Third Session – Forty-Third Legislature

of the

Legislative Assembly of Manitoba

Standing Committee on Public Accounts

Chairperson
Mr. Kelvin Goertzen
Constituency of Steinbach

Vol. LXXX No. 4 - 3 p.m., Friday, April 17, 2026

ISSN 0713-9462

MANITOBA LEGISLATIVE ASSEMBLY
Forty-Third Legislature

Member	Constituency	Political Affiliation
ASAGWARA, Uzoma, Hon.	Union Station	NDP
BALCAEN, Wayne	Brandon West	PC
BEREZA, Jeff	Portage la Prairie	PC
BLASHKO, Tyler	Lagimodière	NDP
BRAR, Diljeet	Burrows	NDP
BUSHIE, Ian, Hon.	Keewatinook	NDP
BYRAM, Jodie	Agassiz	PC
CABLE, Renée, Hon.	Southdale	NDP
CHEN, Jennifer	Fort Richmond	NDP
COMPTON, Carla	Tuxedo	NDP
COOK, Kathleen	Roblin	PC
CORBETT, Shannon	Transcona	NDP
CROSS, Billie	Seine River	NDP
DELA CRUZ, Jelynn	Radisson	NDP
DEVGAN, JD	McPhillips	NDP
EWASKO, Wayne	Lac du Bonnet	PC
FONTAINE, Nahanni, Hon.	St. Johns	NDP
GOERTZEN, Kelvin	Steinbach	PC
GUENTER, Josh	Borderland	PC
HIEBERT, Carrie	Morden-Winkler	PC
JOHNSON, Derek	Interlake-Gimli	PC
KENNEDY, Nellie, Hon.	Assiniboia	NDP
KHAN, Obby	Fort Whyte	PC
KINEW, Wab, Hon.	Fort Rouge	NDP
KING, Trevor	Lakeside	PC
KOSTYSHYN, Ron, Hon.	Dauphin	NDP
LAGASSÉ, Bob	Dawson Trail	Ind.
LAMOUREUX, Cindy	Tyndall Park	Lib.
LINDSEY, Tom, Hon.	Flin Flon	NDP
LOISELLE, Robert	St. Boniface	NDP
MALOWAY, Jim	Elmwood	NDP
MARCELINO, Malaya, Hon.	Notre Dame	NDP
MOROZ, Mike, Hon.	River Heights	NDP
MOSES, Jamie, Hon.	St. Vital	NDP
MOYES, Mike, Hon.	Riel	NDP
NARTH, Konrad	La Vérendrye	PC
NAYLOR, Lisa, Hon.	Wolseley	NDP
NESBITT, Greg	Riding Mountain	PC
OXENHAM, Logan	Kirkfield Park	NDP
PANKRATZ, David	Waverley	NDP
PERCHOTTE, Richard	Selkirk	PC
PIWNIUK, Doyle	Turtle Mountain	PC
REDHEAD, Eric	Thompson	NDP
ROBBINS, Colleen	Spruce Woods	PC
SALA, Adrien, Hon.	St. James	NDP
SANDHU, Mintu, Hon.	The Maples	NDP
SCHMIDT, Tracy, Hon.	Rossmere	NDP
SCHOTT, Rachelle	Kildonan-River East	NDP
SCHULER, Ron	Springfield-Ritchot	PC
SIMARD, Glen, Hon.	Brandon East	NDP
SMITH, Bernadette, Hon.	Point Douglas	NDP
STONE, Lauren	Midland	PC
WASYLIW, Mark	Fort Garry	Ind.
WHARTON, Jeff	Red River North	PC
WIEBE, Matt, Hon.	Concordia	NDP
WOWCHUK, Rick	Swan River	PC
Vacant	The Pas-Kameesak	

LEGISLATIVE ASSEMBLY OF MANITOBA

THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

Friday, April 17, 2026

TIME – 3 p.m.

LOCATION – Winnipeg, Manitoba

CHAIRPERSON – Mr. Kelvin Goertzen (Steinbach)

VICE-CHAIRPERSON – MLA Jim Maloway (Elmwood)

ATTENDANCE – 9 QUORUM – 6

Members of the committee present:

Mr. Brar, MLAs Chen, Compton, Dela Cruz, Devgan, Messrs. Goertzen, Guenter, MLA Maloway, Mr. Wharton

Substitutions:

Mr. Wharton for Mr. Ewasko
Mr. Guenter for Mrs. Stone

APPEARING:

Tyson Shtykalo, Auditor General

WITNESSES:

Tyler Gooch, Deputy Minister of Innovation and New Technology

Dana Rudy, Public Service Commissioner

MATTERS UNDER CONSIDERATION:

Auditor General's Report – Managing IT Security for Remote Access, dated March 2024

* * *

The Chairperson: Good afternoon. Will the Standing Committee on Public Accounts please come to order.

