First Session - Fortieth Legislature

of the

Legislative Assembly of Manitoba

Standing Committee on Public Accounts

Chairperson
Mr. Reg Helwer
Constituency of Brandon West

Vol. LXIV No. 11 - 2 p.m., Wednesday, September 12, 2012

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
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
TAILLIEU, Mavis	Morris	PC
WHITEHEAD, Frank	The Pas	NDP
WIEBE, Matt	Concordia	NDP
WIGHT, Melanie	Burrows	NDP
WISHART, Ian	Portage la Prairie	PC
Vacant	Fort Whyte	

LEGISLATIVE ASSEMBLY OF MANITOBA

THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

Wednesday, September 12, 2012

TIME – 2 p.m.

LOCATION – Winnipeg, Manitoba

CHAIRPERSON – Mr. Reg Helwer (Brandon West)

VICE-CHAIRPERSON – Mr. Gregory Dewar (Selkirk)

ATTENDANCE – 10 QUORUM – 6

Members of the Committee present:

Hon. Mr. Struthers

Messrs. Allum, Cullen, Dewar, Helwer, Jha, Pedersen, Whitehead

Substitutions:

Mr. Ewasko for Mrs. Driedger
Mr. Wiebe for Ms. Braun

APPEARING:

Mr. Cameron Friesen, MLA for Morden-Winkler
Ms. Carol Bellringer, Auditor General
Mr. Doug Harold, IT Audit Principal

WITNESSES:

Hon. Theresa Oswald, Minister of Health
Mr. Milton Sussman, Deputy Minister of Health
Hon. Steve Ashton, Minister charged with the administration of The Manitoba Lotteries Corporation Act
Mr. Winston Hodgins, President and Chief Executive Officer, Manitoba Lotteries Corporation

MATTERS UNDER CONSIDERATION:

Auditor General's Report–Annual Report to the Legislature, dated January 2012

Chapter 8–Wireless Network Security: Winnipeg Regional Health Authority and Manitoba eHealth; Manitoba Lotteries Corporation

* * *

Mr. Vice-Chairperson: Okay, good afternoon. Will the Standing Committee on Public Accounts please come to order.

For the committee's information, I have before me the resignation of Larry Maguire as Chairperson and Heather Stefanson as committee member of the Standing Committee on Public Accounts. Therefore, I'd like to welcome Mr. Cullen and Mrs. Driedger as new Public Accounts members.

Also, pursuant to rule 85(2), I would like to inform that for today's meeting Mr. Ewasko is substituting for Mrs. Driedger.

Now, before the committee can proceed with the business with this–with the business before it, it must elect a new Chairperson. Are there any nominations for this position?

Mr. Blaine Pedersen (Midland): I would nominate Reg Helwer.

Mr. Vice-Chairperson: Mr. Helwer has been nominated. Are there any other nominations? Hearing no other nominations, Mr. Helwer will you please take the Chair.

Mr. Chairperson in the Chair

Mr. Chairperson: Thank you. Welcome everyone. This meeting has been called to consider Chapter 8–Wireless Network Security: Winnipeg Regional Health Authority and Manitoba eHealth; Manitoba Lotteries Corporation of the Auditor General's report, the Annual Report to the Legislature, dated January 2012.

Are there any suggestions from the committee as to how long we should sit this afternoon?

Mr. Pedersen: Well, seeing as Ms. Braun isn't going to make any suggestions, I'll suggest 3 o'clock–3:30, sorry, pardon me–3:30 unless we have further business and to extend it on after that or if we're done before that.

Mr. Chairperson: The suggestion is that we sit until 3 o'clock–sorry, 3:30 and then review at that time. Do we have the will of the committee? *[Agreed]*

Also, are there any suggestions as to how we should consider this chapter? Perhaps we should deal with Health first, followed by Lotteries? *[Agreed]*

Would the Minister of Health bring her deputy ministers to the table please and introduce–

Hon. Theresa Oswald (Minister of Health): Yes, it's my privilege to introduce to the committee Deputy Minister Milton Sussman. Also, joining him at the table to assist in our discussions today, is Mr. Roger Girard, the CIO for eHealth Manitoba and Mr. Ken Browne, the acting director of information–the information systems branch.

They've been working really hard on these recommendations. And, at the request of the Auditor, Mr. Chair, I would add that they consider it a great privilege to be working with somebody with the vast experience that we're going to hear about today. I told her she should be concerned about the fact that the department enjoyed the audit, which was true, and, perhaps, she should be revisiting that herself.

Mr. Chairperson: Thank you, Madam Minister.

Does the Auditor General wish to make an opening statement?

Ms. Carol Bellringer (Auditor General): And I won't rebut that. We do try our best to work in as collaborative a way as we can, but we do bring full and fair reports to this committee.

I'd like to welcome you first to the new role and say that I look forward to working with you and with all the members at the Public Accounts committee.

I have today with me Norm Ricard who's sitting right behind here. Norm is the Deputy Auditor General and he has responsibility for all of our information technology work, both our IT audits as well as our internal administration. And, Doug Harold, who's sitting next to me–Doug is the IT audit principal for my office who was responsible for conducting the audit. And, thank you very much for the compliment for the very fine work that he does.

Our audit examined the security of wireless networking solutions within Manitoba eHealth and Manitoba Lotteries Corporation. Through inquiry, we noted that the central provincial government does not use wireless networks. However, many of the organizations in the government reporting entity do, so we selected only two such organizations handling sensitive data for our review. Our audit program and assessment criteria were based on internationally recognized standards including COBIT and the National Institute of Standards and Technology wireless standard.

Despite many examples of good practices, we found weaknesses that need to be addressed to protect the wireless networks. We provided our detail findings to both eHealth and Manitoba Lotteries to enable them to remedy all of the weaknesses we encountered. We also provided our findings for eHealth to the Winnipeg Regional Health Authority because eHealth is administratively housed there.

Our findings were that wireless risks were identified but not managed effectively over time. Information technology security policies didn't exist at eHealth, and exists but were not current at Manitoba Lotteries. The wireless security policies did not exist. Network security controls need improvement. Access point configuration standards need improvement. Wireless client device configuration standards need improvement. Wireless monitoring is not performed. Wireless network administrators require additional training, and security awareness training is lacking at eHealth.

