.

One of the comments in the response from officials specifically addresses that and comments that a number of major long-term IT service contracts are up for renewal which will provide the opportunity to strengthen security controls to an outsourced operations.

So those things, I mean they're in different places but they flow through to speak to one area that it's, it, no it isn't the, you know, the smaller pieces of IT hardware that we're all familiar with but it is a large element of the system that the government is operating.

I just wanted to draw it to your attention as an area that–I don't know where it is currently but that's where we left it when we ended the report.

Mr. Gerrard: Yes. Let me start by just a clarification on the scope of the IT information that you're dealing with. You've got the child abuse records, you've got the Child and Family Service Information System which is accessed and used around the province and so on. Just give us a little bit more.

Mr. Doak: Thank you. Outside of Health which is–has its own ICT government system, we have basically all of it. The Justice data, much of the Education data, Child and Family Services, property registry, Vital Statistics, pretty much everything that government proper is responsible for falls under out ICT area.

Mr. Gerrard: In the area, for example, where the property register is in the process of bringing privatized in some fashion what happens with the IT security related to that?

Mr. Doak: Well, I'll only speculate because I'm not intimately involved–that's through another deputy minister and another ministry, but there will be significant processes in place to make sure that the data's governed according to the appropriate legislation for the property registry.

Mr. Gerrard: Now in terms of, you know, if one of the main servers with a lot of information went down what kind of backup is there? Is it off site, on site? How often is there backups, so on?

Mr. Doak: There's a very complex system for backing up data off site, on site; depends on the value of the data and the Auditor General has indicated we need to do more in terms of data classification to ensure that we understand which data is most important and which would be most at risk for being lost.

There's also disaster recovery systems where if a server went down we would look to other service within the system or we might look to services to secure services run by third parties, or in fact, servers that may in another province or another city.

Mr. Gerrard: Now one of the things about the Child and Family Services Information System is that it has had a very bumpy road, as you're probably aware. Back in '87 it was said to be completed in six months and yet we've had Auditor General's reports, you know, like 2012 saying that there's still is a long way to go.

Do you have a role in ensuring that that's where it needs to be or is that up to the department and you just manage it once it's put in place?

***** (20:00)

Mr. Doak: The lead is usually by the business area and we work in partnership with the business area, in this case, Family Services and Labour, and we're actively involved with them in looking at the current system, making improvements to the system where we can, but, ultimately, likely leading to a new system for Child and Family Services.

So we play, I would say, more than a support role, but the leadership does fall within the business areas to carry out the application and development.

Mr. Gerrard: Yes, you know, I'm aware that in other operations one of the things that is done is to hire people who are, sort of, hackers, to see if they can penetrate the system and that can often be very useful to tell you whether there are gaps that you are not identifying. Is that something that you do?

Mr. Doak: We have an Information Protection Centre that–I'm not sure I'd call them hackers–but they test our systems routinely and there are practices in place to test those systems and we're–yes.

Mr. Gerrard: You know, I note in the–one of the concerns relates to the level of encryption that you have, so–but it seems to be lower, is what the Auditor General is saying, than perhaps it needs to be. Do you want to comment?

Mr. Doak: Stretching my technical knowledge, what I would say is, firstly, we accept the Auditor General's recommendation, she has experts in this area. Certainly, we're going to look at it. Clearly, what the Auditor General report has said is that we need to do more, and we're committed to doing more. We've already taken some significant action. We have, as I mentioned in my opening statement, a third party consultant who is–who has expertise in the information protection area, and we'll look at those kinds of things such as data encryption.

Mr. Gerrard: Do you have any idea of the number of computers, as it were, which are accessing various aspects of the system–and, of course, you've got hard computers, you've got laptops, you've got iPhones, you've got iPads and so on. Can you give us some understanding of what range?

Mr. Doak: We have over 450 different applications with thousands–tens of thousands of internal and external agency users. Tens of thousands of computers and mobile devices that access those systems. All of those systems go through some standardization before they're put out, so there's antivirus software put on them, for example. And we have systems in place to monitor anything that's attached to the network so we know what people are accessing, what data they're accessing. It's a very complicated task, but yes, we have systems in place.

Mr. Gerrard: Now in the case of, for instance, laptops and iPhones and iPads and things like that which are not directly connected much of the time but, of course, are correct–connected through cyberspace from– periodically at least. Are the same sort of systems in place for them? What is done to make sure that you've got those areas which are secure?

Mr. Doak: Any device that connects to the provincial network to access systems goes through some due diligence. Either it is what's called a virtual private network, a VPN, that provides security, or the device itself in enabled by our BTT area, or in this building, the Legislative Building Information Systems.

Mr. Gerrard: You know, I mean, presumably, say, when we're working with laptops, devices that require to have some level of password, is that a uniform requirement and what level of complexity, if a password is required in terms of–we know very well that if you've got an easy password, it's much easier to breach.

Mr. Doak: Thank you for that question.

Yes, there are standards in place for passwords. And I won't recite them verbatim, but they often have to include a number alphanumeric and a special character. They also–they have to be changed, you can't have the same password in perpetuity. So every four, six months, you'll get a notice to say your password's going to expire. The password encryption does vary somewhat by device, and we're moving more to standardization so people can't use password as their password.

Mr. Gerrard: Yes. One of the things that I noticed is that one of the typical problems with security leaks is with somebody who's fired, and there seems to be that there isn't as much of a protocol for somebody who's fired as there is for somebody who leaves voluntarily. Can you comment?

Mr. Doak: I believe that was an area that the Auditor General touched on, and we're going to look at the procedures that are in place so that when someone is let go, someone is fired, that we ensure that there are appropriate steps taken to ensure that that person doesn't access data.

It's important for us, for BTT, to work with departments because we may not always know if someone's been let go. So if we don't know, it's impossible for us to react, so it's our responsibility to make sure that we're informed and we'll work with the Civil Service Commission and the departments to make that happen.