Committee Substitutions

The Chairperson: Before we begin with our business today, I'd like to inform the committee that we've received the following membership substitutions for this meeting only: MLA Wharton for MLA Ewasko and MLA Guenter for MLA Stone.

* * *

The Chairperson: I'd also like to table the following documents: the responses from the Department of Justice, the questions from the Standing Committee on Public Accounts meeting on efficiency of court services that was held on January 13, 2026, as well as responses from the Department of Justice to questions from the Standing Committee on Public Accounts meeting on Preparing Incarcerated Individuals for Transition from Custody that was held on January 13, 2026.

This meeting has been called to consider the following report: the Auditor General's Report, Managing IT Security for Remote Access, dated March 2024.

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

MLA Jim Maloway (Elmwood): Mr. Chair, I suggest we sit for an hour and then revisit at that time.

The Chairperson: MLA Maloway has suggested we sit for one hour and then revisit at that time.

Is that agreed? *[Agreed]*

I'd like to also ask the committee if there is leave for all witnesses in attendance to speak and answer questions on the record if desired. Is that agreed? *[Agreed]*

I'd also like to remind everyone that questions and comments must be put through the Chair using third-person vernacular as opposed to directly to members and witnesses.

Before we proceed further, I'd like to inform all in attendance of the process that is undertaken with regard to outstanding questions. At the end of every meeting, the research clerk reviews the Hansard for any outstanding questions that the witness commits to provide an answer to and will draft a questions-pending-response document to be sent to the deputy minister or other witnesses. Upon receipt of the answers to those questions, the research clerk then forwards the responses to every PAC member and to every other member recorded as attending that meeting.

With that out of the way, does the Auditor General wish to make an opening statement?

Mr. Tyson Shtykalo (Auditor General): I'd first like to introduce staff members I have with me today.

Today I'm joined by Assistant Auditor General Wade Bo-Maguire and Audit Principal Ian Montefrio.

Mr. Chair, the COVID-19 pandemic transformed the traditional workplace structure. Employees across many sectors learned to work remotely or to divide their time between home and the office. Advances in technology made this shift possible, providing new ways for employees to access and share information and collaborate from outside traditional office settings.

In response, the Province of Manitoba introduced a flexible work arrangements policy for its core public service employees in June of 2021. The policy formalized expectations for employees working remotely, whether full time or in a hybrid arrangement. It also recognized the need for strong IT security controls in the work–remote work environment to ensure that information remains safe regardless of location.

We conducted this audit to determine whether the Province had appropriate processes and controls in place to mitigate IT security risks in the remote work environment.

We concluded that the Province is managing IT security risks associated with remote work, but some improvements are needed. Overall, we found the Province had implemented several important controls to protect its systems and data. Specifically, data transmitted in the remote work environment was encrypted, access to devices was controlled through multi-factor authentication and systems were regularly patched and monitored for vulnerabilities. However, we identified several areas where improvements were required.

First, we found that, while data was encrypted, some encryption settings did not fully meet provincial standards and could be strengthened. Second, mandatory information security awareness training had not been completed by a significant number of employees. As of March 31, 2023, nearly one third of employees had not completed this required training, even though it is a key defence against cyber threats such as phishing and social engineering. Finally, several IT security policies and procedures had not been updated in many years and no longer reflected current technologies or risks, including those related to remote work.

This report includes three recommendations. These recommendations focus on strengthening encryption settings, improving completion and enforcement of mandatory security awareness training and ensuring IT security policies and procedures are regularly reviewed, updated and supported by appropriate training. The departments responsible agreed with our recommendations and indicated that actions are planned or already under way. Our first follow up on these recommendations will take place in the fall of this year.

I'd like to thank the government officials and staff for their co-operation and assistance throughout the audit. I would also like to thank my audit team for their professionalism and hard work in completing this report.

This concludes my opening remarks. I look forward to the discussion on the report today.

The Chairperson: Thank the Auditor General for the opening statement and the work on this particular report.

Does the deputy minister wish to make an opening statement? And if they do, could you please introduce your staff prior to the opening statement?

Mr. Tyler Gooch (Deputy Minister of Innovation and New Technology): Thank you, Mr. Chair and members of the committee, for the opportunity to appear today. I'd like to introduce Jaime Burbank, the assistant deputy minister of IT risk and cybersecurity. I'm also joined by Public Service Commissioner, Dana Rudy. *[interjection]*

The Chairperson: Sorry, I just need to turn on your mic by recognizing you, so please proceed.

Ms. Dana Rudy (Public Service Commissioner): My name is Dana Rudy, Public Service Commissioner, and I have with me today–

The Chairperson: Minister of Public Service Commission. Go ahead.

Ms. Rudy: And I have with me today Ana Frias Mira, who's our director of strategic and corporate services.