And I will note that while that list sounds like we're only pointing out those things that are negative, the report itself balances that with things we found that–to be in place. But because of the sensitivity and the high risk associated with wireless security, we think it's important to focus on making those improvements.

Mr. Chairperson: Thank you, Auditor General.

Does the CEO, Mr. Hodgins, wish to make an–oh, sorry. Oh, sorry, we're gone to–does the Deputy Minister of Health wish to make an opening statement?

Mr. Milton Sussman (Deputy Minister of Health): Yes.

The results of this audit will assist Manitoba eHealth, the WRHA and Manitoba Health to further enhance existing processes to improve wireless network security. Manitoba Health welcomes the Auditor General's report and thanks her staff for their guidance and insight while conducting this audit. The challenge of information technology security remains a very important focus of Manitoba Health, Manitoba eHealth and the WRHA. Constant vigilance is required to ensure that security measures are kept up to date and to employ best–industry best practices.

The health sector is committed and is very serious about meeting the highest possible standards and considers these audit recommendations to be an active part of that process and an acting–active learning process. The opportunity to improve our processes is welcomed.

I'm pleased to advise the committee that all of the recommendations resulting from the office of the Auditor General's security audit have been accepted and have–are completed or nearing completion. Manitoba eHealth has an active plan to implement all of the OAG recommendations and is reporting back through their governance structures on this process.

The auditor's report specifically mentions the need to effectively identify threats, risks and vulnerabilities to all IT systems, including wireless networks. Risk management practices continue to be an organizational priority.

The purpose of a threat and risk assessment is to categorize information technology assets, examine the different threats that may jeopardize them and identify and correct the most immediate and obvious security concerns. Risk management processes are being formalized across Manitoba eHealth with the recent hiring of a risk manager. A common approach for risk management is being developed and initiated by that risk manager.

***** (14:10)

A formal threat and risk assessment have become standard practice since April 2010 within Manitoba eHealth for major IT system implementations for which eHealth is responsible, and that includes the wireless network infrastructure. After information technology systems are implemented, risk assessments are updated by eHealth when significant changes are made such as new software releases or significant business or process changes occur.

A vulnerability assessment is similar to a risk–a threat and risk assessment in that it can also include the process of identifying, quantifying, and prioritizing the vulnerabilities in a system. However, a vulnerability assessment often includes extra measures by which the defences of a system are tested. To address this need, Manitoba eHealth is in the process of implementing vulnerability management software.

The WRHA and Manitoba eHealth are proactively using technology to detect the presence of unknown and untrusted wireless networks in the WRHA. The WRHA has implemented the various policies that were recommended by the OAG and are moving forward on helping all authorities across Manitoba to do this as well. Manitoba eHealth has prepared technical and security standards, which include wireless network technology standards, and have also shared these with all health authorities. The WRHA-provided desktop computer configuration requirements have been updated to meet wireless network standards.

Manitoba Health–eHealth is training all designated network administrators on wireless technology. They are receiving vendor-specific wireless training and wireless security training and this training will be ongoing. A senior security analyst has been hired by Manitoba eHealth to implement a security awareness and training program within the WRHA. The security of the wireless networks is only one aspect of a security posture. All health sector information assets are also further protected in high security environments and are further subject to various access and security controls.

The WRHA and Manitoba Health–Manitoba eHealth will continue to work towards meeting or exceeding all of the audit's recommendations. Information technology security, as everyone is aware, is critical to protecting the health information of Manitobans. Thank you.

Mr. Chairperson: Thank you, Deputy Minister, and thank you for giving us a printed copy of your presentation. It makes things a little bit easier as we move along here.

Now, before we get into questions, I'd like to remind members that questions of an administrative nature are to be 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 wishes to defer it to the minister to respond to, that is something we would indeed consider.

The floor is now open for questions.

Mr. Pedersen: I'll get it started then. And the deputy minister, Mr. Chairman, said that Manitoba eHealth is in the process of implementing vulnerability management software. Just where are we along in that process?

Mr. Sussman: So Manitoba eHealth has established a vulnerability management platform and supporting

practices. It's now currently using the vulnerability management platform to perform technical security scanning of key wireless infrastructure, and the plan is to expand the use of that platform over time. So, there–it is in place right now with the intent of expanding its reach.

Mr. Pedersen: And, is it a process–are–is this vulnerability management software–is it something that you felt is–has been useful then to have it implemented? Is–obviously, you've taken the step to do it. Are you seeing an impact from having this program in place?

Mr. Sussman: Our–I'm told it is being–it is seen as extremely beneficial. It really does allow us to use a standard to assess, and it provides that rigour in assessing vulnerabilities.

Mr. Cliff Cullen (Spruce Woods): Welcome, Deputy Minister. You made a reference to–I know this particular audit was in reference to the Winnipeg Regional Health Authority and there is reference to other regional health authorities. Assuming other authorities are using wireless systems as well, can you just give us a bit of a sense in terms of what direction was provided to the other RHAs around the province as a result of this particular audit?

Mr. Sussman: All of the policies have been shared with all of the other regions and, as part of the amalgamation of the regions, we are trying to standardize more of these processes across regions. So they've been made aware of those policies and they've been–and it's been indicated to them that we will be implementing those policies across the province.

Mr. Cullen: You know, when you look at the use of these products across the province I think that's real–the crux of the matter comes down to protecting the privacy of individuals, and I'm just wondering, you know, in your directive is there stipulations in there in terms of what role individuals within the RHAs have in terms of protecting that authority and that–the individual information?

Mr. Sussman: Well, the policies have been shared. They haven't–there hasn't been a directive yet to implement them. We've indicated that they will be rolled out. We haven't stipulated the time frame yet with the regions but part of that was just waiting for the regions to be fully formed and more operational with the amalgamation.

There are requirements both–under PHIA, The Personal Health Information Act, that require the maintaining of confidentiality of personal health information, and in the employment agreements that staff have with the regional health authorities that is reiterated with them. So we think there are protections and they are made aware of it.

