IN-CAMERA **PROCEEDINGS BEFORE**

PORTFOLIO COMMITTEE NO. 1 – PREMIER AND FINANCE

INQUIRY INTO CYBERSECURITY

Resolved to be published by the committee on 19 March 2021

CORRECTED

Jubilee Room, Parliament House, Sydney,Wednesday 3 February 2020

The Committee met at 10:40.

PRESENT

The Hon. Tara Moriarty (Chair)

The Hon. Ben Franklin
The Hon. Taylor Martin
The Hon. Adam Searle
Mr David Shoebridge
The Hon. Natalie Ward

The CHAIR: Welcome to the second day of the Portfolio Committee No. 1 inquiry into cybersecurity. Before I commence I would like to acknowledge the Gadigal people, who are the traditional custodians of this land. I would also like to pay respect to the Elders past, present and emerging of the Eora nation and extend that respect to other Aboriginal people present. Before I commence I would like to make some brief comments about the procedures for today's hearing.

Please note that as this is an in-camera hearing, you are bound by the confidentiality of today's proceedings. Please also be aware that the Committee has the power to publish today's evidence if it chooses. The Committee's decision will take into account the confidentiality and sensitivity of the matters discussed. Should the Committee desire to publish some or all of the transcript, the secretariat will consult with you about what is to be published, taking into account your privacy. However, the decision as to what is or is not published rests with the Committee.

As you would be aware, your evidence today is protected by parliamentary privilege. It is important to remember that parliamentary privilege does not apply to what you say outside of your evidence at the hearing. So I urge you to be careful about any comments you make to the media or to others after you complete your evidence as such comments would not be protected by parliamentary privilege if another person decided to take action for defamation. There may be some questions that you could only answer if you had more time or with certain documents to hand. In these circumstances you may take a question on notice and provide an answer within 21 days.

Evidence in camera by **WITNESS A**, Private citizen, sworn

The CHAIR: [Name Suppressed], you are welcome to make an opening statement to the Committee.

WITNESS A: Thank you for having me today. It is a privilege to be here; the place is full of heritage, it is wonderful. Particularly on that matter, having a look at what has happened to us and my family regarding the cybersecurity breach at Service NSW has actually not only catapulted me to have a good, hard look at that matter but how I stand as one of the people of the Commonwealth. I brought my red Constitution today, which is the Commonwealth Constitution, and in terms of the context that I see myself in today, New South Wales has a constitutional responsibility to me to ensure that my rights and privileges as a member of the Commonwealth, as one of the people of the Commonwealth, is maintained.

I have gone back to the first principles to have a look at what is going on and I have spent many, many hours, many late nights researching not only about my situation but in the greater sense and I am not filled with a lot of confidence that we have a sufficient framework in place to take care of the people of the Commonwealth. I do not say that lightly, but I do ask the Committee today to take a good, hard look at their true constitutional position in relation to the people of the Commonwealth—to me—which is the Constitution at the time of Federation, and I notice that the New South Wales State Constitution has been replaced since that time.

It is hard to say, but I thank you for parliamentary privilege to say so, but in terms of the actual by- the- letter-of-the-law connection that I see New South Wales having to me through the Constitution, I have not found sufficient grounds to say that the Constitution that New South Wales is currently constituted with is providing a direct link to me as one of the people of the Commonwealth. I know this is outside the terms of reference, but in terms of dealing with this properly the Constitution is going to be the way to go. It is going to give the clout that is needed to have a look and to also having the lawful clout to take action because in terms of what happened with us with our breach I have spent many hours on the phone with Service NSW and I have had the run-around many times. My local member, Clayton Barr, has been helpful in that he has provided some information for me as to some extra evidence that I have tabled today, which was regarding the privatisation of IT.

So that is just a bit of setting for you. I have lost some very key data for myself: I have lost my birth certificate, my wife's birth certificate, my child's birth registration, my driver licence, my Medicare card and some credit card details as well. So it is a very serious matter that we deal with this today. Thank you.

The CHAIR: Sorry, in that statement you mentioned that you wanted to table a document, is that right, because there is a process for that to happen?

WITNESS A: That is fine. The other ladies [the secretariat] have copied these off for me, which I just want to pass around. There were a couple of links that Clayton Barr sent me when I had spoken to him on the phone about what happened to us and he said to me that Service NSW and some of the other systems that are in review have been outsourcing their IT and I think that is something to certainly investigate in regards to what has happened with Service, if it is something to sort of really zoom in on as to whether that was the problem or whether it is systemic. I do not understand how this place works, to be honest—I am just a member of the Commonwealth—but I am really trying to understand and trying to appreciate the work you do, but at the same time find a traceability there and I expect that this inquiry will actually have the powers that it needs to do something.