Mr. Chairperson: If I could follow up on that, Mr. Doak, there are several of these areas that, of course, are critical. That one though, probably happens more often than not, not just people being fired, that may be rare, but people leaving the civil service. And maybe a more critical area to deal with now, than something to think about. Comments?

Mr. Doak: Yes, I would agree that, you know, we need to ensure that we have appropriate check lists when someone's terminated–whether they retire, leave voluntarily for another job, or get fired. That what we have to make sure is that people have access only to the systems that they have a right to have access to.

Fortunately we haven't had a breach of data but that doesn't mean that it can't happen, and we have to be diligent to make sure that it doesn't. We're going to prioritize that. We're working with PricewaterhouseCoopers on a number of things. They're the third party that I mentioned, and that will likely be one of them.

Mr. Gerrard: One of the things that you mentioned is that you're providing updates or training for people every four to five years. That would seem to be a long time in a IT world. And I–it would seem to me that you need to have something communicated effectively to people a little more frequently than that.

Mr. Doak: That was a recommendation of the Auditor General to do training more frequently, and we're going to look at it. It does take significant resources to get onto people. And I think you have to get onto people in an interactive way. Sending them a memo or sending them email, I think that that can be useful, but you need to have–you need to–people need to appreciate how important it is. And as I mentioned, it's not important until something goes wrong. That–you know, so we need to get out there with that message. And we'll certainly take the Auditor General's recommendation seriously and look at what we can do to improve our training.

Mr. Chairperson: Mrs. Driedger, you had a question?

Mrs. Driedger: I actually have a couple of them.

The deputy minister indicated that there have been no breaches but there have been intrusions. Can you give us an indication of what intrusions are and how many there might have been in the last year, and what that means?

Mr. Doak: Intrusions may mean that someone's been able to compromise certain of our security measures, get over a firewall, for example, but not then access a database. So there are different measures in place to prevent access. So, like almost all organizations around the world, there have been intrusions, but no one's been able to download data or access data inappropriately.

And sorry, what was the second question?

Mrs. Driedger: Can the deputy indicate how many there might have been in the past year? And I'll just add to that too, are you able to track where they come from?

Mr. Doak: I don't have a specific number. I can take that under advisement and provide that to the member.

We sometimes can figure out where they're coming from. Often just a geographic location. Hackers are very ingenious and they have time and resources, so it's sometimes difficult.

What's most important to us is to determine what the vulnerability was and close that hole, determine if data has been compromised, and if so, how, and then determine what we would do to prevent that from happening, not only the system or the server that it happened to, but across the system.

Mrs. Driedger: A question for the Auditor General's office.

Going back to point–or 7.3.3 of the report, the high-security zone not fully used. Can the auditor or her staff give us a bit of an explanation of what she's meaning or what the report is meaning, that the high-security zone is not fully used?

Mr. Fraser McLean (Audit Principal, Office of the Auditor General): What we noted was that there were a few items in the high-security zone but we did note from various IPC pamphlets that there were higher risk sensitive data that they put in their pamphlets, or types of data that they expressed in their pamphlets, but yet those were not in the high-security zone.

***** (20:10)

We did not follow up as to reasoning as to why they were not in the high-security zone, but we were asking the question as to whether or not you deem them as highly sensitive and yet they're not in the high-security zone.

Mrs. Driedger: Well, that was leading me into my next question. What is some of that information that is highly sensitive that should be in there but isn't in there?

Mr. McLean: I would point you to the section dealing with data classification, where that is up to the government to classify their data and then determine what should be in there, and that should be up to the business in collaboration with BTT.

Mrs. Driedger: And you found some of that in your review of this, that there was some that you identified as being highly sensitive or you saw it that the government had identified that it was highly sensitive, but they didn't put it in the high-security zone?

Mr. McLean: Yes, in the report–I believe it's section 5–we state that there is no formal data classification or–standard or information management framework which would help the government determine what is sensitive and what isn't and then, hence, what should go into the high-security zone. We can't comment on what the appropriateness of what wasn't or was placed in that high-security zone. We're simply commenting on the fact that there is no classification towards what should or shouldn't be.

Mrs. Driedger: And just to clarify something for me, you said you had seen a pamphlet and in the pamphlet it said that these were in a high-security zone but–

Mr. Chairperson: Mr. McLean.

Mr. McLean: I believe it was a security pamphlet in which we got that from.

Mrs. Driedger: And just clarification on that. It was stated in the pamphlet that certain information was in the high-security zone and you didn't find it there, though, even though the pamphlet said it was there?

Mr. McLean: Yes, if referring to 7.3.3 within their published security awareness pamphlet, IPC states that the following information managed within the environment is highly sensitive. We did not take that a step further to check if it was in the–we determined that some of that information wasn't in the high–in the–sorry–in the high-security zone, but hence, why we said that it was not fully used.

Mrs. Driedger: Thank you very much, and a question to the deputy. With the third-party review that is going on right now, can the deputy give some indication as to when his department expects that report to be finalized?

Mr. Doak: We're going through–just to continue on this point–we're going through a process now with departments on data classification. And I believe, if I can speak for the Auditor General, that's what she's telling us to do, is need to do a better job to determine which of your data is sensitive and make sure the most sensitive data is in this high-security zone.

We're working with PwC now. I think that we've made some significant progress on data classification. We're technical experts. We need to go to the departments to fully understand the data. They need to help us or they need to tell us how to classify it, and then we'll secure it appropriately. I think that we've made considerable progress, and my expectation is within the next nine to 12 months we'll have most of that part of the work substantially complete.

Mrs. Driedger: In the auditor's report, there are 41 recommendations. Can the deputy give some indication as to whether or not any of them have been met or if they're all in progress, and how long it might take for all of them to reach completion?