Mr. Cullen: I appreciate your response to that.

This is getting into another kind of a new area of technology in which Manitoba Health is engaging and it's in the telehealth, and I'm just wondering if the same sort of parameters that we've laid out for wireless–are those same sort of mechanisms and parameters are going to be in place for that new technology that we're looking for in terms of telehealth around the province?

Mr. Chairperson: That's a little outside this report, but if you're willing to answer, go ahead.

***** (14:20)

Mr. Sussman: The Telehealth program, as it exists now, and I think there will be an evolution of the Telehealth program as we get into other kinds of diagnostic abilities and the ability to look at telehealth in desktops and things like that. But the current structure is actually a much more mature system. It's been in place for 10 years and there are systems are–that are already in place. I–so it–I don't think it's facing quite the same risk and it didn't grow quite as quickly as the wireless network. Systems in the health system have grown and expanded.

Mr. Cullen: And you did touch on an important topic there, and that's the idea of new technology moving forward. Clearly, when the audit was done, and over the years we've had some older technology that was involved. Where is the department–where's Manitoba Health in terms of getting rid of some of that older technology and moving into the new technology? And does that new technology that we're, I assume, we're purchasing, does that provide us a higher level of privacy?

Mr. Sussman: So I think there is a process where we are replacing older technologies, I think, and moving to newer standards that will take some time given the legacy and the scope of the entire health system. I think the new technologies, I think, have with them better opportunities for security, and we will be going through the government of Manitoba standards as far as the implementation of those new technologies that IEM is really the leader for. So we will be consistent with those kind of policies.

But the safety and security of patient health information is something that is very important throughout the system and they're–I know in–even in the development of the electronic health record we've been in–working very closely with the Ombudsman to ensure that we are taking the necessary steps to ensure that that privacy is protected. So we've been having regular and ongoing meetings with the Ombudsman and getting their feedback in the development of all of our eChart electronic health records.

Mr. Cullen: Just reflecting on the Ombudsman and report that came out today, you know, clearly there's more work for us to do in terms of protecting privacy. And I guess it really–it comes back down to, you know, the people that are working within the department, primarily, that we have to rely on their ability to properly manage that. And I just want to make sure that, you know, those things that are–been put out by the Ombudsman today, that they are reflected in your policy going forward.

Mr. Chairperson: Is there a question there, Mr. Cullen, or–

Mr. Cullen: Well, no. I'm just glad to hear that there is consideration and discussion with the Manitoba Health and the Ombudsman office. Obviously, they've recognized there's some issues, and the issue is relevant to the people and the staff within there. So I know the deputy made reference to the guidelines that people sign. I guess we have to be diligent that we're making sure that those guidelines are being followed. So more of a statement than a question, Mr. Chair.

Mr. Chairperson: Madam Minister, do you have a comment?

Ms. Oswald: Yes, Mr. Chair, and the member raises an important point that did come out today on an issue that the Ombudsman raised concerning an issue that hadn't been contemplated under PHIA legislation. We accept the advice from the Ombudsman, and we're looking very closely, and I'll be working with my department on that policy matter to close any gaps as identified because patient privacy must be paramount in all of the evolution of technology that we see going forward. So, I can assure the member and all members of the committee that that policy matter will be addressed straightaway.

Mr. Wayne Ewasko (Lac du Bonnet): Thank you, Deputy Minister, just a quick question. You mentioned, as the report had come out in January 2012, Manitoba eHealth is training all designated network administrators on wireless technology, and then later on you mentioned that the training is going to be ongoing. You say that you've hired a senior security analyst.

I'd like to know: Had that security analyst been hired prior to the training had already started? Was that hiring done from within? And how much is that analyst being paid?

Mr. Sussman: I think the training didn't wait for this person to be hired. It–but it was going on while the person was being hired and after. The person that is being hired has responsibility for training going forward. But we had–we were doing training prior and during the person's–when the person was employed. The–I don't have the salary at my fingertips, but it would be one that would be disclosed in the disclosure that the WRHA does, but I can also provide it to you.

Mr. Bidhu Jha (Radisson): On this issue of eHealth developing certain standards, that says in the auditor's committee, is in the process. Have they been completed, and, if they have been, are they shared with all regional health authorities?

Mr. Sussman: Yes, the standards have been completed, and we've developed standards for the wireless networks, for desktop computer, for configuration, for passwords, and that those have been shared with all of the regional health authorities.

Mr. Jha: Just to clarify, when these standards are practised in all regions, are there any limitations in terms of the technology upgrading in those areas that it could be difficult to follow the standard?

Mr. Sussman: So the standards are in place within the WRHA. The standards have been shared with the other regional health authorities and they are in the process of implementing those standards. And at this point we don't believe that there will be an issue in them adopting the standards.

Mr. Ewasko: Now, just back to the analyst position, Deputy Minister, you mention that the training had already begun before you hired that position. Why did the WRHA feel that you needed to hire a senior security analyst?

***** (14:30)

Mr. Sussman: Well, the audit also referenced security training for the users of this system, and the

health system is a significant employer, and so we think that there was a requirement to have someone who could co-ordinate and lead those training initiatives. And, I think, in general, I think we want to ensure that we are on top of the audit recommendations and want to ensure that we are constantly updating that training and paying attention to what is clearly been identified as a very significant issue. So we do think it's a critical position to–and a critical issue for the system to pay attention to.

Mr. Ewasko: Mr. Chair, I do agree that it is a very important position and a topic to–for the regional health authority to pay attention to. But one thing is that who is initiating that training right after the audit was done, and was that person who received the position of senior security analyst–was that within–was that a hiring within or an appointment, or–

Mr. Sussman: The person came from outside of eHealth–that was hired–and he was hired in March 2011.

Mr. Chairperson: Mr. Ewasko, we need to stay on the report, as such, as well.

Mr. Ewasko: So if the person was hired in March of 2011, the report was done in January 2012, this person was already hired as the senior security analyst back then?