The CHAIR: Thank you. We are looking at this across a range of issues in terms of how this particular breach happened but also cybersecurity generally across government, but do you want to just talk us through what has happened with you, what the breach was in your personal circumstances?

WITNESS A: I got a letter from Service saying that my birth certificate was taken, my driver licence, my Medicare card and my child's birth registration and it was very ambiguous on that letter that they sent out to me in the beginning as to what those items were and I had to pump them for the exact information and actually work out—I mean, when you look at it from the top down, just a driver licence has your name on it, it has your location, it has your signature, it has your face and the actual amount of data is quite huge, especially when you even look at your birth certificate: my parents' details, where I was born and stuff. The network across the information is very comprehensive and I am concerned going forward, not just for the systems to be in place to manage this in the future, I am not just concerned about that because that is, to me, the Government's job to make sure that is right, but in terms of what we have permanently lost as a result of what has happened, and not heeding the Auditor-General's advice back in December 2019 has left us in this position and is it evidence of something else going on?

My neighbour said to me that his gun licence was hacked at the Firearms Registry. So I do not know whether this is just specifically targeting Service or whether it is system-wide review, I do not know, but there is some extra information for you to have a look into. I just do not get any confidence that the Government, as such, as far as the organisation is concerned, is taking care of the voter. The sovereignty of Australia rests with its people not with the Government.

The CHAIR: When were you notified of the breach? I think it is in your submission, but when were you told about it?

WITNESS A: I was told about it—I actually have the letter here, the original—on 7 September 2020. So that was potentially, I guess, four months after the event, and I noticed that they had to have time to work it out and who is the victim. When I first rang up to follow up off the letter they just said, firstly, "We want to apologise", and then they offered a reprint of my driver licence and some other things. I thought, just getting another driver licence card number is not the problem; it is that I have lost something permanently. Essentially, my legal fiction name has been lost. My wife was feeling quite stressed about it. She has been pregnant and has just had a child. In terms of the response we got from within the department, I have had to do all of the chasing and milking for information. By lodging an Information and Privacy Commission [IPC] complaint form I found out how to take it further because it was not presented clearly to me. It was not that they did not present it but it was not presented as what you could do if you were really unhappy.

I filled out the IPC complaint form and that took it to the next level to actually get a report out of them for the extent of the privacy breaches insofar as crimes are concerned. It is crimes, you know. I am speaking up today because there are potentially 186,000 other people. The initial inquiry into this was closed in September last year and the letters were going to keep rolling out until December. So a big swarm of angry ants—as far as the public is concerned—was unable to voice their concerns and their frustrations. I am here today as one person who can speak for many. I hope it has the same amount of weight.

The CHAIR: We appreciate that. Do you feel as though it has been resolved at this point?

WITNESS A: They have sent me an outcome letter, which I sent to you. I think it has been included in my correspondence with you. There was an outcome letter and that is as far as I have gotten with them. As far as listing all of the crimes—the breaches of the Privacy Act, exactly which documents, how it was related and all of that—that is all in there, which I have seen. I do not think it is up to them to take it further. They are dealing with managing their systems but the issue is greater than that because it is something a tribunal needs to hear. I have tabled it with the NSW Civil and Administrative Tribunal [NCAT] and I am going to self-represent in that regard against Service NSW. I think that they need to be held to account, to not treat people as customers. We are not customers; we are people of the Commonwealth and subjects of the Queen. In the name, "Customer Service", that this all falls under with Minister Domino's portfolio—no slander against that. But the name "customer" is exactly how I feel. I get good customer service in the centre but on the back end when all this happened it was very bad customer service. I do not like feeling like a customer.

I went back to the Constitution because it deals with us as living people, not as digits on the screen. I think that is the danger that this will fall into straightaway with our digital world. There is no constitutional basis for some of the new technologies that are coming out; there is no constitutional recourse for people. It is just coming in from the side with more and more systems being integrated. We are entering a digital world that will leave common law behind. That is the danger that I feel. I need to say very clearly today that there needs to be an immediate address of this. There needs to be, for lack of a better word, a referendum with the people of the Commonwealth to ask, "Do you want to enter this world that is coming?" Because it is responsible government to do so. I see what is happening, many others see what is happening and it is being foisted upon us all with more and more digital integration of everything. When it goes wrong, it goes wrong very badly. I am concerned that even government will lose clout in this scenario that is presenting itself.