Mr. Doak: Just flipping through the recommendations, I would say that the vast majority of them are work-in-progress, mostly working with PricewaterhouseCoopers on developing a plan. Some of them are further along than others. For example, we've developed a strategic plan, and we've developed–excuse me–a security policy; so, there's a number. And if the member would like, I could go through them, but there are a large number of them. I'd say, we've started on most of them with PricewaterhouseCoopers. Some of them we've completed within the department; some we've worked with other departments.

My expectation and direction to the department was that we have to have substantial progress within the next year by the end of the fiscal year, and I regularly meet with my CIO and review the recommendations. So my hope is by the end of the year we have substantial progress done. These do take time. They do take resources. And there are many competing priorities with 450 applications to maintain–not trying to make an excuse, just to give you a context of what we're dealing with–but we take, you know, we take ITC security very seriously, and, as I said, we accept the Auditor General's recommendations and we're actively working towards implementing them.

Mrs. Driedger: And, I guess, just to the Auditor General, you know, based on that response, do you have a comfort level that some of these challenges will then be addressed, you know, sooner than later, that there are some serious concerns because of the fact it is about security? Do you have some comfort, then, in the process that the department is going through now?

Ms. Bellringer: I don't know yet. I haven't seen anything, so I really don't know.

Mr. Cullen: Yes, to the auditor, can you–you made a comment earlier about a–you've been looking at this for eight years. Could you expand on that comment you made? Have you been looking at this particular department for a number of years?

Ms. Bellringer: We did have an eight–a comment about eight years specifically in this report. That was referencing a fairly comprehensive audit that the audit–that the office had done at that time. So that was where the eight years came from. And we did have some comments in this report about a few pieces of the framework that we had found in place back then that were no longer in place at the time of doing this audit. So we, I'm–other than being disappointed, I'm not sure what you can do about that. So they would then flow into further recommendations to remedy those areas.

There were a number of other–we've done management letters–we've issued management letters as a result of financial statement audits that we've done. We've had a couple of reports that have been in public reports that we've issued through the Public Accounts audit and others where we've had related recommendations, and we're referencing that when we talk about progress that hasn't been made.

Mr. Cullen: Do you have any ongoing dialogue, then, with the department as a follow-up to your report? Is there any back and forth with the department in terms of your recommendations and how they're going to proceed?

Ms. Bellringer: We haven't with this report. The staff haven't with this report. We do have some–I mean, we still have contact with the department within a totally different context when we're doing the audit of the financial statements for Public Accounts. But we haven't had any conversations back and forth with this audit.

Mr. Cullen: So when can we expect a follow-up report on this issue?

Ms. Bellringer: So, normally, all of our follow-ups are–I mean, our process has been one year after the issuance of the report we'll do our first follow-up. I'm a little concerned with the nature of this audit and trying to do it that way because it's almost an all or nothing. I mean, you get into, you know, if you want to have assurance over the integrity of the security management practices as a whole, you have to look at all of the aspects. And given that there were so many outstanding areas, you almost have to go back and do it again. And I'm not sure what time period I'd recommend for that, but I'd probably say our old time frame we used to look at was within three years we would expect full implementation of any of the sets of recommendations that we issue.

So I'd probably say other than an–an ongoing dialogue would be helpful along with a full audit around three years out.

Mr. Cullen: The auditor's report indicates the BTT provides IT services to more than 13,000 users of government's network, including 18 departments. And I'm wondering about–I'll call them arm-lengths agencies; maybe Child and Family Services might be an example. Do you provide IT services for those types of agencies as well?

Mr. Doak: I think, if my memory serves, Child and Family Services is a bit of an exception that we provide services to them. Outside of Child and Family Services, I don't–there's some special operating agencies which are really just an extension and creation of government. So it's really the child and family services agencies which are incorporated and governed by their own boards that are the anomaly.

***** (20:20)

Mr. Cullen: Just to follow up, then, in terms of Crown corporations, is there any overlap or do you do any work with Crown corporations in terms of your network?

Mr. Doak: I'd say that there's no overlap, but we often work with Crown corporations where we have common interests. For example, we might run the same SAP software, and if we're looking at development, we'll look to the Crowns for partnerships or to lever the systems that they have in place.

Mr. Chairperson: Mr. Gaudreau, do you have a–

Mr. Gaudreau: I just wanted to see, do you have an estimate of the cost of all the recommendations for all this upgrading and all this software? Do you know that?

Ms. Bellringer: No, we don't.

Mr. Chairperson: I can just intercede here for just a moment. In terms of systems that you run–wired networks and Wi-Fi networks–do you have a breakdown on percentages?

Mr. Doak: The vast majority are wired. Wireless still has security challenges, so we discourage wireless usage. I'm not sure that people do access our system through virtual private networks, through wireless which creates the security–the encryption that we need. Generally, all of our offices that I'm aware of are hard-wired, because it's the most secure and it's the fastest as well.

Mr. Chairperson: And to follow up on that, what would stop someone from setting up a wireless or Wi-Fi network attached to your wired network if they had the expertise? I do, for instance, but I have not set one up that way because I reconnect my laptop every day. But if I got tired of doing that, what would stop someone from doing that?

Mr. Doak: You may be able to do it, but in order to access the system, there's credentials required. There's a username and password required or there's a VPN token–you know, the tokens with the numbers on them required. So, if you were, you know–and for example, at home, when I'm working at home, I can access my work email through my laptop, but I go through a security system to do that. So you might be able to access it; it shouldn't do you much good unless you have the credentials to actually access data.

An Honourable Member: He's going to be watching you.

Mr. Chairperson: I know enough to be dangerous, but not enough to be good. That's–Mr. Cullen.