Mr. Gooch: This report examined how the Province managed information security risks associated with remote access from June 20–or 2021 to June 2023. Remote access is a standard operating practice for government and business today. It enables departments to deliver services to Manitobans at any time, from anywhere, increasing the resiliency and responsiveness of public services. At the same time, it requires strong and continuously evolving security controls to protect government systems and Manitobans' data.

The Auditor General's report concluded that the Province is managing the security risks associated with remote access and identified three recommendations to improve encryption settings, completion of mandatory training and ensuring security policies and procedures remain current. The department accepted these recommendations and has been working to address them. The Province has implemented several foundational controls that support secure remote access. Remote users access government systems using Province-issued managed devices.

Access to those devices is protected with multi-factor authentication and automated patch management, which ensures security updates are applied regularly. Security monitoring and vulnerability management processes are also in place to identify and respond to threats affecting remote access technologies.

Since the time of the audit, further improvements have been made to strengthen our overall cybersecurity posture. We have reviewed encryption configurations against security standards, enhanced governance processes for security policies and procedures and strengthened oversight of security awareness training across the organization.

These initiatives are part of ongoing continuous improvement of our cybersecurity. It is important to recognize that cybersecurity is not a static objective. Threats evolve continuously, and the controls used to protect government systems must evolve with them. Our work is not only focused on addressing the specific findings of this report, but on strengthening the overall security framework that supports digital public services.

The department appreciates the work of the Auditor General and the constructive recommendations provided in this report. They have contributed to ongoing improvements in how the Province manages cybersecurity risks related to remote access.

The Chairperson: Thank the deputy minister and I thank the Public Service Commissioner.

The floor is now open for questions from members of the committee.

MLA Carla Compton (Tuxedo): I have a question around the mandatory training. And I guess–and maybe the number is different now, but what I read is it said that there's still 31 per cent not completed or not completing in a timely manner.

***** (15:10)

And I'm wondering if–whether it's the deputy minister or one of the other folks that are here today–could clarify: (1) Is that number still accurate; and (2) What is the plan to remedy that–or resolve that?

Because I know, myself, coming from a health-care background, you know, there's important trainings around safety, security, PHIA training, for example. Our own cybersecurity training, that is essential, and there were things in place to make sure that it didn't just fall by the wayside.

And we know, especially in this day and age, cybersecurity is becoming more and more of a concern. And we want to ensure that–we say it's important, that we value ensuring the safety and security of all the data, people's data, so what are we doing to ensure that that value is being upheld and implemented in a timely manner within the folks who work for us and for Manitobans?

The Chairperson: Thank you, MLA Compton.

Ms. Rudy: Thank you very much for the question.

As reported by the OAG, in 2023, there were 31 per cent of public servants that had not completed the course. And I'm pleased to share that as of March 31, 2026, it's 12.5 per cent of the public service that has not yet completed it. And I just want to comment that that would be active employees, including staff that had just recently began in their role as well as those that may be on leave for a variety of different reasons as well.

The Chairperson: Follow-up, MLA Compton?

MLA Compton: Just a quick follow-up. So is there a specific policy or, like, a time threshold, for example, if within your systems or whatnot that it might get flagged for, say, a new staff, for example, if they've exceeded the time frame, the preferable time frame, for them to have it completed? What are the mechanisms–or what mechanism is there in place to catch that before, you know, it's six months or a year has passed?

Ms. Rudy: So, at this point in time, our employees are expected to complete all mandatory training within six weeks of being hired, and there is an onboarding process that is done. Most departments encourage staff to do that in the early days of their employment, given the volume of activity hasn't necessarily started. And many have started to build it in as part of corporate orientation for new hires.

Each month, each department receives a detailed report outlining the completion and non-completion rates for every staff. And they also have access to the talent analytics dashboard so that they can go in and retrieve information. We've built the review of the completion of mandatory courses as part of the probationary period as well, as there's a required form that needs to be completed, so that they can, again, attest to whether they've completed the mandatory training.

And then, on an annual basis, staff are required to participate in a performance development conversation with their supervisor. And in that form as well, it details the completion of mandatory training. And when it hasn't occurred, then management and staff are working together to develop a plan to ensure that that is completed.

MLA JD Devgan (McPhillips): Actually, that was my question, and every one of my questions were answered, so I'm good.

The Chairperson: Should be that way during questioning period.

Other questions?

MLA Jennifer Chen (Fort Richmond): My question is mostly around recommendation 3 in the report, on page 18, as the table listed a number of outdated documentation.

So my question is: What are the steps being taken by DTS to ensure an annual review of the identified outdated policies, procedures and guidelines?

Mr. Gooch: So DTS has, in light of this recommendation, taken several steps to ensure that our security, policies and controls remain up to date. In fact, we are doing a full review of all security controls. We created the chief information security officer position in part to strengthen our capabilities and ability to deliver on IT risk management practices, not only operational cybersecurity but also risk assessments and management plans and the development of the associated controls, policies and practices that are required to protect public information.