That is why I have said we need to get back to our Constitution and even to the New South Wales State Constitution. That is why I brought it up, even though it is outside the terms of reference. I have paperwork here from Sir John See from the *Hansard*. He rushed through a brand new Constitution that was a re-enactment of the Constitution under New South Wales' banner—not under Queen Victoria's banner. That has changed the constitutional relationship between the people of the Commonwealth and this current New South Wales Government. Essentially, my view from my research—and I am a bush lawyer so take it for what you will—is that something so fundamental as that was rushed through and debate was silenced and members were gagged. It has probably been a burden to address but something as fundamental as that needs to be addressed. In terms of going forward and dealing with these things we have to have a proper constitutional basis for us to relate to our current government and to have a proper two-way discourse about matters that are at hand, our rights and what the Government is going to do to protect us from foreign interference. Some of this stuff comes under national

security, really—this being a corporation fits under the Federal Government's Corporations Act broad interaction. I hope that is okay to say.

The CHAIR: Of course. Thank you.

The Hon. ADAM SEARLE: I just have a couple of questions. You mentioned going to NCAT. Has Service NSW made you any offer to redress the data breach—whether money or any other kind of offer? Secondly, apart from the understandable distress of having your personal data compromised, are you aware of any other consequences? Are you aware of any third party trying to use that data to impersonate you or your wife? Have there been any other consequences of that kind that you are aware of presently?

WITNESS A: To answer your first question, as far as their remedy—I guess you would call it a remedy for my situation—I think their hands are tied. But they have somewhat offered, I think, $500 but it included things, from memory, that were along the lines of counselling and some other things. It is at NCAT because it is not addressing the crimes. The crimes need to be addressed. I am going hard for myself but I have to do it to set a precedent for everyone else that this can be done. That is where I am at with that. Sorry, I have forgotten your second question.

The Hon. ADAM SEARLE: The second question was about whether you are aware of any other consequences from the data breach—whether anybody has tried to use your or your family's data.

WITNESS A: Okay. I am not aware of that personally. I did my diligence to inform my bank and other places—certainly, Service NSW and getting new Medicare cards as well. I did that but, no. That is not a conclusion either because all it takes is a USB stick to take that data from wherever it has gone to somewhere completely unrelated. As I raised—I do not know if I put it in, but I have spoken to them before—in an age where crimes are becoming more rampant, people are desperate and they do different things that may not necessarily seem to be related to this event but could be based on data that has come from it somewhere. My children's details and location are known. My personal safety and children's safety are number one in my mind. If someone knew the ages of my children, where I live, what I look like, my signature and everything, and if they were to take them the police would look at it as a crime there and then. But they may not see a link between that and what happened with Service NSW.

That is why I have kind of thought to the extreme, but it is not really an extreme when you consider these people that are brazen enough to do this. If it is the same people that have targeted the Firearms Registry, who are they and what do they want to do? Certainly, in holding me to ransom, I would be ruined; I could not pay for the lives of my children, you know? That conversation always ended in the gutter with Service NSW because it is too big, too complicated. It ended in the gutter with the counselling service that they offered me. I think it was icare or one of those counselling services. I said, "Look, I've done the thing with changing passwords and stuff, but as far as the real problem of permanent data loss and safety risks, it's almost"—like, where do you begin? It is unquantifiable. It may not ever happen, but that is assuming in the positive that we can't necessarily do. Is that an answer to your question?

The Hon. ADAM SEARLE: Yes, it is. Those are my questions.

The Hon. NATALIE WARD: Thank you, [Name Suppressed], for coming along today. I am sorry to hear about your experience. It really is regrettable. I will be very brief because I think we are tight for time. You mentioned the counselling that was offered to you. Did you take that up?

WITNESS A: Yes, I did it twice over the phone. It was a bit salt in the wound to me just on account of saying them saying, "There, there," is not going to fix the real issue. I did appreciate the offer and I have said twice—I ended up speaking to the same lady twice, but we kind of ended in the same thing that I have done the immediate issues but—

The Hon. NATALIE WARD: Sorry. I do not mean to cut you off, but I am just trying to be quick.

WITNESS A: Thank you.

The Hon. NATALIE WARD: You were offered financial compensation. Is that right?

WITNESS A: I do not know if I have that in front of me. It was not in any way overwhelming, but I remember $500 was an amount. It did have a breakdown, I think, of what it was. If you want me to take that on notice, I can supply that.

The Hon. NATALIE WARD: That is okay. And you took that up?

WITNESS A: I haven't yet because I did not want to settle anything until this is looked at by the tribunal.

The Hon. NATALIE WARD: Was there anything else offered?

WITNESS A: No.