Mr. Cullen: Yes, Mr. Chair, you know, clearly, the auditor's laid out quite a number of recommendations here in a pretty strong wording in her report here. And it clearly–she talks about significant improvements are required. What is your biggest impediment to getting those recommendations addressed?

Mr. Doak: I would say it's resources and competing priorities. But, you know, as I said, we accept the Auditor General's recommendations. We're going to 'repriorize' what we do to make sure that we make substantial progress on these over the next year. That may mean some lower priority things have to be shifted, but that's what we'll do.

Mr. Gerrard: Yes, when you're dealing with somebody like Snowden who's gone in and downloaded a whole lot of material–you've got 450 approximately different software applications. How many of those software applications could somebody go in, like Snowden, and download a whole lot of valuable data?

Mr. Doak: You'll have to forgive me. I can only speculate. Generally, people are only granted access to data where they need access. For example, in the child and family services system, you can only look at your cases. You don't really–unless your granted that ability–you don't have the ability to download the whole database, for example, like Mr. Snowden has done.

There would be certain people within our ICT area who have the credentials who would be able to do that–developers and such–and those are the people that we do security checks on. So, I would say that there's a relatively small number of people who could download a whole database and potentially use it or misuse it.

Mr. Gerrard: With a database like the CFSIS database, for example, some electronic systems are set up so that you know when somebody accesses it, who's accessed it, when they've accessed it, what changes they've made. I mean, does that apply in, for instance, the CFSIS database?

Mr. Doak: My understanding that there's an audit trail on all Child and Family Services transactions.

Mr. Gerrard: Yes, and how many of the 450 software applications would that apply similarly? Do you know?

Mr. Doak: I don't have a specific number, but I know on sensitive systems like Child and Family Services or the Social Allowances Management Information Network, which deals with provincial welfare information, there are audit trails. I presume that there are in the Justice ones and the other critical ones, but I can't be assured of that without taking it under advisement.

Mr. Gerrard: Now, I mean, it would seem that that would be something that would be important to check and to know.

You mentioned something about, you know, the time consumingness of training if you're going to do more than four or five years. But it seems to me that, you know, there are ways of checking that people have sort of upgraded their knowledge or have reached a certain level of, you know, checking the security of their password or what have you.

And just as you have somebody change their password every six months, you could, in fact, have people answer a rotating series of 10 questions every six months and that would provide you a pretty good indication of whether they know. And if there's some deficiencies there then you could have them say, well, I mean, you should be taking an upgrade. I mean, there are ways of doing this I would think that would actually be quite economical instead of having a standard training session.

Mr. Doak: It's a good suggestion. We'll look at what the possibilities are and what other jurisdictions do.

And I think that you can enable training, enable testing, enable due diligence through technology. And we need to do that. It'll be difficult for us to sit desk to desk, across the desk from some 15,000 employees and do training every several months or even every several years.

So, certainly we'll look at potentially using technology to do that. Thank you.

Mr. Chairperson: I guess, Mr. Doak, I have a question about data ownership, if you don't mind.

We all have email accounts; some of them are government email accounts. Everybody, I believe, at this table has a government email account that flows through government servers, and we presume them to be private and we expect them to be so. However, if there were legal issues I'm sure they could be accessed through a subpoena or something of that nature.

So can you tell me, does the government own that data or what are the legalities of that?

Mr. Doak: Not being a lawyer, I'll give you my layman's view. The data that we have as civil servants, it's not my personal data, it's government data. Whenever I create a record, that record's governed by policy, it may be governed by the FIPPA–the freedom of information protection of personal information–sorry, I think I got that wrong–or it may be subject to some judicial review.

It's not my data. And, actually, I don't have and shouldn't have an expectation of privacy around the emails that I send. I send them as a deputy minister. I don't send them as Grant Doak, ordinary citizen. So government has a right and responsibility to control that data, manage that data and use that data as it sees fit. And that applies to all civil servants.

Mr. Chairperson: Any further questions of the deputy or the–Ms. Bellringer, do you have a comment?

Ms. Bellringer: Just on that last question that you had around the personal information, I mean, it's somewhat related to recommendation 20. And there is a complication with regards to–I mean, this is where we recommended that the commission amend their security check policy to require periodic statutory declarations from employees in designated positions. Once a data classification system's in place, require a periodic security check on employees in designated higher risk positions.

So it's not as simple as government can just go in and look at everything on your computer. There are some implications to that with the Civil Service Commission. So, we have drawn that out within here to make it something that can monitored to ensure there's nothing going on from the other side.

Mr. Gerrard: An additional question with regard to what's happening, because you brought up the property registry as one of the databases. And we are–the government is in the process of privatizing that in a fashion. And that–I mean, the whole goal of privatizing, as I understand it, is to have a easily searchable database, which, of course, the private corporation will market access to in effect, because they are selling information that's there on the property rights or the property entitled information.

***** (20:30)

And what–can you tell us a little bit more about the boundaries that will exist with–between, you know, what's government property and what's private sector property and what the rights in terms of that information are in this respect?

Mr. Chairperson: Mr. Clarkson, are you able to answer this question for us?

Mr. John Clarkson (Deputy Minister of Finance): So I think I can cover most of this answer for you.

In terms of the sale of the property registry, we are selling the processes related to it and the organization that provides the services related to the functions that are there. The data itself is being maintained under the ownership of the government and we're responsible for that data. We are going to be giving them an exclusive licence to use that data for the purposes of providing the property registry services and we are maintaining responsibility for all of the parameters related to the usage of that data and so there is a fairly extensive licensing agreement that we're entering into with them, regarding the actual utilization of the data itself.

Mr. Gerrard: Yes, and in terms of–I mean, we've been talking about data security, right? And so what–because obviously this data is going outside of the government servers, I would presume. I mean, I don't know precisely what the arrangement then, but what's the arrangement in terms of data security?

