HANSARD

NOVA SCOTIA HOUSE OF ASSEMBLY

STANDING COMMITTEE

ON

COMMUNITY SERVICES

Thursday, June 20, 2019

Committee Room

Protection of Confidential Information

Printed and Published by Nova Scotia Hansard Reporting Services

COMMUNITY SERVICES COMMITTEE

Keith Irving, Chair
Rafah DiCostanzo, Vice-Chair
Ben Jessome
Bill Horne
Hon. Gordon Wilson
Keith Bain
Larry Harrison
Susan Leblanc

[Hon. Gordon Wilson was replaced by Hon. Margaret Miller]
[Larry Harrison was replaced by Brad Johns]

In Attendance:

Darlene Henry
Legislative Committee Clerk

Gordon Hebb
Chief Legislative Counsel

WITNESSES

Department of Community Services

Tracey Taweel, Deputy Minister
Vanessa Chouinard, Executive Director of Policy and Innovation

Department of Service Nova Scotia and Internal Services

Maria Lasheras, Chief Information Access and Privacy Officer

House of Assembly
Nova Scotia

HALIFAX, THURSDAY, JUNE 20, 2019

STANDING COMMITTEE ON COMMUNITY SERVICES

10:00 A.M.

CHAIR
Keith Irving

VICE-CHAIR
Rafah DiCostanzo

THE CHAIR: Good morning, everyone. I would like to call the meeting of the Standing Committee on Community Services to order.

As committee members would know, this was rescheduled from June 4th. We had the appointment of a new deputy minister. Congratulations, Deputy Minister Taweel, on your new appointment. Given that that happened days before the planned committee meeting, the committee chose to reschedule this for today to give the deputy minister an opportunity to settle into her seat.

I would like to begin by first going around the table and having members of the committee introduce themselves.

[The committee members introduced themselves.]

THE CHAIR: A reminder that the washrooms and coffee can be found outside in the anteroom. In case of emergency, we'll exit to Granville Street and gather by St. Paul's Church on Parade Square. A reminder to turn off your phones or put them on vibrate. Also a reminder to our guests in the audience that photographs are only permitted by registered media. Just a reminder both to the members of the committee and our guests to be acknowledged by the Chair before you speak. That helps us with Hansard and keeping order at the committee.

As well, usually at this committee, we do a question and a supplementary and then move on to the next questioner. As time permits, depending on how many folks I have on a list, we will move to just one question and try and get as many questions in as we can.

With that, I would like to welcome our witnesses today. I'll turn it over to Deputy Minister Taweel to introduce her colleagues here today and proceed with the presentation.

TRACEY TAWEEL: Thank you, all committee members, for being accommodating and allowing the date to shift from earlier in June. I have been in the chair now, I think, seven days. I do appreciate having the opportunity to have seven days before coming. Given the importance of this committee, I wanted to make sure that we were able to discuss the issue that you had invited the former deputy to come and speak about. Thank you very much for that.

With me today I have Maria Lasheras, who is the Chief Information Access and Privacy Officer with Service Nova Scotia and Internal Services. Also, my colleague from Community Services, Vanessa Chouinard, who is the Executive Director of Policy and Innovation. It is indeed our pleasure to be here today.

We do have a presentation that we will deliver for you. Maria and I will go back and forth on the slides. With that, I would ask Maria to begin the presentation.

MARIA LASHERAS: Good morning. I am going to speak a little bit about the role that Service Nova Scotia and Internal Services have in the context of our privacy program. We were established in 2015, and we were mandated by Treasury Board to establish a privacy program providing leadership division and a strategy for government as a whole. As such, we had developed a corporate privacy policy which includes related processes and tools.

We also provide operational support to the majority of government departments and some agencies. A couple of departments, including DCS, determined that due to the extensive amount of personal information and the nature of their mandate, they would keep the operational privacy in-house. So we set the policy and the Department of Community Services implements that and also includes additional protections, if you will, or guidelines that are going to work for their clients.

We provide corporate awareness training. We develop the tools and the departments adopt and deploy them to their staff.

The fourth component is the monitoring and reporting. It is important to monitor how we are doing for the purpose of accountability and continuous improvement.

We established our privacy program, which was really disseminated across all departments. We determined that there were essentially four pillars that will support privacy overall. In particular, the first pillar is about governance and accountability - how

are decisions to be made, who determines what the direction might be. It is critical in all areas, but particularly in privacy that there are very clearly articulated roles and responsibilities. We did that through our corporate privacy policy.

We interpret and deploy the legislation. The legislation is the responsibility of the Department of Justice, but Service Nova Scotia and Internal Services interprets and applies the legislation. We provide the tools to the departments so that we can do consistent support of privacy protections.

The other area is program controls and processes. As I mentioned, we developed a privacy policy that came into effect on May 2018. That includes identifying what tools we are going to use, what processes need to happen in the context of protecting privacy. We provide professional and specialized consulting services. It is important that privacy is considered a discipline that is well applied by professionals with appropriate education and background.

We have implemented privacy assessments - not only the tools, but the how-to. It is very important to ensure that all of the departments are aligned with the objectives of a robust privacy program. We have a complaint management process, agreements, et cetera.

It's very critical to collaborate - that is the third pillar. It is critical because the outcomes and the outputs are always at their best when there is collaboration and working together among all of the departments.

Finally, the fourth pillar, which is monitoring and oversight. We need to monitor what is happening, we need to measure, and we need to report to make sure that we include continuous improvement in our practices.

In a nutshell, this is how Service Nova Scotia and Internal Services provides the support to all of the client departments. Back to you, Tracey.

TRACEY TAWEEL: The Department of Community Services does have, as Maria mentioned, a dedicated privacy resource. I was very happy to learn that when I arrived at the department. That resource - the title is the Manager of Information Services and Privacy. She works very closely with Maria and her team to ensure that the Department of Community Services is in compliance with all relevant pieces of privacy legislation, policy and guidelines.

In addition, she has a role in overseeing overall records management for the department, overseeing the FOIPOP process for the department. She also provides expert access and privacy advice; helps to investigate and respond to privacy breaches and any privacy complaints; oversees the privacy impact assessment process, including the identification at the outset of any potential privacy risks that may perhaps be relevant to new program design or any service that we might be changing and ensures that any appropriate mitigations to offset those risks are implemented. She develops and delivers

training to Community Services staff from one end of the province to the other. While she may be located here in Halifax, her mandate extends right across the province to all of our regional sites. In addition, she works with the Office of the Information and Privacy Commissioner to resolve and respond to privacy complaints which may be referred to their office.

I'll pass it back to Maria for the next slide.

MARIA LASHERAS: In terms of the specific work together with SNS and IS, and DCS, there are four main areas that are critical for our common success. One I want to stress again is collaboration and knowledge sharing. There is always the risk of duplication and inconsistent approaches. DCS and my unit in Information Access and Privacy services look and share experiences. We learn from each other. We learn through situations so that we can go back to continuous improvement. We share resources. We try to eliminate redundancy where possible.