The Hon. NATALIE WARD: Counselling? Financial—

WITNESS A: Ongoing counselling—I kind of thought no. That is where we ended.

The Hon. NATALIE WARD: Mr Searle, my colleague, asked you about any consequences that you are aware of. I do not mean to be a lawyer, but were there any other damages or anything else that you can point to that has been a consequence of this breach at this time?

WITNESS A: Not physical. Probably just distress that my wife has felt in dealing with her own case manager; our cases are not rolled together. So she has been frustrated. She has been listening to what I have been saying. But she has been pregnant, so she has been stressed out by the thing to try and chase it up. We have felt like there has been a window of opportunity that if we can't sort it in that time or properly, then the stress of that is added to the situation which—

The Hon. NATALIE WARD: Presumably, she has been offered counselling as well?

WITNESS A: Yes, as far as I know, she was offered all the same things I was.

The Hon. NATALIE WARD: Okay. You referred to being a bush lawyer. Are you a lawyer? I am not saying it in a negative way—are you a lawyer?

WITNESS A: No. I am interested in the law, but I am not a lawyer.

The Hon. NATALIE WARD: Sure. Great. Somebody needs to be. What is your role? What do you do?

WITNESS A: My trade is a fitter and machinist. I work on heritage steam locomotives. Because of that, I think I just have a real interest in our ancient history.

The Hon. NATALIE WARD: I appreciate that, and thank you for the work you do. I am just asking this because you referred to Clayton Barr and, I think, Sophie Cotsis: Did anyone help you prepare your evidence today or the submissions?

WITNESS A: No, self-prepared. Sophie was helpful; Clayton was helpful. Sophie told me that she had been breached, so that was a thing in common we shared. Clayton was helpful in as far as the extra information on the digital side of things—Unisys and Infosys, I think they are called.

The CHAIR: He is your local member, right?

WITNESS A: Yes, Cessnock.

The CHAIR: Thank you so much, [Name Suppressed], for your time. We really do appreciate it. Thank you for all the work you have put into it.

WITNESS A: Thank you for having me. See you later.

(The witness withdrew.)

(Evidence in camera concluded.)

REPORT ON PROCEEDINGS BEFORE

PORTFOLIO COMMITTEE NO. 1 – PREMIER AND FINANCE

INQUIRY INTO CYBERSECURITY

CORRECTED

At Jubilee Room, Parliament House, Sydney, on Wednesday 3 February 2021

The Committee met at 11:00.

PRESENT

The Hon. Tara Moriarty (Chair)

The Hon. Ben Franklin
The Hon. Taylor Martin
The Hon. Adam Searle
Mr David Shoebridge
The Hon. Natalie Ward

The CHAIR: Welcome to the second hearing of the Portfolio Committee No. 1 inquiry into cybersecurity. Before I commence, I acknowledge the Gadigal people, who are the traditional custodians of this land. I pay respects to the Elders of the Eora nation past, present and emerging, and extend that respect to other First Nations people present. Today's hearing will hear from the Audit Office of New South Wales, the Information Commissioner and Privacy Commissioner, Department of Customer Service representatives, as well as the NSW Police Force.

Before we commence, I would like to make some brief comments about the procedures for today's hearing. Today's hearing is being broadcast live via the Parliament's website. A transcript of today's hearing will be placed on the Committee's website when it becomes available. Parliament House is now open to the public. All visitors, including witnesses, are reminded that they must have their temperature checked and register their attendance in the building via the Service NSW app. Please see the secretariat if you need assistance with this and please remember to maintain appropriate physical distancing at all times.

All witnesses have the right to procedural fairness according to the procedural fairness resolution adopted by the House in 2018. I remind everyone here today that Committee hearings are not intended to provide a forum for people to make adverse reflections about others under the protection of parliamentary privilege. I therefore request that witnesses focus on the issues raised by the inquiry terms of reference and avoid naming individuals unnecessarily. There may be some questions that a witness could only answer if they had more time or with certain documents to hand. In these circumstances, witnesses are advised that they can take a question on notice and provide an answer within 21 days.

IAN GOODWIN, Deputy Auditor-General, sworn and examined

SCOTT STANTON, Assistant Auditor-General, Financial Audit, sworn and examined

CLAUDIA MIGOTTO, Assistant Auditor-General, Performance Audit, affirmed and examined

The CHAIR: You are welcome to make a short opening statement. Perhaps one of you would like to do that.