Mr. Clarkson: So, in terms of the data security, there is a component of the licensing services agreement, which outlines the use of the data. It also specifies the security requirements related to the data itself and we're working through those processes with the company today itself.

Mr. Gerrard: Yes, and so, all right, the company operates, you've got the licence agreement and so on. What happens if there's a breach, a security breach at the company level?

Mr. Clarkson: In terms of any kind of non-performance activities related to the contract itself in which the breach would fall under, there are provisions for us to have remedies related to that, right up to and including having the service come back in-house, if that was required to do that.

Mr. Chairperson: Thank you, Mr. Clarkson.

Any further questions of the deputy or the minister or the Auditor General?

Thank you, Mr. Doak and Mr. Minister. I would imagine, given the length and breadth of the questions, you can understand we are interested in this area and want to ensure that security is good in the government services and that Manitobans can be ensured that their data is secure.

I want to ask you a final question on how you can help to ensure this committee that these recommendations–I understand you have a lot of things to do and you have a moving target here–but how can you can assure us that these move from the to-do list to the being-done list?

Mr. Doak: Thank you. Thank you for that and thank you again for inviting me tonight.

I, personally, take data security very seriously. I come from a child and family services background. I understand how important that data is to individuals and the auditor will ensure that we do move ahead with the recommendations. There'll be a review done within a year and I've emphasized to my department that we need to make substantial progress on these recommendations, particularly considering the pointed comments that the OAG made around past recommendations and the lack of action on them.

Mr. Chairperson: Any further questions?

Thank you, Mr. Deputy and Mr. Minister. Thank you for your time and your staff for joining us this evening, and we look forward to a follow-up report and see how we're doing here.

So we will now move along to Chapter 8, Senior Management Expense Policies, with the Minister of Finance (Mr. Struthers) and Deputy Minister Clarkson joining us at the table.

Thank you, Mr. McLean and Mr. Harold, for joining us this evening.

Does the Auditor General have–wish to make a statement on Chapter 8 we will be dealing with?

Ms. Bellringer: Mr. Chair, so on the audit of senior management expenses, we examined senior management expense policies in a 113 provincial agencies, boards and commissions. We wanted to find out if the policies existed in each of these organizations, so we actually put a survey out to them, and whether–once we got them, we compared them to the central government's General Manual of Administration. We then randomly selected 10 for detailed examination to determine if the senior management was complying with the policies in place in their organization, and to assess if all of the expenditures were reasonable.

We found that the GMA generally covered appropriate topics related to senior management expense policies and those policies were comprehensive.

Not all provincial organizations had senior management expense policies in place. The policies that were in place varied significantly from one another and from the GMA.

For the sample that we examined in detail, senior management was–were complying with the policies with few exceptions, and in the 10 organizations in our sample, we did not identify any excessive expenditures.

Over three-quarters of government spending takes place outside of government departments. We–this is something that we quote in the report, at a time when government is working to reduce deficits, clear central guidance about spending expectations is critical to control costs. Compliance monitoring and enforcement strategies are also necessary to ensure that expenditures–expectations, rather, are being met.

We recommended in the report that Treasury Board Secretariat monitor whether all agencies, boards and commissions have appropriate expense policies in place, consistent with the GMA or applicable legislation.

One thing I just want to point out, we did, after the report was issued, we sent specifically this chapter of the report, we sent a copy of that to all of the organizations that were surveyed, and we sent detailed comments to the 10 organizations that we sampled.

Mr. Chairperson: Thank you, Ms. Bellringer.

Does the deputy minister wish to have an opening statement?

Mr. Clarkson: Yes, just wanted to say thank you to the auditor and her office for the work that they have done in this area and the recommendations that were made.

We certainly understand the importance of controls in this area and appreciate the recommendations that are there.

We also appreciate the review that was done of the General Manual of Administration and the nature in which that policy has been reflected on in her report, and the importance of ensuring that all of the government-related agencies have similar kinds of activities for their senior policy activities. So, thank you.

Mr. Chairperson: Thank you, Mr. Clarkson.

The floor is now open for questions.

Mrs. Driedger: Mr. Clarkson, a question to you: With the recommendation from the Auditor General that Treasury Board Secretariat monitor whether all agencies, boards and commissions have expense policies in place, can you indicate whether all of them do now have expense policies in place?

Mr. Clarkson: So we are in the process of gathering that data. We have requested that through the various individual departments, and we are hoping to have that information together by the fall of this year.

Mrs. Driedger: There was also a recommendation that the expense policies that will be in place will be consistent with the GMA or applicable legislation. Is that a component of what you are also addressing as you are moving forward with this?

Mr. Clarkson: Yes, it is.

Mrs. Driedger: How then do you intend to do compliance monitoring? Has that been discussed?

Mr. Clarkson: No, we haven't yet discussed the issue of how we're going to monitor this on an ongoing basis. We will do that as part of the results that we get back from the information we collect.

Mrs. Driedger: And the Auditor General had indicated that she had provided information to the various groups. I would ask how the government intends to, you know, communicate all the requirements to all the affected parties. Is that something that has already been done as the department is moving forward, to move this issue forward? Have you communicated now to all of those boards and commissions, and–where's that at, I guess?

***** (20:40)

Mr. Clarkson: So the first stage, as I mentioned, is we'll be going through and collecting the information regarding which agencies and boards and commissions this should apply to. We will then work through the individual departments that are responsible for those areas, to communicate what the policies should be, and we will deal with–also determine, from there, the follow-up activities that need to take place.

Mrs. Driedger: Are there some organizations that do not fall under the GMA scope?

Mr. Clarkson: Most of them do. We are examining whether all of them do, and we'll have that information available for us too.

Mr. Chairperson: Any further questions on this section?

Mr. Gerrard: Yes, I note on page 252–but let me start with a more general question, and then I'll get to that.