From a corporate perspective, we do provide corporate tools. We share all of those so that Community Services then can build on those and protect the information of their clients in a way that is specific to the Department of Community Services. We develop a series of privacy tools that are used across the board, and that is so that we get a head start. Then, as I said, departments - in this case DCS - build on those. We have advisory consultation. As the deputy has said, they have their own privacy monitor. We work very closely to ensure that we are consistent in our practices.

In the context of the mandate that IAP services received from the Treasury Board, that is the direction that we provide, which is corporate in its approach but very collaborative and consultative in our practice.

TRACEY TAWEEL: As I referenced, we do have a dedicated manager, a dedicated resource, who works collaboratively within the department to ensure that the protection of privacy is front and centre for all of our staff. We also have detailed measures in place to protect the privacy of the clients that we serve. We regularly consult with corporate IAP services as appropriate to get their input and feedback on any privacy-related matters. This would include things such as a privacy breach or a complaint that the department might receive; privacy impact assessments, which I referenced a moment ago; and privacy research discussions, where we would be looking to monitor emerging trends and understand that the corporate IAP resource certainly has a finger or an eye on the pulse of what is happening internationally vis-à-vis privacy.

We complete privacy impact assessments for any new programs or services or any changes that the department may be contemplating to existing programs that would involve personal information. The privacy impact assessment is used to identify any risks or concerns with respect to the collection, use, disclosure, retention, or destruction of personal information. It is certainly a critical tool in developing mitigations for risks before any change is implemented.

It's important to note that third party service providers, of which there are many, that work with Community Services - private and non-profit service providers do not fall under the FOIPOP Act. They fall under federal privacy legislation, which is the Personal Information Protection and Electronic Documents Act. We do, however, include privacy and confidentiality provisions in all contracts and agreements that we have with service providers to ensure that they are aware of our expectations around the treatment of personal information being shared. This would include a privacy breach reporting provision and a guide for how they should respond to and report any privacy breach, should one occur.

[10:15 a.m.]

Examples of the privacy practices that we have in place to mitigate risks would include - as I referenced earlier - ensuring that risk mitigations are discussed during the policy design process. I think it's important for the committee to know that the manager of information services and privacy participates in the policy design process from the very beginning. She is a member of the department's Policy Management Committee. So even when it's just a small idea, she is at the table and can weigh in on any potential risks that she may see, given her expertise in the area of privacy.

We complete privacy impact assessments for any changes, as I referenced earlier. We incorporate a privacy-by-design approach, meaning that we incorporate a privacy lens to program and policy design to mitigate risks that is tailored to the particular policy, program, or service that we are contemplating.

We also limit the collection, use, and disclosure of personal information to only what is necessary to provide the service or provide the support that a client requires. This is supported by the completion of the privacy impact assessment, as well as privacy awareness training and other privacy-related work at all levels of the department.

We also work to ensure that our clients know and understand what information we collect, how we're going to use it, and who we're going to share it with. This is supported by the use of consent forms, staff training, and communication with clients about our programs and practices.

Additionally, it's important that we limit access to personal information to only those employees who need to know the information to carry out their duties. So staff have access to the information they need to deliver services to their clients, and sharing of personal information does follow the provisions in the FOIPOP Act, particularly Section 27. We also use security roles in technology solutions to make sure that access is limited only to those who require that access.

We ensure that reasonable security arrangements are in place to prevent privacy breaches. This includes, but certainly is not limited to personal information being securely stored in offices. I would call it the more traditional security measures: locking cabinets in file rooms, putting things away at the end of the day, locking offices. Processes are also in

place to monitor user accounts in our case management system to ensure staff who leave the department no longer have access to files that they would have had access to when they were employees.

We have a reporting mechanism to detect dormant accounts, meaning staff who have not had access to the system in six months. We can track that and eliminate access, as well as confidentiality agreements in place with any contractors or consultants that we have in place who are doing work for us.

We work to ensure that staff are well-trained in the privacy protection protocol and that privacy is front and centre and part of the culture within the department. Staff are required to complete mandatory access and privacy awareness training, which my colleague referenced earlier, corporate training. Staff are continuing to complete this training. Some are still outstanding. We'll have a continued focus on that in the months ahead.

We are able to track who has completed that training in the corporate learning management system. In the role of deputy, I will be receiving quarterly reports on who has completed the training and who hasn't. We'll be working to ensure that we have complete compliance with that mandatory training.

In addition, the manager that I referenced earlier develops distinct modules for the Community Services staff and routinely visits our regional offices, as well as supports the staff here in Halifax in understanding the importance of privacy and developing specific modules that relate to the work of staff in Community Services, helping them understand the difference between privacy, security, and confidentiality. As well as the more formal training, she provides training upon request at various times throughout the year.

At the Department of Community Services, we also have the benefit of having an internal share point site - an intranet, if you will. That site is used to constantly reinforce the importance of privacy. It provides tips and things like that. It's a very well-visited site. I was really pleased to see it when I arrived at Community Services. It's a really valuable tool for staff. We also have ongoing engagement and collaboration with our colleagues in the corporate IAP office to ensure that Community Services remains aligned with government policy practices. Lastly, we ensure that we are staying current with latest trends in terms of corporate training and privacy awareness.

With regard to the privacy breach, which is the topic at hand today - privacy - the majority of breaches that DCS would see are caused by human error, and that means that breaches are not intentional or malicious in nature. Some examples could include emails being sent to wrong recipients or letters being placed in an incorrect envelope being sent out to an incorrect client. Since 2014, there have been 122 reported breaches in the department. In all 122 cases, 99 per cent of the information was recovered. Again, in the majority of those cases, they were the result of human error.

The number of reported breaches, I am pleased to see that breaches are reported in the department. I think it's a signal of the growing level of awareness with staff and the growing level of awareness in the environment within which we're operating. We hear about things like this all the time, not just within a government context, obviously, but in a corporate context as well. I think we need to continue to raise awareness. I would much rather have our staff know exactly the proper protocol to follow and be reporting anything that they have concerns about than not reporting things that they have concerns about.

With that, we would be happy to take your questions. Thank you very much.

THE CHAIR: Thank you, Ms. Taweel. We'll begin questions with one supplementary. Ms. DiCostanzo.

RAFAH DICOSTANZO: I know you're talking about the training, and as you're talking, I'm trying to imagine how many hours the new employees are trained at the beginning and how often they are trained. If you can just give me more of a picture of what the training looks like, how many hours, and where we are compared to, let's say, 5 or 10 years ago - how much we have to increase because the computer system is always changing, and things have to be updated. I know that you said you're developing modules. I'm assuming this is added to constantly. I just wanted to know more about the training, how it happens, how many hours it is, and what's involved.

TRACEY TAWEEL: I will start and then perhaps my colleague may have something else to add. I can speak specifically to Community Services. The mandatory corporate training model is required on an annual basis. In addition to that training, we have ongoing training. I guess in answer to your question, it's an ongoing, continuous process of training. As the field of privacy changes, and as new technologies evolve, and as awareness grows, the need to continue to train our staff and ensure that privacy considerations remain front and centre is an ongoing effort.