Mr GOODWIN: We would like to thank the Committee for the opportunity to appear before and contribute to this important inquiry. Cybersecurity, as has been pointed out by previous witnesses to the inquiry, is an important strategic and critical area for the New South Wales Government sector. The ubiquitous nature of cyber attacks makes the scope of the inquiry relevant for the government sector and citizens of New South Wales. Safeguarding citizens' data, supporting the conduct of online transactions and ensuring the continuity of government services from cyberthreats is important to ensure that the people can have confidence that the Government is doing all they can to ensure a cyber-safe environment and limit the severity and impact of the inevitable risk.

As the State's independent auditor, the Audit Office plays a key role in assessing areas of risk to government and planning a proportional audit response. This includes the area of cyber risk. Our audit work program seeks to continually monitor and respond to the changing risk environment faced by the New South Wales Government, local government and university sectors that we audit. Our assessment of risk and our proportion audit responses are outlined in the Auditor-General's work order work program and her audit reports to the Parliament. This includes acknowledging that the risk posed by cyber attacks on government agencies is significant.

Over the last few years we have, in a number of our tabled reports, assessed and reported on agencies' resilience to cyberthreats and we continue to do more work in this space. This includes recently responding to a request from a Minister to conduct an audit following a high profile data breach. I would note that that audit was not an audit of the breach itself but rather the processes for managing customers' personal information. For your ease of reference, our submission to this inquiry—No. 6 dated 8 September 2020—includes extracts from reports tabled by the Auditor-General focused on cyber risks. Since that submission was made the Auditor-General has tabled, on 24 November last year, our internal control and governance report; on 10 December, the central agencies report; and on 18 December, the request audit titled *Service NSW's handling of personal information*.

Collectively, these audits identified the need to improve processes, to handle customer and business information to ensure its privacy, improve weaknesses in IT controls, including deficiencies in managing privileged users and password management, and prioritise and focus on implementing [audio malfunction] NSW Cyber Security Policy. The Auditor-General recommended for a second year that Cyber Security NSW and New South Wales government agencies need to prioritise improvements to their cybersecurity resilience as a matter of urgency. The Auditor-General's forward work program acknowledges cybersecurity as a significant risk along with other challenges. Agencies' cyber resilience will continue to be an area of focus and we will continue to monitor the risks and challenges and respond accordingly. I am joined today by Ms Claudia Migotto, our head of Performance Audit, and Scott Stanton, our head of Financial Audit, and we are happy to take any questions from the Committee. Thank you.

The CHAIR: Thank you for your original submission and also for noting in that statement that it does refer to some further reports that you were doing. I am certainly going to focus on one of them in particular today, which is the *Service NSW's handling of personal information* report that you did. You said in your recommendation—and it is clear in your statement and it is also clear in your report—that you have recommended that government prioritise cybersecurity. In your experience, are they doing that? You have been looking at this for a couple of years. Digital is increasing in terms of how government interacts with people. Do you see any sense of urgency in terms of how this is being dealt with by government?

Mr GOODWIN: Yes. Thank you for that question. I think that is a really important question because on the one hand we have said that this is an area that needs priority and needs attention, but that does not mean that it is not getting priority and it is not getting attention. It is a journey piece and, in many senses, because of the ubiquitous nature of the risk, it is very hard to get a defined end point and so you are constantly evolving your risk management practices to the constantly evolving threat environment. What I would acknowledge, and I think it is important to acknowledge, is that since the performance audit in 2018 which recommended that there should be a whole-of-government response, there has been a series of government responses.

Those government responses include the establishment of Cyber Security NSW and the establishment of a cybersecurity policy subsequent to 2018. In addition to that, it is my understanding that the Government has allocated about $240 million to deal with cyberthreats and, indeed, it is certainly my understanding that the secretaries board, through the Department of Customer Service, has got a very focused attention on cyberthreats. The short answer to your question is that it is getting attention, but it is a complex area and that is why we are saying it needs priority.

Mr DAVID SHOEBRIDGE: Thank you all for your work throughout the year as well as the submissions and the audit reports you did. I might drill down on some of the findings in your December report into Service NSW. First of all, the personal information of more than four million residents in New South Wales had been phished and accessed with a very large privacy breach. That was what led to a referral to your office to commence that inquiry into Service NSW. Is that right?

Mr GOODWIN: Yes.

Ms MIGOTTO: The number that we had to hand at the time of this audit or that was provided to us by Service NSW—and this is not audited information but we do reflect it in our report—is around 186,000 residents impacted and five million documents, individual documents, were released as part of that phishing attack and about half a million of those contained personal and private information.

Mr DAVID SHOEBRIDGE: This attack was made possible because of those serious security weaknesses that were in Service NSW insofar as large amounts of residents' information was being passed from Service NSW to various partner government agencies by way of email. Is that right?