Mr. Sussman: As the audit did allude to this, but as the auditors were conducting the audit they did interact with our staff and did identify a number of issues. And I think we felt and they felt, in some situations, and it references it in the audit, that they wanted us to get going on fixing a very significant problem quickly. And in the same vein, I think, we heard the issues that were being identified as the audit was proceeding and felt we needed to act and not wait for the formal report to come out before we took some action, and I think that was really the basis of the starting of the position. When an audit comes in it really does get you to reflect on what's going on in the organization and what steps, and I think it just identified the need as well as what the auditor pointed out in the report. But I think we clearly felt that it was a valid issue that we needed to start getting on with.

Mr. Ewasko: Just a quick comment, Mr. Chair.

Thank you, Deputy Minister, for that answer. There, for a little bit I was wondering about the fantastic foresight you had.

Mr. Pedersen: Mr. Chairman, and I'll sort of preface it by being that I am a low-tech person; I am not a high-tech person. So I have a lot of trouble keeping up with a lot of this.

But–and we know that the technology just continues to change almost daily, and you have a security analyst hired now to do this. Is there–with smartphones and things like smartphones and memory sticks and that, is–what do you do on the ground for staff that's coming in? Is–does that pose a threat with the new technology that people just carry on themselves these days? And how do you address that?

Mr. Sussman: I think the policies, I think, address that. I think some of the standards that the audit recommended that we put in place essentially mean that if they walk in with a smartphone or some other device and try to access the network, that they would be prevented from accessing it.

So I think–but having said that, I think that is, I think, the basis of the threat assessments and the risk assessments and the need to be current on those and not to just do it once and then if there's no changes, just rely–I think the point that we needed to do this on an ongoing basis is been an important one and as new technology emerges, I think we are in touch with the vendors and there are software updates and there are patches that come up and we're trying to be as current with those as possible, and there is a process of making sure that we get those and implement them.

Mr. Pedersen: Then I'll ask sort of the same question, then, to the Auditor General, is with technology changing basically daily, is this–is the wireless networks of WRHA–Manitoba eHealth at risk with new technology?

Ms. Bellringer: I'll make a general comment on this. If you need any technical specifics, we'll hand it over to Doug.

When we designed the audit, two things are relevant within the context of the way that we went about looking at this that I think answer that in part. We looked at IT generally, and then you'll–that–which is where you'll see the recommendations which would capture anything, from something that's not wireless to being wireless to being a hand-held device. Anything that's within the entire information technology world we're assuming would be captured in the overall, overarching policies for IT.

We then looked at specifically wireless. So we were looking in that for about–for two things: what were we finding at the date of the audit and what was in place to make sure that it was maintained on a current basis. So when we were saying things like, there was a policy but it wasn't being updated, we're looking not just that it's there, but that there is a regular mechanism in place to make sure that it does indeed stay up to date as you're suggesting, and that's where you'll see various findings in different areas as to–there were areas that needed improvement with regards to that update in particular.

Mr. Chairperson: Mr. Pedersen.

Mr. Pedersen: Oh, sorry. We'll defer to–

Mr. Chairperson: Okay, Mr. Friesen.

Mr. Cameron Friesen (Morden-Winkler): Thank you to the deputy minister for providing this information today. Just had a question related to the deputy minister's statements earlier about the hiring of both a risk manager and a senior security analyst to oversee specific areas of responsibility to respond to the Auditor General's concerns. I was wondering, at this time, does the deputy minister understand that these two new hires will be sufficient to address the concerns identified by the Auditor General, or do you anticipate there still could be subsequent hirings of senior IT people to assist?

***** (14:40)

Mr. Sussman: I think we viewed these as significant improvement or positions that would help in the process, but this–these two positions or additional positions won't address the findings of the audit. It has to be a comprehensive approach that eHealth and the WRHA and the regional health authorities and the department all take responsibility for. So they will be leaders or–in that process, but it–the span of responsibility is much broader than them.

But we think that these are some key areas that needed to be addressed that were shortcomings, but we don't anticipate that to implement the recommendations that we would need to bring on additional staff beyond that at this point, certainly.

Mr. Friesen: Just further to that, my colleague made the comment earlier this afternoon about how these decisions in the WRHA would work their way out into the other RHAs. And we understand that the whole system right now is in transition with RHAs combining 'apross'–across the province of Manitoba.

In any case, do you have a timeline in mind by which you would like to see those new RHAs completely aware of what's gone on here with the WRHA and completely able. With those IT managers in those locations, that you will have a high degree of confidence in their understanding of these issues and their addressing these issues? Do you have a kind of an end date in mind for when you would like to see that accomplished?

Mr. Sussman: We're looking to see significant progress of the rollout of the amalgamations during the course of this year. So–and we've signalled very clearly that we were going to have one IT kind of standard, one kind of IT policies for the province, and so the CEOs have been made aware that this was the direction that we're moving in. They've been–the information has been shared with them. We're in that process now of trying to work with them on how does this–how do the structures work on the ground with Manitoba eHealth, with the department, but I anticipate that we will see significant progress during the course of this year.

Mr. Friesen: I thank you for that response. And just further to that, would I understand correctly then that each new RHA would have its own senior IT administrator who would then work in conjunction with an overall IT director within the framework of the department?

Mr. Sussman: Different titles, but I think that concept is exactly what we're looking at. That ultimately Manitoba is too–it's not big enough to have multiple, large systems in place in health care, and so I think we are looking to have a provincial approach to all of our IT investments. And the health systems that we implement, we are looking to implement province-wide, and there may be differences to reflect the difference in size, but, essentially, we're having–we're trying to standardize across the province and benefit from the economies of scale. With–you know, if you have five different systems, you don't get any of that scale.

Mr. Friesen: Thank you for that response. You indicated that it would be different title but I was definitely on to something there. Could you provide for us, just for this committee, what would be the title that would be assigned to some kind of senior IT administrator within an RHA?

Mr. Sussman: There's been a variety, and so we're–they're currently working some of those out. We–there have been CIOs in virtually all of the regional health authorities prior to the merger, or directors,

depending on the size. Those, I think, would still be there. In some situations they may be combined with a VP role; it would depend. But we have given pretty clear direction that their IT systems, their development of ITs have to be consistent and co-ordinated with Manitoba eHealth.