So, yes, in short, the answer is that we are going through a process right now of redeveloping every policy practice and reapproving them with effective governance over the next 18 months or so.

The Chairperson: Follow-up, MLA Chen?

MLA Chen: Yes, a follow-up question.

So, on page 18, among all this documentation, what is the current status for this documentation? Have they been updated as–there's a last updated years for these documents? And are those still stand or some have been updated?

Mr. Gooch: So, as we put in the new governance approach, we put in a formal approval process. So these have not gone through that formal approval process yet. When–we wouldn't–when the auditor comes in to review this, we wouldn't put these forward as having been updated in that regard. But we are working on them, and, in practice, we are implementing improvements to them.

MLA Jelynn Dela Cruz (Radisson): I would like to express my gratitude to the witnesses who are here today. These folks are doing incredible work trying to keep up with the pace at which technology is evolving and artificial intelligence is changing our digital communications.

And on, I guess, on page 16–just to pivot to the question that I had here–it states that the service desk is the one that handles–or the central office that handles the incident management process for IT security incidents.

So, with timely action in mind, what metrics does the department track to evaluate the efficiency and effectiveness of that office, the service desk, in responding and resolving security incidents related to remote access technologies?

Mr. Gooch: Yes, the service desk does co-ordinate our incident management processes, including cybersecurity incidents.

The majority of cybersecurity incidents are identified by systems monitoring and reporting to the service desk. So there is a fairly robust practice around measuring and reporting those internally. I personally receive a monthly report identifying any incidents that have been identified by the service desk or through the automated monitoring processes and any remediation actions that have been taken for identified incidents.

The Chairperson: Follow-up, MLA Dela Cruz?

MLA Dela Cruz: Yes, to follow up on that, then, when it comes to these metrics specifically, my hope is that, since the report was first released, that the metrics will be able to paint a picture of the progress that has been made since the report has been released and the plan has been put in place by the department.

And so I'm wondering what changes our witnesses can identify since the report?

Mr. Gooch: With the context that I've only been in this role for a year and I don't have the full history, what I can say is that the monthly reporting that I receive is very comprehensive, it's very detailed and it meets the highest standards that I would expect for reporting on cybersecurity incidents and remediation efforts.

The Chairperson: We'll just allow another follow-up from MLA Dela Cruz before we go to MLA Brar.

MLA Dela Cruz: I think what I'm–what I was trying to get at with that is whether there are any trends in the metrics, in the data that's been reported through the service desk and the types of things that are being identified?

Mr. Gooch: Yes, thank you. I understand more fully what you're getting at.

***** (15:20)

There is an ongoing and continuous trend of increasing cyber threats and attacks. What I would say is that successful cybersecurity incidents are minimal to none in a typical monthly report, and so that trend is very positive in that it demonstrates that our controls are working.

Mr. Diljeet Brar (Burrows): I want to say thank you to the AG office and the department for all the good work you're doing and identification and implementation of these important issues in the department.

My question would be regarding the reorganization of the department, how this change has impacted your ability to implement those recommendations in positive, negative way.

Mr. Gooch: By escalating the responsibility for cybersecurity to an assistant deputy minister level, we've increased the visibility of both the deputy minister's office and the minister's office into cybersecurity issues and incidents, as well as, I think, communications across the organization at the department-head level.

We've also been able to add a few resources that are specific to IT risk management, which is a separate practice from day-to-day operations of cybersecurity systems, so these are folks that are thinking about cybersecurity from a public service lens and the risks to public service delivery and public service operations and helping to manage management action plans and address the risks in audits like this.

The Chairperson: Follow-up, MLA Brar?

Mr. Brar: Are there any specific barriers that the department has identified in implementation of these recommendations so far?

Mr. Gooch: The short answer is no. These recommendations are aligned with industry best practices. They're aligned with good management, and we haven't experienced any barriers in implementing the recommendations.

The Chairperson: Another follow-up MLA Brar?

Mr. Brar: What would be the expected timeline to implement all the recommendations on this report?

Mr. Gooch: Yes, in terms of the encryption recommendation, I would say–we haven't had the auditor back in to confirm this–but I would say that we have fully implemented that recommendation. I'd also say, based on the significant improvement in the training–mandatory training rates, that I would put forward that we have implemented that recommendation as well. And the third, as I mentioned earlier, we're doing a full review of our security policies and control framework. And that's projected for the end of 2027.

The Chairperson: Can I do a follow-up question to the Public Service Commissioner? You'd indicated, I think, if I heard correctly–and I missed–I'm sorry–part of the opening comments. I'm used to people shouting in this Chamber, so I may have not heard you correctly.

But about 13 per cent or so were now non-compliant with the mandatory training, and some of those just might be early on, you know, hire. Is that sort of the rate that the Public Service Commission considers to be transitory rate or an acceptable rate for waiting for mandatory training?