Mr GOODWIN: I would just acknowledge, as I said in the opening statement, we did not audit the breach itself; what we did audit was the handling of the personal information. There is a limit to how much I can give you a definitive answer given the parameters of our audit. But it is true that information within Service NSW is passed via email and that was subject to phishing attacks. There are mitigation strategies that can be put in place that will enhance and harden against those phishing attacks, but they are about hardening not about foolproofing.

Mr DAVID SHOEBRIDGE: Is it true that, in fact, the reference you got about this very substantial data breach, which on the basis of Service NSW information is hundreds and hundreds of thousands of personal records—you were not tasked with actually investigating that breach at all? Is that right?

Mr GOODWIN: There was a very, I would say, coordinated and quite an extensive approach to investigating how that data breach occurred. There were experts that were brought in to deal with some of the technical aspects of the breaches and we were brought in to—that information of what those technical experts did to look at that data breach was made available to the audit. So it was not so much that we were excluded from it, I think it was about finding the right resources to deal with the right questions.

Mr DAVID SHOEBRIDGE: But I am reading from your report here and your report identifies:

> One of the business processes that was a key contributing factor to the data breach was the emailing of personal information by Service NSW staff to client agencies.

Mr GOODWIN: That is correct.

Ms MIGOTTO: That is correct. We investigated that as part of a personal information management and privacy protection issue.

Mr DAVID SHOEBRIDGE: But your investigation also found, if I am correct, that Service NSW knew this was a major risk, knew it had a vulnerability here and was given notice of that prior to this large data breach. They were on notice before the data attack happened. Is that right?

Ms MIGOTTO: That is right. Internal risk reports had identified this process of emailing information as a risk around 12 months before the breach had actually occurred.

The Hon. ADAM SEARLE: Your report of 18 December in relation to the Service NSW handling of personal information on page 17 talks about the lack of a multi-factor authentication process being a risk. This risk was identified in a 2018 audit. Service NSW was supposed to remedy that by 30 June 2019. It had not done that, and this was in fact a key vulnerability in the 2 March 2020 attacks.

Service NSW was told what the problem was, there was a time frame for compliance, it did not happen, which enabled these breaches. This multi-factor authentication is a pretty standard approach used even on Gmail; it is used in banking; it is not radical or new. What comfort can we take that Service NSW is actually ever going to address the very many deficiencies you have identified not only in your 20 December 2020 report but in all the other five reports you refer to in your submission where vulnerabilities right across the public sector are identified by you? When will Service NSW lift its game?

Mr GOODWIN: There are elements of that question that are probably best answered by the Department of Customer Service in terms of the actions that they have since taken, but it is my understanding that, on the question of multi-factor authentication, that has now been put in place.

The Hon. ADAM SEARLE: That was just one weakness. You have identified very many and they just do not seem to be able to, in a timely way, get their act together. Looking at your other five reports that you have mentioned, there are many recommendations. Can we have comfort that these agencies are implementing your recommendations in a timely and a robust fashion or should we be concerned?

Mr GOODWIN: In this most general sense I think, because of the ubiquitous nature of cyberthreats, everyone should always be alert and I would use the phrase "alert" rather than "alarmed". As I say, the Department of Customer Service is going to be better placed to talk to the actions that they have since taken, but the context is important here. The context is that the New South Wales Government over the last two years has put resources, investment and policies in place to deal with cyberthreats. Those things take time and my experience at the Commonwealth level is that they do take time and, when you are dealing with complex systems, there is a degree of complexity around it. It is not as simple as putting in place multi-factor authentication when you have got disparate and complex systems which sometimes are legacy systems.

The Hon. ADAM SEARLE: The State Government constructed these systems and made them operational without putting in place these safety measures.

Mr GOODWIN: As I said, it is a journey piece and there has been a significant journey since the 2018 performance audit, which is why we recommend that priority has to be placed in terms of dealing with cyberthreats and why we have put in our central agencies report where agencies are in terms of their maturity levels against the Essential Eight mitigations strategies. Multi-factor authentication, though, is just one of those strategies and it is not the only strategy that is going to prevent a cyber breach.

The CHAIR: I think we can accept that that is just one strategy, but you are saying that there has been a journey within government since 2018 and your recommendations that you made then but your report into Service NSW handling of personal information from just a month ago, in December, is pretty damning and says that Service NSW is not effectively handling personal customer and business information. That is two years later. This is two months or six weeks ago that you have handed down this report with some urgent recommendations for Service NSW to implement by next month. If this was a business, if this was a bank, if this was happening in the real world, this would not be good enough. It is not good enough to say that it is a journey, particularly given that the Government is trying to force us into a more digital world at a rapid pace, which is also something that you found in your report.