In comparison to, say, five years ago, I would ask my colleague to respond more succinctly, but from my experience elsewhere in government, I don't believe a corporate module in this way existed five years ago. I think we have made tremendous steps forward in terms of raising awareness. Again, as I referenced earlier, it is a function of raising awareness within government, but it is also a function of the changing world that we're operating within and the need to be always mindful of protecting privacy and personal information.

MARIA LASHERAS: Just to complement Tracey's response, the e-modules that we developed as a corporate tool for training of all the staff - they take about an hour and there are three modules. We tried to make them fun and interesting because a lot of people think that privacy is not fun or interesting, and we want the participation. It takes about an hour, and anyone can do it on their own time at their preference. That was launched in early 2018 and it is mandatory for all civil servants.

That in itself is not enough, so in addition to whatever the departments do that is tailored to their own needs, we also developed corporate tools. For example, what is snooping? What does that mean? As we learn more and more about privacy, we continually strive to actually make and build that awareness. Privacy will be successfully protected when the culture is about protection of privacy.

We constantly develop tools – what is phishing, what is snooping. In January we have the privacy day we do through our Yammer sessions, we post tools. We are constantly throwing bits out and being present so that we can actually make sure that everyone receives and is aware of all of that. I guess it's fair to say that it's a continuous process.

RAFAH DICOSTANZO: A supplement to that question is: Are these training modules similar in other provinces, in other jurisdictions or are we developing our own? Do you have consultation with other provinces as well when it comes to training?

MARIA LASHERAS: Yes, we do. Nova Scotia participates in a pan-Canadian committee where all jurisdictions have discussions about privacy and access issues. I think that it's fair to say that we are well aligned with all that is happening in other jurisdictions. There are other tools developed by private organizations such as the International Association of Privacy Professionals that we also consider among the tools that we may deploy. We are always looking, but we are well-positioned to protect the personal information and make sure that our civil service is fully aware of the obligations that they have.

THE CHAIR: Mr. Johns.

BRAD JOHNS: Thank you. Of course, one of the main concerns that members of our caucus has brought up in the past is in regard to security and security breaches. We do feel that when people submit their information to government, they need to have a sense that the information is protected and confidential. So I am glad to see that there are some things that your office is doing.

I'm really confused about something. In the presentation that was forwarded on May 29th on the last page - and you did raise the number 122 breaches since 2014. In the original presentation that was sent out and the presentation that was sent out yesterday morning - in writing - it said 122. Then yesterday afternoon, the presentation was revised and a new presentation came out with that one specific line removed. Can you tell me why you would go through the problem of removing that one line from the whole presentation, yet you brought it up here anyway? I'm confused about that.

TRACEY TAWEEL: Actually, other things did change in the deck - principally, the proper naming of the Department of Service Nova Scotia and Internal Services. It was incorrectly named because of when the deck went out. That one particular bullet was just moved into speaking points. There is no reason - it was just moved into speaking points.

Really the main reason for resubmitting the deck was to ensure, for the record, that the department was properly named.

BRAD JOHNS: We have noted that there have been over 7,000 records inappropriately downloaded in the breach here last Fall. Of those 7,000, can you tell me exactly how many of them, if any, were directly related to your department?

[10:30 a.m.]

TRACEY TAWEEL: I can tell you that there were 361 DCS files that were impacted through the breach. Of those, we worked with the corporate IAP service to mitigate and triage the risk associated with all those files and categorized those into significant risk, lower-level risk for sensitivity, and then low risk. We communicated directly with those clients to ensure that they were properly supported and aware of what had happened and then provided additional supports to all of those clients all through the process.

I believe my colleague can speak a little bit about the more global process, but as it relates to Community Services, we worked very collaboratively with our colleagues to make sure that we were managing all risks appropriately and communicating with our clients.

The one other piece that I would add is that our manager, who I referenced a few times, ensured that there was a constant information flow to our front-line staff in case clients came directly to our regional office, for example, to express concern or perhaps confusion about the letter they had received. We made sure there was a constant information flow and supported our clients and our staff and adhered to the corporate response throughout.

It is my understanding that all files associated with the privacy breach have now been deemed closed by the privacy officer. My colleague can speak more to that. In a nutshell, that was the Community Services response.

MARIA LASHERAS: Just to confirm what the deputy has mentioned, yes, there were 361 files. Highly sensitive included 60 of them, 213 were sensitive, and general - which would have been name and address - were 88. One point that the deputy did not mention was remediation or support to clients of the Department of Community Services and anyone else who had their information breached during the breach of 2018, were provided with credit monitoring for one year to make sure that in cases of sensitivity of the information, if there was a risk of identify theft, they could monitor personally and could then approach us and remediate where possible. Yes, we did work extremely close together because we did understand about the sensitivity and the importance of collaborating among the two departments in support of all of the clients.

THE CHAIR: We'll move now to Ms. Leblanc.

SUSAN LEBLANC: The procurement process has started for the online services to support the delivery of services to clients in child, youth, and family services, the Disability Support Program, and the income assistance program. Of course, these are clearly individuals who are vulnerable, and we want to be very careful with their sensitive information. Can you talk about what risk assessments and threat analyses have been conducted for these projects? What is being done to make sure that the department doesn't make the same mistakes that we did see in the FOIPOP privacy breach?

TRACEY TAWEEL: Yes, you're quite correct. We have hired a vendor to begin that work. As I believe I referenced in the presentation, any project, in particular something of this magnitude, will undergo a privacy impact assessment. Our manager and other resources as appropriate will be part of the design process. That work is beginning now. As you would probably be aware, this will be a multi-year, multi-phase development and rollout of the digital platform. I would not expect to see the first element of that for probably two to three years. That work is ongoing. Discussions have begun.

As I also referenced in the presentation, in terms of the contract with the vendor, we have ensured that in that contract the appropriate privacy considerations are also in place. It is incumbent upon all of us, everyone who is working on the design of this - the vendor, staff, and others - to ensure that privacy is paramount and is front and centre with regard to the development of this new platform. We know that our clients want to see more services move to online platforms, so it does make sense for us to go there. But with that, we need to be making sure that we embark on threat risk assessments, that we have appropriate mitigation measures in place, and that privacy is front and centre.

The only other point that I would add is that in addition, even once we have moved to a digital platform, we will still always have the opportunity for clients to receive face-to-face service or complete paper applications if that's what works best for them. In those instances, we will also need to ensure that the more traditional, as I referenced earlier, means of protecting information stay in place. It is a constant process of threat risk assessment, managing privacy, keeping it front and centre, and ensuring that that is the case all along.

We will also, as the project develops, consult appropriately with the corporate resource that exists in Maria's shop and also with the privacy officer as well as we work through this process.

SUSAN LEBLANC: You mentioned this is going to be a multi-year rollout, and also you mentioned that the clients of the department want to go online. I want to pick up on two of those things.

We recognize that $2 million was included in the 2019-20 budget for these online services for ESIA and DSP. The NDP caucus requested freedom of information for all documents and correspondence related to the decision to provide online access for income, employment, and disability supports from September 1, 2018, to the middle of January.

The response we got back from the department was that there were no records responsive to that application.