One of the things that's mentioned here is the importance of enforcement strategies. Can you tell me, in terms of your expenditure management, what your enforcement strategies are?

Mr. Clarkson: I guess I would like to–just clarification on what you're meaning by enforcement strategies and which you're referring to in the report, which section, which page?

Mr. Gerrard: Well, for instance, on page 250–sorry, 249: Compliance monitoring and enforcement strategies are also necessary to ensure that expectations are being met.

And this is the bottom of the page. And the–I mean, what it's saying right at the bottom is that you need to have compliance monitoring and you need to have enforcement strategies if people are deviating from your, well, the GMA process and manuals, yes.

Mr. Clarkson: So, in terms of enforcement strategies, they would generally deal with our normal management practices, in terms of how we would be responsible for the areas that we look after. So, in terms of the senior managers reporting to us, that would be my responsibility as a deputy minister, to deal with the–enforcing the policies related to our senior management expense activities. In my case, that would be a responsibility for the people that would sign off on our–on my expense claims. Those policies would be outlined within our controllership framework for each of us, in terms of how to deal with it, as long–as well as within our General Manual of Administration. And so we would deal with it in through the normal practice of your management relationships that you establish.

Mr. Gerrard: I notice that while some of the areas of government are using the GMA approach, that others are using different approaches, in terms of their approach to expenditure policies for senior management. Why do you have this variation across government, and is this something that you're going to just continue to let happen, or are you going to bring everybody under the GMA policies?

Mr. Clarkson: It's part of the work that we're undertaking now. We're determining who is in and who is out and some of the reasons and rationale for that. There may be cases of specific legislation that people fall within that requires them to be different. I'm not positive about that, but we'll know those reasons afterwards, and then we'll be able to address that issue as to who should be in and who shouldn't and why that they might be different and then–and the need related to that.

Mr. Gerrard: Page 252–there appears to be areas which are adequately covered under the GMA and areas which are not, and the auditor, in looking at this, said that GMA includes policies on all of the appropriate property topics with the exceptions of reimbursement of traffic violations and reimbursement for alcohol.

So, I mean, what is your plan in terms of filling in that gap? Are you just going to leave those areas not covered?

Mr. Clarkson: Again, we'll undertake that as part of the work that we're doing around–right now just surveying what is going on and then we can manage both of those kinds of issues, and we'll look at what needs to be added to the policies to make sure they're comprehensive and complete.

Mr. Gerrard: You know, I mean I'm a little surprised because I have the impression that you're really just in the front end of trying to look at these processes across government. This is–seems to be a fairly recent initiative, in terms of looking at standardizing GMA policies and other policies across government.

Mr. Clarkson: This part is a fairly recent initiative. The recommendation itself is a report from January of 2013 and we designed the way in which we wanted to approach that, working through the various departments to deal with that, and so it is one that is in its early stages of implementation.

Mrs. Driedger: A question for the deputy minister: As MLAs we're not allowed to claim liquor when we are expensing a meal. Can the–*[interjection]*

Okay–you listen now, here, then.

There is a–on page 279, there is a–quite a bit written actually here about alcohol and senior management expense policies. Can the deputy indicate who within senior management–I'm not looking for names of people–but are there actually staff people that can have their booze paid for at events?

Mr. Clarkson: I have not looked at this issue. I'm not aware of the extent of this taking place and it would be certainly something we would be looking at as we move forward, in response to Dr. Gerrard's question, as well, too, as to how we're going to deal with this issue.

Mrs. Driedger: I guess I would just add to that, that probably is something that should have a closer look, you know, for a variety of reasons. But, certainly, when–I know the rules for us are extremely tight in this particular area. And I think probably taxpayers would want to know that we are addressing this part very, very responsibly. So I'll leave that with the deputy.

Mr. Chairperson: Mr. Clarkson, do you have any comment on that?

Mr. Clarkson: No.

Mr. Chairperson: Okay, thank you.

Further questions?

Mrs. Driedger: Okay. Well, there's a few really interesting things in here, like dry cleaning. But a question that has come up to me and actually has been posed to me by the public and it is related to senior management expenses: Are there any restrictions when cars are provided, you know, leased vehicles are provided, you know, whether it's to Cabinet ministers or to senior staff? Are there–are these, like, bare-bone cars or are they all, like, high-end vehicles with XM Radio and, you know, are they, like, high-level cars or are the cars that we are providing through the leasers, are they, you know, basic good leased cars in running order, middle-of-the-road kind of cars or are they sort of high-end cars?

Mr. Clarkson: The vehicle policies are set in terms of what we can qualify for. I don't actually have a government vehicle so I don't know what those policies are. But you would have to deal with people in– government services, I think, are the people who actually control vehicle policies. But I know there are policies related to executives, ministers and others, in terms of their transportation needs, and I do know that for executives and MLAs, the issue is some of them are hybrids, and I just don't know what the policy is. So you'd have to deal with government services.

***** (20:50)

Mr. Cullen: Yes, just a question regarding the GMA. I'm just wondering how often that manual is revised.

Mr. Clarkson: There is a regular and routine review of the General Manual of Administration that is done, and it's updated on a fairly regular basis. I don't think there's a time schedule, but it is done on a regular basis.

Mr. Cullen: Then, who does that, makes–who does the review and who makes the changes?

Mr. Clarkson: The staff people that are responsible for the General Manual of Administration are within the Treasury Board Secretariat and they're responsible for undertaking that review. They would bring those changes forward through the Treasury Board process and then they'd be communicated throughout government.

Mr. Cullen: To the auditor, then, did you have a–obviously, had a look at the GMA policy there. Was there anything in there that you saw alarming or in any recommendations arising out of that review that you had of the GMA?