Ms. Rudy: Yes, I think we're very satisfied with the number that we have before us right now. We continue to try to make improvements across the board in all of our mandatory training.

The goal is to achieve at least 80 per cent of a baseline, just given the changes to staffing on a continuous and ongoing basis. And the improvements that we're making through monthly reporting to departments have proven to be successful. But we continue to explore other strategies around escalation by having direct conversations between our Public Service Commission and the managers within departments.

The Chairperson: And there are other mandatory training courses, I believe, throughout the public service.

Is the process to ensure that folks are doing the training the same as you've implemented for this particular mandatory training? So, you know, there's sensitivity training or other kinds of training there. Is it the same sort of process to ensure that people are doing the mandatory training in different courses throughout the public service? *[interjection]*

The Chairperson: Sorry. Public Service Commissioner.

Ms. Rudy: All of our mandatory training is reported in the same way, and managers have access to those monthly reports, whether it's our anti-racism training or truth and reconciliation modules. And they have the ability to retrieve the information from the Talent Analytics Dashboard as well.

The Chairperson: And you may not have the information in front of you. Maybe you can provide it to the committee, but would–with the compliance rate, for lack of a better word, be similar among those different mandatory trainings, as you described for the IT training today?

Ms. Rudy: The compliance rate for the information security course is the highest.

The Chairperson: Could you provide for the committee the compliance rate for the other mandatory courses that are required through the public service?

Ms. Rudy: Yes, we can, and we report our rates of completion in our annual reports, but we're happy to provide the more recent data as of March 31, 2026.

The Chairperson: I thank you.

MLA Dela Cruz: Just to build off of the previous question, actually, I'm wondering if the commissioner would be able to provide a high-level understanding for the committee on, you know, what departments may be more challenged than others when it comes to the completion rates of the mandatory trainings, but as well, like, what some of those challenges might be compared to other departments.

Ms. Rudy: So if I heard the question correctly, it's looking at the challenges departments experience in ensuring that staff complete the mandatory training.

There are a number of departments that have a significant number of staff that are in operating front-line roles that don't access or interface with computers on a day-to-day basis. I would say that is the largest challenge.

Furthermore, in some of our operations where we have 24-7 staffing models, it is challenging to schedule time for staff to participate online–in an online training and, frankly, an in-person training as well.

So we have some large departments that have operational roles including Transportation and Infrastructure, Justice, the Department of Families, and we see the opportunity to increase our compliance through engagement with managers. And I've seen evidence that there's strong support for ensuring that mandatory training is taking place. And in Justice, for example, staff are scheduled in to complete those mandatory training.

The Chairperson: So we'll go to MLA Maloway for a series of questions, then MLA Compton and then MLA Chen.

MLA Maloway, you have the floor.

MLA Maloway: I think my questions should be directed to the chief information security officer–or the deputy, but I think the chief information security officer.

You know, I understand the EU just recently announced that they are moving away from Microsoft. They're going to go with Linux. Is that being looked at here in Manitoba? Because there's huge cost here in dealing with Microsoft. We've been paying them a lot of money for many, many years now and as soon as we get one version in, it's practically ready–we're ready to put another one in, right? And Linux is its own operating system where it's free, right? So I'd just like to know what your comments on that would be.

The Chairperson: The chief information security– *[interjection]* Yes, I think we need you at a microphone.

Deputy Minister.

Mr. Gooch: Yes, the question of Microsoft, which is extensively used through government and business in Canada, versus open-source software like Linux. There can be benefits from using open-source software. The transition costs would be very high in terms of retraining, process review and re-engineering. So we always remain open to all of those options and are always exploring what our options are to provide the best services to Manitobans. But at this point we don't have a plan to transition off.

MLA Maloway: And my follow-up question would be regarding the use of AI. Assuming that you're using

some AI platform to check for vulnerabilities in the system–I'm assuming that's being done because, I mean, if it's not it should be.

* (15:30)

There was some announcement in the last day or two that there's some big new program developed that is picking out vulnerabilities in all the other systems. In other words, this program works on the basis that it finds a vulnerability in AI system–this AI system–in this AI system, and it works through the whole group of them.

And it's sort of like the super vulnerability nuclear option here, and so, if this is all real, we should be looking at this and making sure that we're not–that it's part of the vulnerabilities and all these big corporations are now, like, privately meeting to discuss this whole issue.

So are you people aware of this and are you doing anything about it?

Mr. Gooch: Yes, yes, we are very aware of the emerging implications of the use of generative AI for cybersecurity. The generative AI is a powerful tool that provides new capabilities to both attackers and defenders in the cybersecurity world.