When you say that the clients want this rollout to happen or this program to have online options, I'm curious to know how the decision was made to move those services and how the assessments were conducted with a lack of paper trail connected to those conversations.

TRACEY TAWEEL: I will answer as best I can, given that I am still fairly new. My understanding is that the planning for this work happened long before that time frame that you have indicated. The work around transformation has been occurring for four to five years, and first voice client input has been fundamental to that all the way along. The decisions around moving to a digital platform - while we may be making that decision and have let the contract, as of December - consideration for that has been ongoing and been part of the plan for quite some time.

I can certainly also look into what you have raised. As I come up to speed, I would be more than happy to have a follow-up conversation with you.

THE CHAIR: Mr. Jessome, you're next up.

BEN JESSOME: I guess I'll add a disclaimer that no exposure of private information is a good one, but I'm wondering, deputy, if you could comment on the nature of these breaches generally, whether they were malicious in intent or not so much.

TRACEY TAWEEL: I assume you're referring to the 122 that I referenced, not the larger breach. Of the 122, the vast majority were things such as an employee putting the name of a client in an email and sending to an incorrect address within government or mailing out information to the wrong client, for example.

I don't like to say "human error" because I don't want to make it sound like that happens a lot because it really doesn't. It doesn't happen very much. I agree with you - any error, any potential privacy breach is not a good thing. But to my earlier point, in those 122 cases, 99 per cent of the information was recovered, and we are working hard to raise awareness within the department and with our staff to help them understand that even something that could be categorized as minor - such as the examples I have provided - still warrants reporting and still warrants a review of the process that led to that happening in the first place.

Sometimes it's important for people to just take a breath and make sure that all their i's are dotted and t's are crossed, and that privacy and protecting that integrity and the relationship that we have with the client is of paramount importance at all times.

I would say Community Services serves a vast number of clients, and in the vast majority of cases, all the information is protected. There are many safeguards in place. Any

breach, however, is not welcome and is very unfortunate. We'll continue to work hard to raise awareness so that if it happens, it is also reported, but also to try to prevent any of those from happening in the future.

BEN JESSOME: Deputy, I do appreciate - and I'm sure we all do - the consideration for that relationship with our client base. In that respect, I'm wondering if you can comment on the activity that took place, the level of engagement with the affected clients, and what was done to make it right - if there is such a thing in this scenario.

TRACEY TAWEEL: Again, with regard to the 122, similar to the process that was used in the larger privacy breach in 2018, each of those breached would be triaged to determine the level of sensitivity around the information that was breached.

For example, if medical information or services being received by a particular client - if that information was somehow inadvertently shared, we would contact the client. We would work with them and help them to understand exactly what has happened, exactly the steps that we are taking to retrieve the information if we have not yet retrieved it, and we would make sure we stayed in close contact with those clients to help them manage their way through the process.

Other breaches we would characterize - and I use this term advisedly, given that any breach is not good - some would be more minor in nature, if you will, such as the name of a client being sent in an email to an incorrect recipient. In those cases, we would categorize those slightly differently.

Within the department, a number of staff have received the corporate training. We still have many more staff who need to receive that training. As I referenced in the presentation, it will be a priority in the coming months to ensure that I work with the executive team to make sure that they impress upon their teams the importance of this training and the importance of using our in-house resource.

By coincidence, she was the very first person I met when I arrived in the department. She took advantage of that five-minute meeting to fill me in on all of her work. I think to say that privacy and its importance is a priority in the department would be a bit of an understatement. She is everywhere and working hard with her colleagues right across the department to protect the information because it is vital.

We have a very intimate relationship with our clients, and things like a breach, whether it's categorized as minor or major in nature, run the risk of compromising that relationship. I know that is not something that any of the staff at Community Services ever wants to see happen.

[10:45 a.m.]

HON. MARGARET MILLER: This has been very interesting this morning. I find it a little bit overwhelming. We're talking about breaches over five years, the 24 breaches or incidents - I think I would call them more incidents than breaches. When you talk about the emails going to the wrong recipient, you can see that easily happening. The same with something being put in the wrong envelope.

I think our biggest concern is, of course, the technology. I know the technology is improving all the time. They're coming up with new technology to better serve Nova Scotians - to protect their privacy. Obviously, with the first two categories it was human error or a misplaced piece of paper sometimes. Will there ever be a technology that will be fail-safe? Will we always have a certain percentage or a little bit that's still coming through and will there always be issues?

TRACEY TAWEEL: I will start and then perhaps the expert in this area might have a comment to make as well. As long as I think we have human beings that are involved in the holding of information, there is always going to be a margin of error and there are always going to be risks.

The environment that we all live in now - whether it's interaction with government or it's our personal banking information or any number of things, we are all providing a lot of information to a variety of sources. I think the more that happens, as the world changes around us, there remains a risk.

I think the way that we can mitigate risk insofar as Community Services is concerned, is to continue to do all of the things that we've discussed thus far this morning - keep privacy front and centre, keep drilling home how important that is from the moment an individual is hired, right through their entire tenure with Community Services specifically, and with government more broadly, since we know people do move around.

I think it is a constant vigilance that we need to maintain as individuals, but importantly, as public servants we sit in very privileged seats and we're privy to a lot of information. Community Services has, as I referenced earlier, a very intimate relationship with our clients and we need to hold that sacred, and above all else, work as diligently as possible to protect privacy. But I don't believe we can ever be 100 per cent certain that nothing will happen.

MARIA LASHERAS: Just to complement what the deputy is saying, in general terms, technology and privacy are sometimes at odds. What we can do about that is really build a culture that acknowledges and understands the value of privacy at the level of all of the civil service; that paired with executive and organizational support and understanding from government that privacy matters, and support to all of us to make sure that we actually do our work on a daily basis with that in mind.

Having said that, what we learned from our experience last year, and from what we learned from the Auditor General and the Privacy Review Officer reports, was that we needed to make certain changes that were going to be critical in the context of technology developments.

From the cybersecurity perspective, we have increased the complement, added six or seven - I don't have the exact numbers, but six or seven staff to continuously monitor and put processes in place. We have developed or deployed anti-viral software to all of our devices. We've upgraded all of the firewalls to new, bigger, and better devices to improve capacity and all of our security capabilities.

We are really doing a tremendous amount of work in the cybersecurity space so that we can protect the privacy of Nova Scotians while we also meet their demands from an individual environment.

MARGARET MILLER: I'm just thinking, is this a recent thing? Is this something that is just happening in the last five, six, or seven years? Was this not an issue 10 and 12 years ago with privacy, or is it as technology is getting better that we're getting more info?

TRACEY TAWEEL: It's probably better answered by my colleague. I would say just in general terms that I think it continues to evolve - the field of privacy continues to evolve. The importance of protecting privacy has always been a hallmark of the work of the Department of Community Services and the work of government. I believe from a technical perspective, from a digital perspective, that world has evolved tremendously over the past 10 years.

MARIA LASHERAS: The concept of privacy goes back to the 1800s. The right to be let alone is what privacy is all about. In the 1800s, we did not have the technology that we have today or in the 1950s, the 1960s, even the 1980s and 1990s. It is technology that has really presented the risk to that ability for the individual to actually control how their information is going to be managed.