Mr. Friesen: Mr. Chair, I'm going to confess, along with another of my colleagues, that I don't have a great deal of expertise in this area. But I wanted to ask a general question and ask the deputy minister if he could comment on what additional challenge is presented because of Manitoba's vast geography. And whether, you know, just because of the availability of networks and wireless capabilities and the speed of Internet access and things like that, is that a complicating factor in all of this in bringing controls–overarching controls? Does it make it easier or more difficult, or is it a challenge at all?

Mr. Sussman: The biggest challenge is really the people and skills in more of the more remote parts of the province. I think that's going to be the biggest challenge. I think the–there are infrastructure challenges, but I think the network bandwidth presents a challenge, particularly if you look at the development of–I'm trying to think of a way to describe it, that–for doing scans and diagnostics. Thank you. For diagnostics, the size of the information that is shared puts some challenges on the bandwidth in real time. And so–but I think that sort of–that really is the reason, I think. But between some of those issues and the people skills, I think that is part of the driver for us, having a provincial approach rather than leaving it to regions to try and figure this out on their own.

Mr. Friesen: Thanks for that response. I actually heard some anecdotal evidence exactly on that type of thing this week, where the challenge was for one particular region is that they were trying to access and send test results from a hospital to a clinic, and they're running into challenges in terms of the bandwidth being able to accommodate this. And I know you're somewhat limited by the bandwidth that is available within a region. So it's exactly on that same topic that you were talking about.

And I can understand how, then, when you're sending such sensitive information, you have to be doubly and triply sure that you can first ascertain that it will be securely passed through that. Is that also something that's–that was directly addressed within the scope of this audit, or something that you worked on, is that ability to relay test results and information from one location to another in a–improve the security in the way you do so?

***** (14:50)

Mr. Sussman: So, I think right now we are using other techniques to help deal with that. We are using telehealth to try and deal with some of those people and skill issues. I think as bandwidth expands throughout the province, we're going to use that to help enhance the services. The security of the information that's being sent is paramount and really that wasn't in the scope of this audit, but, certainly, it has been of paramount concern throughout the development of a provincial approach.

Mr. Friesen: I have another question and I'm not sure if it would be better directed to the Auditor General or to the deputy minister, but it just has to do with–well, perhaps, to the Auditor General first. I just wanted to know if your decision to address this area of wireless information technology, if it was predicated at all on any known attacks on the health information systems, whether it had come to your attention that there were any co-ordinated or specific attacks and whether at any time the databases had been compromised.

Ms. Bellringer: No, we hadn't had any complaints brought to us. There was nothing that actually triggered it other than our own risk assessment. Of all of the various areas within the IT world that we could select, we selected these. We have a couple of–on our list in our operations report that you'll see that are in progress at the moment that are more central, and we're always putting a plan together for that. So it was just part of that planning.

Mr. Friesen: And then a subsequent question just to the deputy minister. In the time since the department has begun to address these things and to improve its systems with respect to information technologies, have you become aware of any co-ordinated or malicious attempts to glean and gather information in any way? Has data been compromised? Have you become aware of attempts to do so?

Mr. Sussman: No, we haven't seen any co-ordinated attempt. There are viruses that come up and they're addressed, and that's sort of ongoing risks that we deal with on an ongoing basis. But we didn't–we haven't identified any co-ordinated threat or any breach that we're aware of.

Mr. Pedersen: To the Auditor General: In this fast-paced technology world where it's changing constantly there are some recommendations that

were not made public that you went directly to eHealth about just for safety-wise so that it wouldn't compromise. Can you walk us through what will happen from now on? The report will come back eventually, but just walk us through what happens with this report and the ongoing work with eHealth.

Ms. Bellringer: We'll do the formal follow-up of the report. We do it one year after the issuance. So this one will be included in the public follow-up that you'll receive in January 2014. We do the follow-up as–we call it a review as opposed to an audit. So we do limited work on making sure that those areas implemented have indeed been implemented and we do that as at June 30th, 2013. Not so much because this is more sensitive than others, but just it's been–there has been a bit of an informal ongoing dialogue just to–we've been provided with updates and so we would expect that would continue. But that would not be formally followed up until June 2013.

Mr. Chairperson: Are there any further questions for Health?

Seeing none, thank you to the Minister and Deputy Minister of Health and staff, and we will now proceed to Manitoba Lotteries.

I now call the minister responsible and the CEO of Manitoba Lotteries to the table.

Can the minister introduce his staff, please?

Hon. Steve Ashton (Minister charged with the administration of The Manitoba Lotteries Corporation Act): I will introduce with appropriate titles. Well, we have the chair–yes, the chair of the board of directors, Tannis Mindell, who many people will know from her previous role; Peter Hak, executive vice-president, Corporate Services; Rick Gilhuly, chief information officer; Marilyn Robinson, vice-president of people's services, and, of course, Winston Hodgins, who is the CEO of Manitoba Lotteries, and, of course, is now the CEO for Manitoba liquor and lotteries, which is just the working title for what will be an amalgamated Crown corporation.

Mr. Chairperson: Thank you.

Does the Auditor General wish to make an opening statement?

Ms. Bellringer: No, Mr. Chair. When I made the statement previously, I included both.

Mr. Chairperson: Thank you.

Does the CEO, Mr. Hodgins, wish to make an opening statement?

Mr. Winston Hodgins (President and Chief Executive Officer, Manitoba Lotteries Corporation): Mr. Chair, I would like to begin by thanking the committee for the invitation to provide an opening statement on Manitoba Lotteries' response to the recommendations provided to us by the Auditor General as a result of their review of our wireless network security.

Manitoba Lotteries uses several wireless networks in a variety of locations for a variety of purposes, and our wireless networks are not exclusively for access to the Internet. We do maintain wireless networks at each Winnipeg casino for guests to access the Internet, and these are similar to the Wi-Fi systems you see in airports and restaurants and have become common and expected in the hospitality industry.