Mr GOODWIN: If the word "journey" is capturing attention, what I am trying to set out is that there is a context. Yes, our report does find that there were weaknesses and our report has made some pretty robust recommendations and the department has agreed to implement those recommendations. But there is an important context that this is a complex space and these are complex systems and it is not as simple as just switching on a switch. I am not trying to downplay the threats, because the threats are outlined in the Auditor-General's report. What I am trying to just do is provide a context that it is a complex area and it does requires prioritisation and it does require leadership and focused attention, which is why we have made that recommendation.

Mr DAVID SHOEBRIDGE: I accept it is complex and I think you are right to point out it is complex, but there are some aspects of this that are just simply bad practice and one of them is sending large amounts of personal information with often detailed, deeply private data in it by email and Service NSW is still doing that, isn't it?

Ms MIGOTTO: At the time that we published this report they were certainly still doing that.

Mr DAVID SHOEBRIDGE: I will read from your report. It :

> Service NSW has not put in place any technical or other solutions to avoid Service NSW staff having to scan and email personal information to some client agencies.

So far as we know, at least as at 18 December last year, they were, with all of the data vulnerabilities in place, still emailing personal information about hundreds of thousands—potentially millions—of residents. Is that right?

Ms MIGOTTO: That is correct. During the conduct of the audit some improvements were made to ensure that the possibility of breaching large volumes of information held in storage and email accounts was reduced. It was risk reduction, not removal. And that was automatic deletion of email archives at a particular time and reinforcing with staff the need to double delete emails, so you delete it from your inbox and you delete it from your deleted files as well. So those practices were put in place—

Mr DAVID SHOEBRIDGE: They probably learnt them from the Premier.

The Hon. NATALIE WARD: I object to that.

Mr DAVID SHOEBRIDGE: Sorry, I'll withdraw it.

Ms MIGOTTO: —but certainly the practice of emailing was still going on.

Mr GOODWIN: I will just emphasise the point that Ms Migotto said. It is true what you read in the report, 100 per cent, but it is not necessarily true to suggest that the controls that existed at the time of the data breach are the controls that exist now, because those controls by the Department of Customer Service certainly have been enhanced and they are better placed to talk about the measures that they have taken.

Mr DAVID SHOEBRIDGE: But you are not resiling from your report's conclusions that sending large amounts of personal data and information by email is a security risk that should be removed from Service NSW?

Mr GOODWIN: It is not a good practice.

Mr DAVID SHOEBRIDGE: Indeed there are numerous alternatives to that to share data between agencies in a much more secure way. Can you detail some of those?

Mr GOODWIN: In terms of detailing the alternative strategies the Department of Customer Service are going to be better placed to talk through those things. Our report stands, but I am just trying to be helpful and just trying to provide context. But the business of government has to continue to go forward and so, given these are complex systems and there are a series of prioritisation decisions that need to be made, the first step you would expect to do is that there is some strengthening of the processes around that. It does not support a good practice, but what would be disappointing is if they just continued on with the existing practice without any enhancement and that is simply not the case.

Mr DAVID SHOEBRIDGE: Your report shows they have put some bandaids on, but they have not fixed the essential problem, have they, in this regard? They put some bandaids on it but it is still a nasty problem that has not been fixed.

Mr GOODWIN: There are fixes being put in place and, to be fair to the Department of Customer Service, they are better placed to answer where they are at the moment. It is very easy to focus on the technical aspects to this but there are a series of governance and people aspects that are attuned to this as well—an awareness of it and governance and focus on that.

Mr DAVID SHOEBRIDGE: Trust me, I want to come to that. Often we focus on all the technical risks as though the major risks are some kind of technical phishing attack or a cyber attack, but in actual fact some of the real problems here are the way in which people engage with data—the lack of clear roles, the lack of auditing of access to data—and it is those people-based risks that I will move on to. But perhaps the Opposition has other questions on the technicals.

The Hon. ADAM SEARLE: Reading your December 2020 report, there were a number of echoes of the shortcomings that were identified in the 2018 report. I note you have said that Service NSW has agreed to fix these problems, but are there clear time lines for the fixing of those problems and what monitoring is going to be undertaken by your office or anybody to make sure that these fixes are done as and when committed?

Mr GOODWIN: I might just ask Ms Migotto to talk to the time lines. Then I will just come back to the monitoring aspect.

Ms MIGOTTO: The time lines for our recommendations are sequenced, reflecting the steps that need to be taken to progressively close down the vulnerabilities that we see here. There are several actions that they have agreed to take by March of this year and then several that follow in June and December of this year as well.