It is in that context that our responsibility as a government and a department and as civil servants, we have the obligation to look at what risks that technology brings to the concept of privacy and the whole issue of collection, use, and disclosure of personal information and how we are going to mitigate those risks. That's where we are by the government really enforcing the cybersecurity complement and also resources on the privacy side.

THE CHAIR: Let's move across the table. Mr. Bain.

KEITH BAIN: Thank you for your presentation this morning. When there's a privacy breach with DCS with highly sensitive things like adoption records or personal statements of abuse or anything like that, would that be available in those privacy breaches, that somebody could actually access those things like adoption records?

TRACEY TAWEEL: The 122 breaches that I referred to, the vast majority of those were what we would characterize as minor, so the description I provided earlier - a name being sent in an email, et cetera. Certainly information such as what you have referenced is held with the utmost reverence if you will and protected using all of the mechanisms that I referenced earlier in terms of locked file cabinets; pursuing any dormant accounts and making sure they're removed; if staff leave the department, removing their access; restricting access for employees only to the information that is germane to the job that they have to do.

If an employee does not work in ESIA, they would not be able to access that information. The 122 that I referenced earlier were not of the nature that you have described. We do have safeguards in place to protect information. In the vast majority of those 122 cases - 99 per cent - the information was appropriately recovered.

KEITH BAIN: A lot has been said, even this morning, about protection online, but the statistic is also that the majority of them took place as a result of human error. Am I correct in saying that? It's saying we can spend millions of dollars to secure our cyber system, but letters are still being mailed to the wrong people - and a lot of correspondence goes out from Community Services. My question is: What steps other than increased cyber protection are taken to ensure that those letters stop going in the wrong envelope?

TRACEY TAWEEL: To put the 122 into context, it's 122 since 2014, and you are quite correct, a lot of correspondence goes out from Community Services - both traditional, through the mail, and also through electronic channels.

I think the answer to your question lies in creating a culture - to the comment that my colleague made - where people understand that job one is protecting the privacy and the relationship that they have with the client who has entrusted them with highly personal information. So creating that culture, raising awareness, ensuring that we have appropriate processes in place and safeguards in place to try to protect - and as strongly as possible, prevent those things from happening. Then having a culture in place as well that says, if it does happen - in those unfortunate cases where it happens - ensuring that employees know the appropriate steps to take and that they need to make the appropriate individuals aware that it has happened.

That all comes back to culture as well, and being willing to say, I made an error, I made a mistake, I may have compromised information here, and raising that with the appropriate resources so that - for example, our manager can follow the appropriate process to investigate what happened, notify the client and, importantly, seek to get the information back and mitigate any risk that may have arisen as a result of that error.

THE CHAIR: Ms. Leblanc.

SUSAN LEBLANC: In the government's privacy policy, Section 4.11, it states that, "Employees of government entities who prepare or manage contracts that involve the

collection, use, storage or access of personal information by any third party shall consult with legal counsel, and shall ensure that privacy protection provisions recommended by counsel are included in such contracts."

However, the Auditor General's Report found that when the FOI website was implemented in 2016, there was no amendment, change order, or contract created. So I'm wondering - and maybe this is for you - can you please explain how it is that this project was able to move forward with no contract in place?

MARIA LASHERAS: I will try to answer as best I can. If I understand correctly, the finding was not that a contract didn't exist - if my recollection is correct. The government had a contract with the vendor of the AMANDA platform. We did leverage that contract to deploy a module that was sitting in that platform.

What I believe there wasn't was a change management - a change order of some kind, but the contract did exist, and I believe the Auditor General found that. Did that answer your question?

SUSAN LEBLANC: In a way, I think you answered my question. However, if I had to ask it again, which I won't because I want to ask something else, I would have said then why was the change order not properly protected? But that is not the question I'm going to ask.

I'm going to move on and say also, within the government's privacy policy, there is the requirement of all employees of a government entity that they complete mandatory privacy awareness training once every two years. Ms. Taweel, you have suggested that there are people who have taken the training in the department - people who still need to. I'm wondering if you are able to provide to us a report on those numbers. How many employees with the department are up to date with the training - that means the mandate of every two years - how many are not up to date, and how many haven't taken it at all?

TRACEY TAWEEL: I was having them do it every year, so it's good to know that it's only every two years.

SUSAN LEBLANC: I take it back.

[11:00 a.m.]

TRACEY TAWEEL: I'll keep telling them it's every year. There are approximately 460 staff within Community Services who have taken the mandatory training. A fair number of employees still remain to take the training. That would be a focus in the upcoming months. This particular module, I believe, was only created maybe a year ago. Those 460 have been through the new training module, and we'll be working to have the rest of the employees go through that module. It is mandatory training, so we will be pushing to have the rest of the staff go through the training.

SUSAN LEBLANC: How many employees are there?

TRACEY TAWEEL: About 1,600.

THE CHAIR: We'll move on to Mr. Horne.

BILL HORNE: Good discussions. I would like to concentrate a little bit on monitoring, one of your pillars of the program. It's only as good as the training the monitors have, what type of qualifications they might have, how they work. That maybe includes cyber detections and different programs and their knowledge of IT. I wonder if you could just comment on some of those issues.

MARIA LASHERAS: I think that creating the culture of privacy together with the middle ground of establishing the policy and then monitoring how we are doing is critical to improve, to identify risks, and to mitigate those. In the context of privacy, the experience of the events of last year, the breach of privacy on the FOI technology, has taught us that process improvement and monitoring how we are doing is the only way to actually achieve the objectives of privacy protection. We are in the first step of developing the privacy policy.

The first determination is, what is it that we are going to monitor? Getting to understand and count how many privacy breaches occur in the course of a quarter, or however the departments want to measure that, is one of the metrics that we are going to be considering. Of those breaches, for example, how many of them are significant? How many of them bring or may bring harm or embarrassment to the individuals? That is another of the metrics that we will be considering. How many we are going to report to the privacy review officer is also based on the sensitivity of the information that has been breached, et cetera. This is one type of metric specific to privacy breaches.

Another type of metric that we want to develop is, for example, how many privacy impact assessments departments have developed to make sure that we identify the risks that new technologies and new services bring along. Monitoring all of those privacy impact assessments is critical because the privacy impact assessment is about identifying the risks and how we are going to mitigate those risks. There is always going to be some residual risk, but the important part is to monitor and report on how we are doing. How are we doing in terms of mitigating those risks?

There are other elements that might be about privacy complaints. How many complaints have we received? How many have we resolved satisfactorily for the clients, et cetera? Those are the types of metrics that are going to inform our improvement. We also will be monitoring legislative changes that are happening in the world environment, best practices, et cetera.

BILL HORNE: How many specialists would you have hired to deal with the issue of monitoring in particular? Do they have special training? Are they just naturally good at detecting things, or what?

MARIA LASHERAS: We want to believe that we are good. From the cybersecurity perspective, it's not my area, but I do know that they are in the process of hiring. I know all of the things that they have already put in place to monitor and prevent. We need to work on prevention from the cybersecurity perspective.