So I think a lot of the recent media coverage is around using generative AI to identify vulnerabilities in software. That's part of our standard cybersecurity practice today. We use other tools, some of which have different types of technologies built into them to find those vulnerabilities, and I expect that those tools will integrate these new capabilities in short order as they come out because the protectors want to stay ahead of the defenders, and that's how–been how cybersecurity has operated for many decades.

MLA Compton: So I just want to start with a wee bit of a comment around the–what was shared around practice of, like, injustice and stuff like that, scheduling the time for the mandatory training. As someone that myself, I come from front line–being a front-line worker that often, even if there is a computer, you don't necessarily have time to sit down and do the module, and I–and when my own unit started doing things like that, it was a significant difference. So I just want to say I think that's a really good practice, because I personally experienced how it was a positive impact where I used to work.

I want to go back to the action plan and recognizing that your ministry is not very old, and I think this action plan was probably created before your existence, and from what was explained to MLA Chen in her question, I'm wondering if the procedures that you have right–that the department has right now for reviewing policy and stuff is in any way different than the action plan or if the action plan is–do you get what I mean?

Like, are you following this action plan, because there's dates here, you know. Have things been completed according to this action plan with, you know, May 2024, August 2024 or since the ministry's inception, which was after this action plan was created? Is there a different way that your department and ministry are going about achieving this? Does that make sense?

Mr. Gooch: Thank you for the question.

The action plan, like, we've looked at this action plan and agree with it conceptually. Some of the dates may, you know, not be what our current planning is, but with the creation of the new ministry, I think, and inclusion of some cybersecurity responsibilities in the mandate letter have been beneficial for us to elevate and professionalize the practice of cybersecurity for Manitoba.

The Chairperson: Follow-up, MLA Compton?

MLA Compton: So would–is there a way to revise or acknowledge that maybe the department is not wholly doing this or saying–I'm a person that likes, like, either it's resolved, it's not resolved or we're addressing it, but we're addressing it in this way now–I'm all about documentation.

Is that something that has been considered or to just say using in this new–and I realize I'm not great with words in how I'm trying to describe this right now–but this is feeling like an unresolved piece for us to be reviewing as a committee and now if–recognizing that the ministry is new and you're developing your own policies, procedures and moving forward, you know, how do we just acknowledge that this is something that's maybe leading the work you're doing–or that the department is doing, but that the guidance or the way that the actions are being taken are not exactly in how the action plan explains it?

Mr. Gooch: Yes, so the audit and the action plan are a point-in-time document. What we do with those within the department is we track all of our audit recommendations and report progress and our current plans on each of them as we proceed. And we work with the Office of the Auditor General to keep them informed periodically.

And then, at their pleasure, they can come back in and, you know evaluate, what has your progress been.

MLA Chen: I actually have two follow-up questions.

The first one is just follow-up with what MLA Compton's–where MLA Compton's question ended. This action plan, even though the ministry is new, and knowing these tentative target dates are–have passed, except for two that, I think, were completed. However, the OAG 'rependations' still–are still valid.

Hearing the department's–earlier, deputy was saying the department is developing your own reviewing–or your own, like, procedures, but the OAG's–it's still based on the OAG's recommendations, is that correct?

Mr. Gooch: Yes, so many audits have recommendations that are about technology systems. So what I was trying to say earlier was that we track all of the recommendations that are relevant for the provision of technology services. We're not updating them or adjusting them; we're just tracking our progress and making sure that we're achieving what's in those action plans.

The first two recommendations were very much acted on immediately in terms of improving the encryption settings and advancing the training for staff.

The third one around policies and procedures is probably the one that we've taken a more comprehensive view of, actually, since the department was created, in expanding the need to review all of our security policies and procedures and not just the ones on this list.

The Chairperson: Follow-up, MLA Chen?

MLA Chen: So my second question is towards PSC, because what we have–the data in the report on page 17: 31 per cent. The data, I believe it came from 2023, and hearing that PSC was saying the data given–provided an updated 13 per cent.

I'm just wondering if it's fair to say that remote working was one of the contributing reasons that employees–that have a higher number of employees that did not complete the required training. And now with employees return to office in person, the percentage of completed training increased, and if employees are ever going back to remote working for any reason, would that number of not completing training go up again?

Ms. Rudy: So I don't anticipate that the direct impact is–like, the association between remote work and the completion of the of the training. I think that I would attribute our increased compliance to the escalation procedures that the department has implemented, as well as the attention to completion rates across all of our government departments.

The Chairperson: Maybe following up on MLA Chen's question, obviously there would have been–or maybe not obviously–there would have been a significantly higher number of folks on remote work during and then slightly after the pandemic. It feels like more and more people are returning to in-person or maybe a hybrid model of working.

Do you know the number in the public service of how many people would be classified as working remotely?

***** (15:40)

Ms. Rudy: I'd have to get back to you on the exact percentage at this point in time, but we tend to track the number of employees that have remote work arrangements documented as part of our flexible work arrangements policy.