We have a very mobile workforce and have several offices. Therefore, it is important to facilitate flexible access to information and technology tools for our employees. For this reason, we maintain a wireless network for staff to access work files and general applications, and separate networks for those who require access to unique, specific applications and a couple of examples of that would be for purchasing and club-card administration. We also have a network exclusively for our board members as well. Maintaining these separate networks enhances our wireless network security, and that access is only available to each network for specific producers and that limits the exposure for each of the networks. The audit also included an assessment of a network used by casino security staff for radio communications, and I just want to mention to the committee that that communication network has since been decommissioned. Manitoba Lotteries does not use wireless networks for any gaming or other highly sensitive applications such as payroll.

We welcome the office of the Auditor General's review and recommendations. As a corporation, we value their critical viewpoint and constructive feedback, because Manitoba Lotteries maintains a very strong commitment to regular risk assessment and mitigation as a good business practice.

We have implemented a robust internal audit program where we audit our programs and systems from a critical perspective, placing a priority on minimizing risk to our corporation, to our assets, our employees, and our customers. We also work

regularly with our external auditors, understanding that reviews of policies, programs, and systems by third parties, those with expertise in specific areas, strengthens any good risk-management program. And we know that external auditors also lend a perspective that may identify issues not readily apparent to those in the organization.

Recommendations resulting from any review or audit are always given priority, with implementation planning including timelines and resource assessments, and those plans begin immediately upon receipt of the audit results. And our internal audit departments follow up on all recommendations to ensure that they are addressed and implemented within an appropriate timeline. If our internal audit department has concerns that any recommendations are not being addressed appropriately, they can report these matters to myself and the audit committee of the board of directors.

***** (15:00)

It is within this context and business philosophy that we received the Auditor General's audit of our wireless network security. As the Auditor General noted in a report, wireless networks present the type of security risk inherent in all information technology systems. The report also pointed out that some risks are unique to the wireless environment.

Information technology security is a very important part of Manitoba Lotteries' business and it does require active anticipation of risk as new technologies and new risks evolve, and, as a result, we do have a dedicated information security department with five full-time staff. We appreciate the broad scope of the review and have met with Doug Harold from the Auditor General's office to discuss the recommendations and our plans to address them, and his expertise and advice were valuable contributions to our implementation planning.

The Auditor General provided eight recommendations with 15 actionable items that would need to be implemented to fully and appropriately respond to the recommendations. Of the 15 items identified for further strengthened–or of the 15 items identified to further strengthen our wireless network security, Manitoba Lotteries has completed six and 'priorized' eight for completion by December, with one item slated for completion by the end of the fiscal year.

I do acknowledge that we are somewhat behind in the original timelines we gave the Auditor General for these improvements. We have unfortunately had challenges in the area of information technology staff resources when we lost a manager and a senior security technician, and these two positions did take some time to recruit.

We have, however, made significant progress addressing the Auditor General's recommendations. We have reviewed and made improvements to our policies, our processes, our technical standards and controls, our network monitoring and our employee training.

I would like to very briefly report on our progress in each of the recommendation areas.

The first recommendation noted that network vulnerability–vulnerabilities continue to emerge as time and technologies progress. We were asked to develop a process that would identify and manage these risks as they arise.

Since 2008, we have had in place an annual network security review that is conducted by an external auditor. KPMG was recently selected through a request for proposal to conduct these reviews, and prior to that, PwC conducted them. We have now added wireless network security to this annual audit and KPMG is scheduled to conduct their next audit in January.

The second recommendation was for information security policies to be reviewed regularly and for employees to be advised of policy changes. The schedule for updating all information security policies is well under way and we–and will be completed in December.

The third recommendation noted that wireless networks have their own unique vulnerabilities that are not necessarily covered by traditional information security policies. It was, therefore, recommended that we develop a separate comprehensive wireless security policy. Manitoba Lotteries is just finalizing this policy. The policy will define, among other things, procedures for monitoring and for incident handling, and this will be completed in December along with the update of all information security policies.

The fourth recommendation asked us to enhance our network security controls. These are the invisible fences, locks and security alarms which information technology professionals insist are integral to any wireless network.

The recommendations for enhancements to our existing security included improvements to our authentication server configuration and our digital certificates of authority, and this will be fully implemented in December as well. Regular testing of our firewalls will begin in December. We will be introducing a new intrusion detection system by the end of the fiscal year, with planning and preparatory work for the new application already well under way.

The Auditor General's fifth recommendation was to enhance our access point configuration stand-in– standards. The improvements we are making to our digital certificates of authority in response to the previous recommendation will address some of these concerns, and we have rectified signal leakage on all existing networks and have made it a priority consideration in developing all future networks.

The sixth recommendation was to enhance client device configuration standards, and we have reviewed and adjusted the user access rates on all employees' laptops. We are now updating these with a broader range of software patches to ensure new security issues are addressed promptly. And we have improved our encryption process. The new certificates of authority helped to address this, as well.

The seventh recommendation was to implement continuous wireless monitoring in a–in high-risk locations, as well as periodic monitoring in other locations. This helps protect against unauthorized use, and this is–this has been implemented.

The final recommendation was to ensure that all wireless network administrators are adequately trained in wireless technology, and four of our information technology staff are already trained in wireless network security, and we have scheduled training for 10 additional staff in November.

I would like to thank the committee for their attention and their time. Manitoba Lotteries is looking forward to the full implementation of all of the Auditor General's recommendations, and we are committed to ongoing enhancements of our wireless network security program, which will evolve with technology and as a result of ongoing audits and reviews.

On completion of our work to implement each of the recommendations, we will be submitting a final report to the office of the Auditor General, and would welcome any follow-up deemed appropriate by her office. Thank you.

Mr. Chairperson: Thank you, Mr. Hodgins, and thank you for the printed copy of your report. It does make it easier to figure out which questions have already been answered.

So now we have the floor open for questions. Are there any questions of the deputy minister?

Mr. Pedersen: Then, to the Auditor General, and through her to Mr. Harold, the–was this audit based on just the two casinos, or was there other operations within Lotteries that were–the audit was based on?