From the privacy perspective, I can say that the staff in my team are specifically dedicated to privacy. It is a team of six. They all have information management backgrounds, whether it is policy, et cetera. They work very close with the cybersecurity team. The resources associated with privacy are also increasing. We participate in conferences. The last week in May, all 10 in my team actually received the International Association of Privacy Professionals training, and they will all be certified. I'm very proud to say that.

We can't do everything at the same time. What I can say is that cybersecurity and privacy, which are the areas I know a bit, is well-supported by a collective of professionals with education in the field.

BEN JESSOME: I would like to note the work of the privacy officer's office and the series of recommendations that were made related to these circumstances. I'm wondering if either of you can comment on the response taken with respect to this list of recommendations made by the privacy officer.

MARIA LASHERAS: As painful as the privacy breach was, and really the impact that it had on Nova Scotians but also on the privacy team and the department as a whole, we accepted as a department all of the recommendations from Ms. Tully. We accepted all of the recommendations from the Auditor General as well. I can say that we have worked very consistently to actually achieve those recommendations.

I can say that specific to the Department of Community Services and their clients, Ms. Tully had made two recommendations, and we now have correspondence that I would like to table, if I may, about the closing of those recommendations and her recognition that the department is working very diligently to achieve those recommendations. She is quite complimentary, so I'm very pleased to share this.

Of six recommendations from Ms. Tully, we have closed three, and she has accepted that closure. We are working on implementing the other three, and we expect to do that in full by the end of the year.

BEN JESSOME: I'll just add that, dare I say, as the government, we're very grateful for the work of the AG's office and the privacy officer's. I know that overall it has made some substantial accountability and encourages us to respond, and the work that goes on

in those two respective offices is certainly beneficial to the overall governance of this province.

My supplementary was, what's the timeline for completing the remaining three, but I guess we don't have to put a timeline on that if you say they're in the hopper.

MARIA LASHERAS: Yes, they are. The work on the recommendations continues. We continue to look at the recommendations. We have an action plan, which is actually public and is posted on the former Internal Services site and all the activities that are related to that. If I remember correctly, Ms. Tully had put some timelines for implementing her recommendations by the end of the year, and we are well on the way to doing that.

THE CHAIR: Mr. Johns.

BRAD JOHNS: I'm not a regular member of this committee. I'm a fill-in today. I just want to make a comment in regard to your department. I came in today very skeptical, thinking that, similar to other committees that I sit on, I'm going to be stonewalled on the questions that I ask, that I'm going to feel there's not open, honest, transparent remarks and comments by members of the department. I don't feel that today. The openness and honesty to the questions, some of which may not even be comfortable, that you guys have answered today - I think that's what shows that the process works. As an Opposition member, I'm asking questions, questions that, not as government, we may not know, that we're trying to represent for our people. You're answering those.

I just want to comment that I applaud you because I came in here on the offensive, ready to receive the same remarks, the same attitude, and the same things I get sometimes from other departments or some of my colleagues get. I'm not feeling that. You're answering just about everything we're asking as Opposition. I appreciate that very much. (Interruptions) I felt it was important to point out because other departments aren't like that. I have been on other committees where we as Opposition don't have that opportunity.

Of the existing privacy breaches since 2014 - I know that you said that many of them have been minor in nature. I'm curious to know, could you give me not necessarily the exact details but an example of what you would consider the most serious one, just so I can put it all into perspective if you could?

TRACEY TAWEEL: If I could just have one minute.

BRAD JOHNS: I could've asked the question first and then followed up with telling them how good they are. (Laughter)

TRACEY TAWEEL: Thank you for giving me a few minutes, and thank you for your earlier comment. Just to respond very quickly to that, that's part of the reason why I thought it was important that we come now and not wait until the Fall. I recognize the value of these standing committees. As someone very new in the chair, I am interested in learning

your perspective on the issues that we're managing at Community Services as well. Thank you very much for your comment.

Very high level, one breach that we would consider a little more serious - we had someone working with us for a very short period of time who accessed some private information about a client that was inappropriate and was a breach of that information. It was contained very quickly. The information was recovered. We would consider that to be very serious. It was outside of the purview of this individual's job. It was extremely inappropriate and would be very sensitive to the client whose information was breached. That would be an example.

BRAD JOHNS: I'm going to ask this in regard to privacy and breaches of privacy, but I guess it could be extended to any of the services that DCS owns. If there is a Nova Scotia resident who has a concern in regard to how something has been dealt by DCS - whether it's privacy issues or others - is there a formal process? What is that, that they lodge a complaint to have something reviewed?

[11:15 a.m.]

TRACEY TAWEEL: Certainly, if any client has a complaint, I would hope that they begin by having a conversation with the individual who is closest to them first - whether it be a caseworker or someone like that - to try to resolve at that level. Beyond that, a client can always speak with a director and executive director.

In terms of a formal process, we do have a protocol in place for receiving a complaint, investigating a complaint, and resolving a complaint. There is a corporate policy in place for resolving privacy complaints that my colleague can walk through.

We adhere to all of the corporate standards with regard to any sort of privacy complaint that a client may have. If it's not a privacy complaint - if it's more of a service complaint or something like that - then they would work through the department to resolve that complaint.

THE CHAIR: I've got a little update for the committee. I've got five folks here and about half an hour left. I think we can do one and a supplementary, but if more hands come up we'll start moving to single questions. Ms. DiCostanzo.

RAFAH DICOSTANZO: I'll start my question with a comment. You were talking about creating a culture of privacy and confidentiality. I've always struggled with the words "confidentiality" and "privacy", so I just looked it up to make sure I'm on the right track with the exact difference.

I worked as an interpreter for 20 years and I can't tell you how important confidentiality and privacy is with your caseworkers and with the hospital staff. It was the first thing they taught me on day one - if I see you on the street, I will not say hello unless

you smile at me first. These are little things that I wasn't used to or newcomers may not be aware of - that somebody is not being rude, but I don't know you unless you say hi to me or whatever. So I had to educate the newcomers about those issues.

Another thing that I really compliment must be our education because I have two daughters that have gone into health. One is a pharmacist and one just graduated this week as an orthoptist. When I was working, I was struck by the amount of confidentiality - the importance they've put in their education. I had worked on one of their patients in her department - a small department - and I would ask, did you see this child? She would never answer me - mom, that's private, I cannot give you that information. They are really well taught, both in health with case workers. I've seen it with my own eyes. It's very embedded in their work.

The other side of it, I've actually noticed where we've gone to an extreme in some cases with privacy. I worked where a child had files with the Department of Health and Wellness and with the school where it may take two weeks before the two departments can talk to each other, because the parent has to sign to allow this department to talk to this department.

We have so many systems for privacy and confidentiality. It's beyond my imagination sometimes. We're doing really well there. The real question is: How do we manage the issues where it actually sometimes hinders the work to get faster or better because of this privacy? Do you have these issues and how do you work with those?