The Chairperson: So I took that to be a commitment to return with that number to the committee.

Do you have a general sense of that number's trending down or up because of technology changes, or is static? And if you don't have a general number, then I'll just await the real numbers.

Ms. Rudy: I don't want to really make a guess at this point in time. I would say that over the course of–since the pandemic, more staff are working in the office than were at the very end of the pandemic, as our policies have shifted to ensure that employees are in the office at least three days a week as part of our flexible work arrangements policy.

And then, over time, the number of positions that we have that haven't had a significant impact by remote work because of the operational nature of the role, there hasn't been significant change in those areas.

The Chairperson: Okay, and I appreciate you don't want to, sort of, speculate, but if you can provide maybe a three-year window from this year and the two years past, so, how many are registered in the civil services working remotely, that'd be great.

MLA Devgan: Actually, that was kind of where I wanted to go with my question, but I think the number

was 12-something per cent now, but down from one third, so 31 per cent.

I guess, then, I'll ask this question in a different way: How much of an impact did the–sort of, your natural churn in the public service following the pandemic impact these numbers? Like, is this just a higher uptick of people complying with these training requirements, or is this just a reduction in the work-force that led to you with more people complying?

Ms. Rudy: Yes, we calculate the completion rate based on the number of staff that have completed it relative to the total number, so the size of the public service wouldn't necessarily change, although the size of the public service has increased.

I would say that the completion rates are directly associated to the efforts that departments make.

The Chairperson: Follow up, MLA Devgan–go ahead.

MLA Devgan: Okay, so now we've obviously got more people complying with the training. My question is not directly related to anything in the AG report but that of my own curiosity. We could come down to even, like, a lower number, like 5 per cent total, but it takes one person to answer an email and for something to go wrong.

Are you using AI in any way, shape or form to buttress some of this–some of these protective measures that we're taking to prevent hacking or any sort of threats externally?

Mr. Gooch: Yes, we have a fairly comprehensive suite of cybersecurity tools to monitor for those types of incidents. We also provide regular anti-phishing tests to employees to keep awareness high on an ongoing basis, and those that fail the test are, you know, encouraged to take the training again. But the technical controls to monitor for loss of data or suspicious network activity are pretty extensive and they're from industry-leading vendors.

The Chairperson: Just prior to the next question, I'd just remind questioners and respondents to put the questions through the Chair.

Mr. Brar: Our committee thinks alike. A part of my question has been stolen, so–which is a good sign; we think alike.

My question–original question was, like, how the number of employees working remotely in public service–it was around 3,500 or so between 2022 and 2023–has changed over time until date.

And my additional question to this is: Is the government saving any money by these changes? Saving or losing money? Like, how is that related? I don't know how much is this related to the report itself, but just curious to know, more people working remotely, is it better for the public purse? Do we have any idea?

The Chairperson: So I think the first question will probably be answered by the statistics that the Commissioner of the Public Service are committed to provide us.

But there was an additional question regarding savings, and who would like to–Deputy Minister.

Mr. Gooch: Yes, I would–I'd like to–thank you, Chair–I'd like to sort of make a comment that remote access isn't only for hybrid workers. Government employees that are fully in the office do work outside of the network. And so these tools are necessary and there's no real incremental costs from providing the tools for work that happens outside of the network.

The Chairperson: Are there statistics kept–and I suppose this is for the deputy minister–on attacks that happen with–on government, core government, I suppose, you might not have the Crowns or maybe you do, on cyberattacks that happen within the core of government or the Crown corporations? Are they documented in terms of the number of cyberattacks that happen; are they published in any way?

Mr. Gooch: We do track the number of attacks internally. We don't publish those publicly today; that's for core government. The Crowns are not currently reporting into core government their attacks; I would expect that they do track them internally as well.

The Chairperson: Could that, obviously on a–not on a specific basis in terms of the nature of the attacks, maybe, but could the metadata be provided in terms of the yearly attacks that core of government faces, you know, from one year to the next?

Mr. Gooch: Yes, and I would say that academic researchers do publish general information. Govern-ment's, you know, sort of high level information about the number and types of attacks that government experiences, I think would be public information that could be published. We're not doing that today.

The Chairperson: Could you provide for the committee sort of a two-year perspective maybe, or a three-year perspective on those attacks; again, not the specific nature of the attacks, because we–it's like a

justice question, right? We don't want to do anything that helps anybody who might be wanting to perpetrate that, but just the global number of what you would define as a cyberattack.

Mr. Gooch: Yes, we can compile a summary of the cyber incident–or not incidents, sorry, cyberattack attempts and provide that to the committee.

MLA Maloway: Now my question is to the deputy. He will know that the Province has a group of people in what was used to be called OIT, where–actually, I was over there many years ago and there was actually cyberattacks going on and the person in charge was showing us, you know, that this was happening. This is a long time ago.