Ms. Bellringer: No, not other than the ones that were just brought up; the fact that the GMA policies covered many things consistent with other–and we only looked at senior management expenses when we did this audit. And we were saying the only ones that were missing were those on traffic violations and alcohol that we would have expected to have seen something. We are using the GMA all the time when we do our financial statement audits and so we're quite familiar with it in our office.

And I just say, and you know, as a general comment, it does get periodic updates, but it's a huge–if you will–document. I mean, we always look at it online, so I don't even know what it would look like if you were to have a printed copy. But we're talking an extensive document, so I wouldn't expect that the whole thing would be looked at each time there's a revision made. But every now and again, there–it might be a useful thing to, you know, take a look at some of the consistencies. And the thing we drew out in this report was there was a lot of detail in some areas and very little in something else. And it was just missing a bit of balance across the board. So, there's all kinds of other things you might want to look at periodically to just improve it and make it easier for those of us who are having to apply it to be able to do so.

Mr. Chairperson: Any further questions on this section?

All right, we will then move on to the Auditor General's Report–Follow-Up of Previously Issued Recommendations–dated January 2013, Section 9–Public Sector Compensation discloser–Disclosure Reporting.

Does the Auditor General mist–wish to make a statement?

Ms. Bellringer: Mr. Chair, this report was originally issued in 2009. We had three recommendations in the report and all of them remained in progress when we did the 2013 follow-up. One was a recommendation that the threshold be increased. It's a–this is entrenched in legislation. There's a $50,000 threshold, that all compensation above that amount have to be recorded in the reports and made public. It now captures far more than was originally intended by the legislation. So, it's our recommendation that that be increased, and yet it would still accomplish what the legislation was set out to do.

The second recommendation is that all of this information be available on a website. We didn't find it easy to access most of it. The core government information's available through Public Accounts, and you can see that when you–if you look online or the hard copy of Public Accounts, Volume 2. But for all of the agencies, boards and commissions in government's control that are included in the government reporting entity, you have to actually go to them individually and ask them for a copy of their report. So, it's something that's not easy to access. And that was the second recommendation, is–to make it accessible.

And the third was eliminating the audit requirement for not-for-profits. There's a threshold in the legislation, that if you receive an amount greater than that from any agency, board of commission or core government, so it would be a requirement to sort of figure it out from all of those aspects, that you are required to prepare the compensation disclosure. It's impossible to monitor. It's not often requested, and so we recommended that it could be available upon request but not require an audit, which is actually costly for each of those organizations.

That's it, Mr. Chair.

Mr. Chairperson: Thank you, Ms. Bellringer.

Mr. Clarkson, do we–do you have an opening statement?

Mr. Clarkson: No opening statement.

Mr. Chairperson: All right. Questions on this section.

Mrs. Driedger: Thank you–

Mr. Chairperson: Or, sorry, I'm–Mr. Gaudreau, I had indicated–*[interjection]* All right, Mrs. Driedger.

Mrs. Driedger: Thank you. Based on the first recommendation, could Mr. Clarkson indicate whether or not there has been any further discussion about increasing the threshold for reporting compensation?

Mr. Clarkson: Yes, there has been a discussion related to that. We're looking at a number that's around the $75,000 mark to keep in line with what it was originally intended to. And we're working at the legislative process to look at how we can get that through the processes related to that.

Mrs. Driedger: Can the deputy indicate which legislation this is actually covered under?

Mr. Clarkson: I believe the legislation is actually referred to as The Public Sector Compensation Disclosure Act and that we are looking at amendments to that piece of legislation.

Mrs. Driedger: Can the deputy indicate when we might see that legislation coming forward?

Mr. Clarkson: What gets on the legislative agenda is up to the government to decide which pieces of legislation they would choose to bring forward.

Mr. Chairperson: Mr. Gaudreau, did you have a question?

Mr. Gaudreau: Yes, actually it's related to this. Is–I guess, with–when you raise the threshold, it's good; that'll have–actually have some cost savings, right? To try to–when you're not capturing as many people and having to look through all the departments for the names. Will that not have a cost savings to try to find all of those people who are encapsulated in that?

Because I know the original intent was–it was years ago when $50,000 was a lot of money and–not that it isn't now. I mean, I'd love to have $50,000 in my pocket, but it's definitely not as much money as it was when this was originally drafted.

So will that not have some cost savings to us for increasing that limit?

Mr. Clarkson: No, the actual activity of undertaking the search to get the people to produce in the report is a–it's just a program parameter that you would change in that search capacity. So it doesn't really impact on our abilities to undertake the search.

So it doesn't have a cost impact other than printing a few less pages when we actually print it.

Mrs. Driedger: Recommendation No. 2 indicated that compensation disclosure reports for all organizations within the government reporting entity should be accessible on provincial government website.

Is that happening right now? And, if not, are you moving forward to ensure that all of that becomes much more readily and easily available by website?

Mr. Clarkson: Yes, we have been looking at this one, and we're looking at how we can make this information more readily available for all entities that are reporting under the public sector disclosure act.

Mrs. Driedger: And can the deputy indicate when that might happen?

Mr. Clarkson: We'll be looking at bringing forward some recommendations this fall in terms of how to address this issue.

Mr. Chairperson: Before we move along, I see we are approaching 9 o'clock, which was the time we agreed to suspend on. And what was–be the recommendation of the committee?

Mrs. Driedger: I would recommend that we continue 'til we finish, which probably won't be very long.

So, if we said 9:15 to end, unless we end sooner.

Mr. Chairperson: What's the will of the committee?

An Honourable Member: Agreed, 9:15.

Mr. Chairperson: Thank you.

Mrs. Driedger: The third recommendation was addressing the issue of not-for-profit entities who receive government funding and allowing them not to have to provide audited compensation disclosure reports but still the compensation information should be available if requested.

Where is the movement around following through on this recommendation?