TRACEY TAWEEL: Thank you for your comments and for your question. I think you have appropriately referenced the difference between privacy and confidentiality - privacy being a right that we need to protect, and confidentiality being something that is incumbent upon public servants - and in the case of the Department of Community Services, all individuals who would come into contact with any of our clients.

I do think what you've outlined in terms of being able to share information across departments, that is an ongoing challenge that we are working hard across social departments - I can speak to those - to try to balance out the right to privacy, the need to protect confidentiality, but also our desire to treat an individual or a family in a holistic way. Sometimes some of the mechanisms that we have in place to protect privacy, for example, impede our ability to serve the client - that family, that child - holistically.

While protecting privacy is paramount, we do need to use all mechanisms that are available to us to come up with ways to appropriately protect that privacy, but still ensure that the child is being served most effectively. We need to treat people as whole people. They're not cut up the way departments are, the way we've aligned services within government. So the onus is on us as civil servants, I think, to work with lawyers, work with privacy experts, work with others to figure out the most appropriate way to balance privacy with providing exceptional client service and helping, in the case of Community Services, people really live their best lives.

RAFAH DICOSTANZO: I really compliment the Canadian system in regard to privacy and confidentiality. I think we excel in that, if I may say so.

THE CHAIR: Ms. Leblanc.

SUSAN LEBLANC: I'm going to change directions a little bit because I was going to ask some more questions about the privacy breach, but after I've read the thing that you tabled, I think my questions are answered.

Last night, I went to a really great presentation on child welfare - CHILD WELFARE ON THE BRINK: The kids aren't alright. I don't know if you heard about this event, but it was great. One of the things the presenter talked about - she's now a professor at Western University. She was a child that went through the child welfare system in Ontario. One of the actions that her organization is taking is to protect the privacy of children who are aging out of care.

I'm just curious to know what our policies are in Nova Scotia around that. If children are in the care of the minister, would their identification be protected? Then when they age out, is it still protected and for how long? I know that's a big question for someone who just started.

TRACEY TAWEEL: It is. I would say that information would be protected. I can't talk to you specifically about the retention schedule and all of that level. Perhaps my colleague may be able to.

The short answer would be yes, that information is protected when they are in the care of the province and when they age out of that particular stream of care that they've been receiving.

MARIA LASHERAS: Just to add that the protection of personal information on a child that is in care is the responsibility of the minister. As they move out of the system, if you will, our obligation to protect that personal information still remains exactly the same. The difference would be that it is at that time when they have moved out of the care, that the individual is in control of how much information they want to share at their own will.

Of course, if there are requests for access to those records at some point, all of those dynamics and who was in the care of whom at certain times and what information is contained within those files is what needs to be looked at. That is the process that will go through determining at what stage certain information can or cannot be - what types of consents are required, et cetera.

SUSAN LEBLANC: I will look more into that and figure out if there's more conversation to be had.

Also, one of the things I heard from audience members who asked questions and spoke in the discussion afterwards - and this relates to what you were just talking about in terms of caring for an individual in a holistic way. There were child welfare social workers. There were SchoolsPlus social workers. There were MLAs and a bunch of different people who would be working with the family from different angles to support them - people from the IWK mental health system, for instance.

One of the things I heard was that there is some frustration amongst all those folks who are trying to help one person, but can't because of all of the privacy issues and the web of privacy issues. I'm wondering, is that something the department is actively working on with other departments to take down that red tape and take down those barriers to providing good and proper care for people?

TRACEY TAWEEL: Yes, that is something that all social departments are working on. If I can put a different hat on, I have the privilege of chairing a social policy deputy-level committee. That is an ongoing topic of conversation and much work is being done to figure out how we can, to my earlier comment, protect the privacy of the client while ensuring that we're giving them the best possible service.

Work is under way in that area and we hope to make progress soon. It's a complex undertaking, as we try to protect privacy. It is a complex undertaking, but to your point, it is an issue that's being raised by the professionals that you referenced, but also by clients themselves - they're either directly raising it or it's manifesting in other ways in terms of frustration that they feel in having to interface with the variety of systems that government has in place.

My personal belief is that it's incumbent upon us to try to figure that out. It's not incumbent upon that child or that family, particularly if they're in crisis or in need in some way, to have to figure out how to navigate a system that sometimes we're not even sure how to navigate ourselves.

It is a priority. We're working on trying to manage that. The fact that all of these other professionals raised it as an issue is not surprising to me.

THE CHAIR: Mr. Bain.

KEITH BAIN: I'm going to apologize for maybe being repetitive, but I just want to ask a question for clarification. The process that the department uses to report a privacy breach and the length of time it would take for a client or the individual whose information has been obtained to get notice that there has been a breach - I guess it's process and timing for now.

TRACEY TAWEEL: As soon as we become aware that a breach has occurred, we immediately take steps to contain the breach so it's very important that the breach does not kind of grow, if you will, in terms of impact. Immediately, any employees within the

department who need to be made aware of this - because they would have a role in containment, they're made aware. If there is any criminal activity or anything else that might be associated, we would be contacting the appropriate authorities, being careful that we don't destroy any evidence along that process, we would be containing that breach and notifying the clients.

I know I've kind of outlined it in sequential form, but things really happen very quickly in the case of a privacy breach happening. The containment and the notifying of the client, notifying the appropriate staff within the department, those things are happening almost in real time to make sure that the client is appropriately made aware, but at the same time we are containing the potential impact that breach could have on the client.

I think another important piece is that we need to be able to explain to the client what we've done, the steps that we've taken to contain the breach. That's a critical piece of it as well.

Lastly, I guess to ensure that they are aware when it has been fully contained and resolved, and that we are providing the appropriate level of support throughout that process - so if there are any questions the client has, if there's anything additional that they need, that they know where to go to have those needs met, and that we are keeping the lines of communication open with that client and within the department taking appropriate steps to appropriately mitigate and protect against something like whatever the nature of the breach was from happening again.

[11:30 a.m.]

KEITH BAIN: I appreciate that because sometimes you'll hear people say, well, they didn't know about it until a lot of time had passed. Sometimes it's delayed because of the process to make sure things are secure in the first place. I just want to finish off by saying, you said that the majority of the breaches that have taken place are - we'll call them - minor. Regardless of the severity of the breaches, is the client always notified, even if it's a minor breach?

TRACEY TAWEEL: In cases of minor breaches such as a name being sent to another government employee for example by accident, we do not notify clients in those instances. We do, of course, notify clients if there's anything that could be potentially damaging or embarrassing to them - medical information shared, any information about services that they have accessed, are accessing currently, or have accessed in the past. Anything like that is, of course, shared with the client. Breaches that we would deem as more minor or lower risk, we don't notify the client in those instances.

THE CHAIR: Mr. Jessome.

BEN JESSOME: I'm trying to be general, but in terms of the succession that just took place, I'm not trying to be focused on the deputy specifically. My question is related

to how the department includes or embeds succession planning, with a focus on privacy. Deputy, you alluded to the level of briefing that you received and the immediate nature of the feedback that you received from the department. I'm wondering how that's embedded more generally and not limited to the position of the deputy minister.