Ms. Bellringer: And, Mr. Chair, I'll let Mr. Harold answer that, if that's okay.

Mr. Chairperson: That's acceptable, thank you.

Mr. Doug Harold (IT Audit Principal): The audit was–the technical scanning portion of the audit was–it took place at their head offices, Milt Stegall Drive. As well as we looked at a warehouse, Manitoba Lotteries warehouse, and the two casinos, so that's where the technical scanning took place.

Mr. Pedersen: So, in Mr. Hodgins' statement he said that–if I can find it here–the–there is no wireless technology used on the casino, or gambling portion, or the games portion, and on payroll. So, obviously security is a huge issue, but other than security, what would be the draw for hackers, if I can use that term? What would be the–where would they be aiming to interfere in the operations?

Mr. Chairperson: Is that to the Auditor General?

Mr. Pedersen: Yes.

Mr. Chairperson: Madam Auditor General? *[interjection]* Okay, Mr. Harold.

Mr. Harold: Thank you. There are a variety of risks for any wireless network, and looking at a motivation is something that would be specific to the organization, so I would have to defer that to the organization to look at specific risks and threats to their business. But there are things such as denial of service. If the wireless device itself is being used for a critical business process, or a critical health care process, those are things that we would look at in the event that the service, itself, would be denied. Looking at the confidentiality of the information that goes across that network, those are things that businesses should look at, and should determine prior to allowing them over the wireless networks.

Mr. Pedersen: So, then I'll ask the same question of Mr. Hodgins, then. So what is–it's not used for gaming, it's not used for payroll, which would be

banking information and that. Where do you see the–what is your main concerns in terms of tap–if I can use that word, tapping into wireless systems?

***** (15:10)

Mr. Chairperson: Mr. Deputy Minister.

Mr. Hodgins: It's CEO, but it doesn't really matter.

Mr. Chairperson: Mr. CEO–Mr. Hodgins.

Floor Comment: Been there, done that.

Mr. Hodgins: Yes, I'm past that part in my career.

Maybe I can use an example to kind of explain it. Our staff, I could use their laptops, for example, to get in to use the Internet to get into certain applications in our main systems. And so what a hacker could do is–or somebody who's trying to get into our systems–that they could, through monitoring the wireless system, is that they could get a person's user name and they could get the password that the person's using and then that information could be used to get into our main system if we didn't have other security provisions in place.

But we just don't have, you know, user name and the password. There are other firewalls that are in place. The certificate of authorization is kind of like a–it's in the background, and what happens is when people use their laptops to go into the system they'll use their user name and their password to get access. But when they do that, this system that's in the background will check the–you know, the information that they're submitting and also the laptop that they would be using to ensure that it's properly authorized and wouldn't let them into the system if they didn't have the–you know, the proper authorizations.

So, by, you know, I guess kind of monitoring what people are doing and–through the wireless system they could get information, that if we didn't have all these additional firewalls in place, you know, could get into our main systems and really create some difficulties for us.

Mr. Pedersen: Are there–and, again, we had–you are listening in on a conversation we had with eHealth, but is there concerns about employees coming in with their own smartphones or memory sticks, that type of thing there, the technology is out there nowadays within those? Is this a problem, or how do you handle that?

Mr. Hodgins: You–I don't think–and Rick's our CIO; he can correct me if I'm wrong. But I don't think that you can ever be 100 per cent sure that somebody couldn't, you know, get into your system, but we are very, very confident that with the systems that we have in place that we can prevent that from happening.

Mr. Cullen: I want to thank Mr. Hodgins for his detailed report today as a result of the auditor's investigation.

I wonder if you would for me, just kind of take me through a little time frame here in terms of, you know, the process you've undertaken. You know, prior to the auditor's report, I assume that every–all the IT stuff was done internally, so you had a IT staff that looked after all your internal IT programs, technical issues. Is that how it was prior to the auditor's investigation?

Mr. Hodgins: Actually, we've had our external auditor in place since 2008. Prior to KPMG we had hired PWC through a request for proposal to conduct the security audits. So we've had that in place for some time. We have had an internal audit function in place that's been in, well, it's been there for many, many years. So we have had processes in place. We have a very significant information technology department–or division within our corporation that has extensive expertise.

So we've had processes and we've had resources in place for some time. So this–we haven't done that–done this simply because of the audit that was done by the Auditor General's office.

The one thing that we have done, though, certainly, and it's–and we're going to be acting on the recommendations of the auditor's report. But one of the things that we have done as a result of the auditor's report is that we've asked our external auditor to now include in their audit the audit of our wireless network security systems, which wasn't specifically identified previously, but we are having our external auditor do that now as a result of this work.

Mr. Cullen: So PwC previously, and now KPMG, they are, in terms of their external audit, looking just at your IT side of things? Are they just responsible for that in terms of this proposal?

Mr. Hodgins: Yes, they were specifically hired to do that work.

Mr. Cullen: So I just wonder what type of a contract you have with KPMG. Is it a long-term contract that

you have or is it a year-to-year contract that you have to come in and review your situation?

Mr. Hodgins: It's a three-year contract, and the audit they did in January of this year was the first year of that contract so there's two years left and their next audit is scheduled for January of '13.

Mr. Cullen: So just to be clear then, they will supply you an audit on an annual basis?

Mr. Hodgins: And I would add that when that contract matures that we will be going back to the market to either–you know, to hire KPMG to do this work, or, you know, through a competitive process we'll hire some other company that has the appropriate skill sets to be able to provide that service to us.

Mr. Cullen: Does the audit–that group, KPMG, of this point in time, do they report to the audit committee of the board or who do they report to?

Mr. Hodgins: They were contracted by our internal audit department so that there's some separation of responsibilities here. So they were not hired by our IT department. They were hired by our internal audit department, and the internal audit department reports to the audit committee of our board of directors.

Mr. Cullen: I appreciate that response. In your report, you talked about the decommissioning of one of the–I guess, an external system. Could you explain that a little bit further?