Mr. Clarkson: We certainly agree with this recommendation, and we are looking at the amendments that we require to make this happen and also looking at how we can still ensure, though, that people who want to get at the information can manage to get that as well too. So those are part of the solutions we're looking at.

***** (21:00)

Mr. Gerrard: Yes, in regard to No. 2. What–one of the things that seems to be happening at the moment is that if somebody works in a particular department, or in a particular sector of a department, and gets their compensation under one list, then they will be captured. But, if somebody has salary or non-salary income for whatever reason–contract fee for service, what have you–that a person can be on two separate lists, and they will not always be captured if both of those, they are below the threshold, whereas their combined income would be above the threshold.

I'm just wondering what you're doing in terms of assembling this data across government that would allow you to make sure that you're capturing everybody who's above the threshold.

Mr. Clarkson: I'll have to take that one back and look at specifically what we're doing in that area. I don't believe it's a significant issue within government departments proper, because people would be paid through the salary system and, therefore, they wouldn't come up in–and even if they come up in multiple different areas, their name would come up and that would be combined. So, it would be more applicable to those areas that are outside of government and I'll have to examine what we're doing in those cases to accommodate that.

Mr. Gerrard: Yes, I mean, for example, it could apply–it–with somebody who's got an income in, you know, in a special operating agency and then with a non-profit company, because you're trying to capture that which has got government. But if you add the total, they may be above the threshold, but if you take the individual, they're not. What's going to be your approach to that?

Mr. Clarkson: Well, the approach first would be examine what we're doing today, and then I'll determine what we need to do from there.

Mr. Gerrard: Will–where it's clearly the funding is primarily from government sources, presumably you would try and get a total income from government sources and be able to report that. Would that not be your objective?

Mr. Clarkson: Certainly, that would be the objective, and I'll certainly look at exactly what we're doing in those areas today, so that we–I can understand exactly what would–may be the issues we have to address.

Mr. Pedersen: Yes, Mr. Chairman, this is salaries only that is being disclosed? It's not contract work?

Mr. Clarkson: My understanding is that this is the salaries of individuals that are being disclosed.

Mr. Pedersen: I guess my–the question's coming because the law–not only in government sector but in private sector, too, there are people who are retiring and then coming back and working on contract work. So, is there anywhere that shows up, then, as non-salary contract work?

Mr. Clarkson: In terms of the Public Accounts reports that are done at the end of each year, in one of the volumes–I can't remember which one it is right now–there is a listing of all contractual services that take place. It's done on an individual department basis. *[interjection]*

Mr. Chairperson: Mrs. Bellringer, would you like to comment?

Ms. Bellringer: Oh, no. I'm sorry. I was just indicating it's Volume 2, and I said it's sad that I know the details of Public Accounts so well.

Mr. Pedersen: That's all right. I understand you're going to have a life after the end of March, so–

But, so, all contracts and contract services–services contracted–labour services contracted are in Volume 2?

Ms. Bellringer: It's even better than that; it's all expenditures over $5,000, but only for core government.

Mr. Chairperson: Any other questions on this section? Thank you to the–oh, I'm sorry. Mr. Gerrard.

Mr. Gerrard: Yes, I–just a question in terms of what your timeline to try and have this organized so that you'll have these recommendations addressed.

Mr. Clarkson: In terms of the recommendations, we have the proposal in terms of how to move forward with recommendation No. 1 and No. 3, which are the ones related to the limits and the non-profit and the changes available to that. And that really is–moving forward on that is dependent on the government's legislative agenda, to be able to do that.

And on item No. 2, we are hoping to have recommendations by the fall in terms of how to move forward with making the information more accessible for those agencies not part of the core government.

Mr. Gerrard: We're spending a lot of time in the Legislature, so I'm sure that if the minister has a bill, we shouldn't have any problem having it put forward and addressed.

Mr. Chairperson: I'm sorry, is there–was there a question there, Mr. Gerrard? No? *[interjection]* Or a Christmas carol? Okay, thank you.

Any further questions on this report? Thank you, Mr. Clarkson, and the minister for joining us.

We have one more report for us, The Auditor General's Report–Follow-up of Previously Issued Recommendations, dated January 2012. Are there any questions for this report? I see no questions.

All right, seeing no further questions, I will try to do this in the order of which we dealt with the report. Should we? Or–*[interjection]* We'll follow the order we have here and see if we can get everybody's attention.

Auditor General's Report–Follow-up of Previously Issued Recommendations, dated January 2012–pass.

Does the committee agree that we have completed consideration of Section 9 of the Auditor General's Report–Follow-up of Previously Issued Recommendations, dated January 2013? *[Agreed]*

Does the committee agree that we have completed consideration of part 1 of chapter 2, and–well, we'll do this separately, I think.

Does the committee agree that we have completed consideration of part 1 of chapter 2 of the Auditor General's Report, dated January 2013. Chapter 2 is the Citizen Concerns–"Part 1–Business Transformation and Technology"? *[Agreed]*

Does the committee agree that we have completed consideration of Chapter 3–Information Technology (IT) Security Management?

Some Honourable Members: Agreed.

Some Honourable Members: No.

Mr. Chairperson: Hearing a no, that is not agreed.

Does the committee agree that we have completed consideration of Chapter 8–Senior Management Expense Policies?

Some Honourable Members: Agreed.

Some Honourable Members: No.

Mr. Chairperson: No, I hear a no on that one.

That concludes the business before us. Thank you to everyone for coming tonight and for all of your questions. I think you were very engaged. Thank you to the pages and the staff.

And just to remind everybody, before we rise, it'd be appreciated if the members would leave behind any unused copies of the report so they may be collected and reused at the next meeting.

The hour being 9:08, what is the will of committee?

Some Honourable Members: Committee rise.

Mr. Chairperson: Thank you.

COMMITTEE ROSE AT: *9:08 p.m.*