TRACEY TAWEEL: Maybe I'll start very specifically first, with how it has been embedded in the process of my briefings. As I mentioned, just by happenstance, the first person I met was the manager of privacy. I had a very quick briefing with her immediately in terms of the work that she is undertaking. In addition to that, more formally, as would be the case with new staff coming on board, for me there have been a series of high-level briefings that touch on the key programmatic areas of the department. One of the very first briefings was focused on privacy and our responsibilities under freedom of information.

It takes a high priority, and it is embedded in all of the presentations and the briefings that I have received on a branch-by-branch basis. They have all spoken about the importance of privacy and confidentiality as well as in terms of the nature of the work that is done. More broadly, and having worked with the executive team, albeit for a short time, I can say that privacy responding to freedom of information requests and things like that are a regular feature of the standing agenda with that team that meets weekly. They in turn ensure that that has a sort of cascading effect within each of the branches that are under their respective purview.

Lastly, any new employee coming into Community Services is informed of all the mandatory training that they are required to take, as well as signing, as appropriate, confidentiality agreements, being informed of the Public Service code of conduct and values and ethics - all of which have elements of privacy and confidentiality and respect and integrity embedded within. That is a condition of employment, if you will. All employees, whether they are in DCS or in other departments of government, are informed of their responsibilities under those various codes of values and ethics.

At Community Services, I would say it takes a particular importance, given the nature of the information that some of our staff are privy to and the nature of the relationships that they have with Nova Scotians who are sometimes at their most vulnerable when they begin to work with us. It is of paramount importance that any new employee coming into the department understands what their requirements are. That is made clear both in terms of the support that their immediate supervisor would provide in terms of onboarding them, but also in terms of the corporate supports that are provided through our partners in the Public Service Commission, for example.

BEN JESSOME: That's a good segue into my follow-up. I did want to put a focus on new government employees, rather than those that might have had some experience with respect to those rules and requirements in another department. Can you speak to any opportunity for mentorship? I know you referenced supervisors, but is there any structure around mentorship that would include or lend itself to the policies and protocol around privacy and protection of information?

TRACEY TAWEEL: I don't believe at this point there is anything formal within the Department of Community Services with regard to mentorship in that particular area in terms of privacy. However, I would link back to some of my earlier comments - in terms of the training that is provided by our manager, who you're going to think is probably the busiest person in government because she runs all over the place.

Part of her role is making sure that any new employees that are coming on board receive the appropriate training. She in effect serves as a bit of a coach or mentor for all new employees, but also importantly - it's important for new employees, but we also need to make sure that current employees and long-standing employees who may have been in the department for 25 or 30 years, it is still of paramount importance that they understand the changing world that we're in and that the new digital platforms that we're all on and all of the technology changes, that they're aware of the potential impact that those could have on privacy and that they also pursue the appropriate training. It's not just for new employees - it's mandatory training for all employees every two years or every year, as I've been telling everyone.

THE CHAIR: Ms. Miller.

MARGARET MILLER: I only have one question and no supplementary. I want to preface this by saying that I believe all breaches are serious. We don't want to see anything coming out and becoming public or going anywhere it shouldn't be.

With that said, you've identified that there are different levels of breaches. Do you have a system to be able to identify those? When you report the breaches, are there different levels of severity and they're reported as such?

TRACEY TAWEEL: The answer would be yes, and the manager that I referenced would play a key role in triaging the breach and determining where it would fit in that scale of risk, if you will.

I would say regardless of the severity, however, or the level of risk, the same sort of triaging would take place in terms of getting the information back, recovering the records, and looking at risk - assessing how and why it happened and how we can prevent it from happening in the future. The notable difference would be if the client needs to be notified or if the client is notified or if the client is not notified, there is always an investigation that occurs. In order to properly categorize the nature of the breach, it's important that a thorough investigation occur.

Regardless of perhaps how the person reporting the breach might feel it's minor, the manager has expertise in assessing where it fits in the scale of risk. So there is always an investigation done to arrive at a decision in terms of what level of risk to apply.

THE CHAIR: Final question to Ms. Leblanc.

SUSAN LEBLANC: I was thinking back to my question about the new online services for DCS and I'm wondering, given that a lot of the services are going to be moved online - and I recognize there will be a not-online option, but given that you have heard from folks that they would like to have the online option, is the department considering providing an allowance for Internet service in the home of DCS clients?

TRACEY TAWEEL: I'm not sure I can answer that question. I have not had a briefing at that level at this point. What I can say is that I know the department is constantly, in particular through this transformation period, looking at how we improve the service that we provide to clients. I'll certainly undertake to ask that question as I get more deeply into briefings on the digital platform in particular. I'm not sure I can answer that question with 100 per cent certainty, but I will certainly take it back to the department. Again, given the culture of continuous improvement and wanting to make sure that clients have optimal opportunity to take advantage of our services, we are constantly looking at new opportunities to stay current and relevant to the clients that we serve.

SUSAN LEBLANC: I'll just end by saying, as you no doubt understand, the clients who are on income assistance and disability supports are among the very poorest of the province, and the idea that these folks can't afford phones, can't afford groceries, and many of them are having their power cut off this month because it's power cut-off season because it's now warmer - it's a difficult thing to imagine that these folks would be able to afford Internet service in the home. I would strongly suggest, in your new position, that you undertake the review of the amount of money that these folks are offered to live on and take into consideration the high cost of rent, power, Internet service, and phones when you are making decisions that affect these folks.

THE CHAIR: That concludes our questions and comments. I would like to offer our witnesses an opportunity for some closing remarks. Ms. Taweel.

TRACEY TAWEEL: I will just say thank you all very much for your questions today. We have endeavoured to answer as best as possible. If there's anything that you have follow-up questions on, feel free to reach out. I would be more than happy to have a conversation with you. In the coming weeks, I will know more, so hopefully our conversations can be productive. Again, thank you very much for your questions, and I look forward to working with you all in the future.

THE CHAIR: Thank you, DM Taweel and Ms. Lasheras. Ms. Chouinard, clearly, you briefed your new deputy minister well because you didn't take any of the questions. She took them all. Congratulations.

Thank you. It was a very informative discussion around a very important topic. Our witnesses can now be excused.

I think we can whip through our committee business very quickly and not need a break. We have one piece of correspondence with respect to questions on the Career Rising

program. It's some data that the committee asked for. Is it agreed to accept that letter? Ms. Leblanc.

SUSAN LEBLANC: I just wanted to recognize - and I appreciate the information - there's no demographic breakdown according to race, ethnicity, gender, or disability. I just wanted to flag that. I wondered why they wouldn't track that information. I don't know if they don't or not, but it's not in the letter. I was wondering, Mr. Chair, if you would be willing to follow up on the letter - I guess Brandon Grant is no longer in the position - to the new director of ESIA and find out if they, in fact, have that specific demographic information.

THE CHAIR: Would the committee like that information? All right. I'll ask the clerk to draft a note for me, and we'll endeavour to get that information. It's agreed to accept the letter.

Our next meeting will be September 3rd, and the topic will be legal issues on child protection witnesses.

With that, I would like to adjourn the meeting and thank you all.

[The committee adjourned at 11:44 a.m.]