But we know there is a group in each province that meets on IT issues, and we had a program to share software, so we didn't all, going around–you know, a company will sell a program to all ten provinces or all the hospitals within the provinces and make money just over and over again. So you people have a program or a group that meets and they have–you have a conference once a year–used to anyway–where you talk about sharing software.

And I know there's reluctance to do it because everybody wants their own, you know, their own show. But it–what's happened in–this–with the States in the last couple of years right now, there's very big concern about server farms in the States where we're storing our data, we used to store–well, I won't get into it–but we used to store data in the States; I don't know that we do anymore.

So I think if we look into what's happening with EU and this open Linux system–I mean I'm sure they're not doing it for–just because they feel like doing it. There's got to be a reason here, and I'm just thinking we should make a little further look at this, right? Because I'm not suggesting Manitoba would be looking at money that it could save by going open Linux, but we have other provinces, so would it be conceivable to contact the other provinces and see if there's an interest in following up with what they're doing in Europe?

And is it–is there any, like, security issues in that as to what's going on in the world right now, that we want to have a Canadian–because with Linux we could have our own system–Manitoba, or we could have our own Canadian system that would be operated by ourselves.

***** (15:50)

It wouldn't be–we would cut ourselves away from Microsoft. And Linux has been around, as you know, for a long, long time, probably even longer than mark–Microsoft.

Mr. Gooch: There is quite a bit of collaboration and co-operation across the public sector within Manitoba. And the government of Manitoba leads a lot of buying-group efforts to get shared benefits from purchasing software once for the entire public sector.

We have other examples, like there's a special operating agency called MERLIN in our department that does buying-group purchasing for the K-to-12 education system. And I would say that there's also ongoing and active collaboration with the federal government and the other provinces through federal, provincial, territorial groups and through Shared Services Canada in leveraging federal contracts and the buying power of multiple provinces and the federal government in purchasing technology.

The Chairperson: Follow-up, MLA Maloway?

MLA Maloway: Well, that sounds good in theory, but in practice it doesn't work, as you probably know. My question really was about the Linux situation and the security issues, you know, with–vis-à-vis the United States and developing our own software program.

But, you know, where was a plan back in the day to have SAP? In Nova Scotia, they got a much better price than we did because they got the hospital and the City of Halifax and the government all together in the rollout.

And we had the City of Winnipeg go out and buy Oracle, right? And just give–you know, like, do what they wanted to do. So I know there's issues here. You're absolutely right with what you say, but in practice it doesn't always work out.

But this is a totally different issue dealing with the Linux. It's about moving on to a more independent system, open-source. And I only bring this up because–not because of securities issues with the States, but the European Union is moving ahead on this. So, obviously, they maybe know something we don't.

Mr. Gooch: Yes, I think the more recent conversations have been less about open source and more about sovereignty and control over Canadian data and applications. That has been a very active conversation across provinces and with the federal government as well.

The Chairperson: A question, maybe, for deputy minister.

So, when the pandemic happened in 2020, we had to come up with a contingency plan–it wasn't a contingency plan, it was a real life on-the-moment plan–for the Legislature to sit virtually, and the Clerk's office did a fantastic job of ensuring that happened, and we see the legacy of that still today.

What is the contingency plan if there's a cyber-attack and those people who are working remotely can no longer work remotely? Is there a government-wide plan or does it exist within each department about what to do if those folks who are working remotely can't work remotely, which is almost the opposite of what we faced in 2020 when everybody had to go remotely?

Mr. Gooch: Disaster recovery planning is a complex issue, and identifying the known and unknown scenarios that could occur in the future. If–in the event of a cybersecurity attack where employees could not work outside of the network, it would depend on what the scenario was. If they could work inside the network, then I think, you know, it would make sense for them to be inside the network.

It's unlikely that that would be how that would play out. It's likely that if there was an attack that prevented employees from working remotely, it would probably also prevent them from working effectively in the office. And so we do do disaster recovery planning and business continuity planning. I can't speak to that specific scenario in much more detail today.

The Chairperson: Right, and it's hard to imagine every scenario. We couldn't have imagined a scenario we were in five years ago–or maybe people who lived 120 years ago would have told us we could have.

But do those plans reside in each department individually, or is it your department who collectively has the master plan, for lack of a better word?

Mr. Gooch: What we would be planning for is the disaster-recovery plan for the loss of the systems. The business continuity plan is inherently with the departments.

The Chairperson: Are there other questions?

Seeing no other questions, I'll put the question on the report.

Auditor General's Report, Managing IT Security for Remote Access, dated March 2024–pass.

Before the committee rises, I'd like to ask that all members please leave behind the copies of the report so that they can be used again for future meetings or appropriately recycled.

The hour being 3:55, what is the will of the committee?

Some Honourable Members: Rise.

The Chairperson: Committee rise.

COMMITTEE ROSE AT: *3:55 p.m.*