Mr. Hodgins: Our security staff, one of the important elements of fulfilling their responsibilities is communication, and they have to be able to communicate, you know, amongst themselves. Our staff have to be able to communicate with them. We were using a radio system, and I can't just remember the years now, but maybe you can remember, Peter or Rick, but we were using a radio communication system, and then we moved to a new technology. And it was–we moved to that new technology because we felt that it was going to be able to enhance the communication. It turned out that that was not the case. That, you know, it wasn't serving the purpose that it was intended, so we have now moved back to a radio system as opposed to the system that we were using previously. So the wireless system that we were using has been decommissioned as a result of, you know, it just wasn't working successfully.

Mr. Cullen: In this system we're talking about that was decommissioned, was that a system that was, you know, totally contained within the buildings, the casinos, or was it something that was also accessible external to the buildings?

Mr. Hodgins: It was a system that was being used both internal to the casinos, but it was also being used externally as well.

Mr. Cullen: There's some indication that there were some issues pertaining to, I guess we could use the term leakage external to the casinos? Are you comfortable those particular issues have been addressed, and is that part of that decommissioning program that you undertook?

Mr. Hodgins: It was–the leakage issue, which really related to both, it was to the, you know, the communication system being used by security staff, but it was for the other wireless systems, as well, and the strength of the signals was too strong. And I think the recommendation was made that we should reduce the strength and redirect the signal so that it was–the system had more limited range. And so, those problems have been rectified now.

Mr. Cullen: In your report, you used the term intrusion detection. You're going to enhance your intrusion detection capability. Could you explain that term a little more in depth?

***** (15:20)

Mr. Hodgins: I'll do my best to explain this. There's technology that we're currently going to be–well, we're working on putting in place. And what this software will do will it will monitor our wireless–*[interjection]*–this software will monitor all traffic that is coming into our systems and if there's someone trying to access our system that should not then it will alert our people that we're having somebody trying to break into our system. So this is new technology that we're implementing in our system. So hopefully that answers your question.

Mr. Cullen: Yes, thank you, I do appreciate that, Mr. Hodgins.

I guess the other question, too, and it goes back to–and we can design these foolproof systems or we try to design foolproof systems. At the end of the day that really relies on the people that are using those particular systems, and I'm just wondering what type of provisions you have allowed to, kind of, be a

watchdog, if you will, for the individuals working within the corporation.

Mr. Hodgins: We have some very extensive provisions within the corporation to monitor access to the systems that we have, and I'll just use one as an example. Our payroll system, for example, I know that, you know, it doesn't involve the wireless technology, but our payroll system–there is very, very limited access to the payroll information. And if there's someone that wants information out of our payroll system the only way that–that hasn't been approved to obtain information–the only way they can get information out of that system is with the approval of our vice-president.

And so we have both technology in place, plus we also have processes in places to protect the, you know, the integrity of the information in our system. And so, you know, we're constantly monitoring the, you know, the technology we have to enhance it to make sure that it's as secure as possible.

Mr. Gilhuly is our chief information officer and he has a–I think, you know, we have a reasonably large IT division within our corporation that is actively monitoring and upgrading, you know, any of the software that we have in our organization. So it's both from a technology perspective and process perspective. But we do a lot of training in our organization, as well, to ensure that our staff, you know, are aware of what their responsibilities are. For the critical policies that we have in place staff have to sign a document that they have reviewed and understand them after they've gone through a training program so that, you know, we ensure that, you know, as much as possible, they'll, you know, that they're going to help to protect that information as well.

Mr. Cullen: And just to conclude, I want to–just want to thank Mr. Hodgins for his answers and his thorough presentation today. Thank you very much for that.

Mr. Pedersen: Well, if–Mr. Chair, if I can ask, through you to the Auditor General, just give us the background, then, of what will happen as a–on an ongoing basis so we have it on the record here.

Ms. Bellringer: This–the process for this would be identical to that for eHealth and we will be following it up and it will be included in the January 2014 report.

Mr. Chairperson: Are there any further questions?

Mr. Matt Wiebe (Concordia): Yes, just a bit more of a technical question, once again, so, you know, if you can do your best to answer.

But just with regards to access point configuration standards, I'm just wondering, as those become more stringent and there's more of a restriction on, I guess, on the technology in terms of what can access or the types of devices that can access the networks, I'm wondering if that's put any kind of–if that's hampered in any way the implementation of new technologies like tablets or smartphones. And, also, going forward as Wi-Fi or wireless networks become more widely used and implemented, and perhaps new ones are created within the organization, whether there would be any kind of, again, a hampering of implementing those because of the stringent requirements of the technology.

Mr. Hodgins: I guess just a couple of things that I would mention to you. We have not had any serious issues in terms of being able to implement, you know, any of the wireless technology systems that, you know–that we have in place, and at this point in time we're not really anticipating that we're going to have any.

The approach that we do take with the implementation of wireless technology is that we set up separate systems–separate stand-alone systems for our wireless network applications, so it's not like one large system. So I mentioned to you in my comments that we have a wireless network system for our board members. We also have the Wi-Fi system that is available to the guests at our casino. So those are a couple of examples, and those are set up as individual systems. So that, I think, helps us to limit, you know, the issues that we might expect to run into by placing some of these systems and controls in place. So at this point in time we really don't feel that there's going to be any serious problems.

Mr. Chairperson: Any further questions? Seeing none, thank you to the minister and to Mr. Hodgins, CEO, for your patience in answering questions today, and now that there are no further questions, does the committee agree that we have completed consideration of Chapter 8–Wireless Network Security: Winnipeg Regional Health Authority and Manitoba eHealth; Manitoba Lotteries Corporation? *[Agreed]*

As it is agreed, thank you for your patience today for the Chair and thank you to the pages today. I understand this is one of their first outings. Well

done. And thank you, Madam Auditor General, and your staff.

So this now concludes the business before us. The hour being 3:27, what is the will of the committee?

An Honourable Member: Committee rise.

Mr. Chairperson: Before we rise, it would be appreciated if the members would leave behind any unused copies of reports so that they may be collected and reused the next meeting. Committee rise.

COMMITTEE ROSE AT: *3:27 p.m.*