The Hon. ADAM SEARLE: Will you be following up later in the year to see that that has actually happened?

Mr GOODWIN: In terms of the follow-up, I guess, there is a dual aspect to this. I think it is important to acknowledge that the primacy here is—as the auditor, we have made the findings and we have made the recommendations. It is now for management to get on with the job of implementing that and putting in the investment and the leadership and cultural focus to put those strategies in place. And the governance on that is for the Audit and Risk Committee to play a role in supporting management as they oversight governance and audit and risk matters within Department of Customer Service. From a governance perspective, that is where the monitoring primarily should focus. In terms of our role, obviously, we conduct the financial audit of the department. We attend those audit and risk committees. We will be proportionate in our response to how management are progressing on that or how the Audit and Risk Committee is doing it. But I think it is important

to acknowledge where the responsibility for the follow-up and monitoring sits and that that sits within the department's own governance structures.

The Hon. NATALIE WARD: Thank you, Mr Goodwin, Ms Migotto and Mr Stanton, for your assistance. I appreciate it. Mr Goodwin, in your earlier comments you stated, I think, that we should be alert rather than alarmed. Can I ask you to elaborate on that and tell us why?

Mr GOODWIN: Yes. One is that there are responses and there are steps being taken. I think, as the Audit Office, we would be alarmed if there had been no action taken since the 2018 audit. That audit did find that there were things that needed to be done. But things have been done. As an auditor, when you are looking at how recommendations are implemented, you are looking at probably three things I guess: one, leadership, two, investment; and, three, culture. So, while we are not auditing what the Secretaries Board does, I am aware that the Secretaries Board is now providing that leadership because they are engaged in the conversations on cyber. There is that investment. Now, one could always talk about whether the investment could be more. Obviously, with more, you can do more. But there is that investment.

The Hon. NATALIE WARD: You mentioned $240 million has been invested.

Mr GOODWIN: That is my understanding.

The Hon. NATALIE WARD: That is not insignificant.

Mr GOODWIN: Then one is culture. Culture gets to staff training and staff awareness. But the culture is led by the leadership. The trickle-down effect of that is where we are saying that there has to be a priority placed on cyber. When I look even at our own office and the Essential Eight mitigation strategies—we were not in a place in 2018 ourselves, but we are now. The conversations that happen in our organisation around cyber, both at the leadership level and in the staff training, have been enhanced. So that is, I guess, looking now to be replicated about the government sector. But it starts with the Secretaries Board. It starts with priority being put into investment. That's why I say "alert rather than alarmed", because steps have been taken. But the ubiquitous nature of this threat is that you never really get to an end point. So you simply can't say, "I get to level three in maturity across the Essential Eight. Job done," because the threat evolves and your risk management processes need to evolve.

The Hon. NATALIE WARD: Would you agree that the proposition in 2018 is quite a different one to the proposition in 2021—I am a person that still has a paper diary, so I am no expert. But it is evolving. Would you agree that the threats in 2018 are quite different and it is an ongoing battle, if I can call it that?

Mr GOODWIN: Yes. The threats definitely evolve. The threats were there in 2018. But they are certainly there now. I think when you look back on 2020 and the challenges that were put on the public sector to work remotely for periods of time and have people working in an online world just being more vulnerable—that is why, I guess, I say you do need to be alert to these threats.

The Hon. NATALIE WARD: I will defer to my colleague, but I just have one more question on that. You mentioned that you cannot just stop; it would be ideal to drop everything, stop, shut it all down, fix it and then resume but you have to continue business. Could you just tell us why you felt inclined to say that?

Mr GOODWIN: Yes. As an auditor, I probably will always come from the lens of fixing the risks. But if you are sitting in a program delivery area, you do have the job of delivering services to citizens and ensuring the business of government continues.

The Hon. NATALIE WARD: For example, if you are rolling out a QR code in the middle of a pandemic, you might want to prioritise that, potentially.

Mr GOODWIN: Government is going to make their own priorities of what they need to do. The pandemic is a good example of just how priorities do shift. Things get rolled out quickly and then you adjust along the way, but the business of government needs to continue. I guess it just can't continue in an unsecured manner. The risks need to be managed. Now, there is a duality here. In our central agencies report, we do give the aggregate levels of where government agencies have self-assessed on their maturity level against the Essential Eight. We do recommend that Cyber Security NSW and agencies need to give more attention to this because there are a lot of agencies that sit at either level zero or level one. But if you compare that to 2019, it is an improved situation. There is improvement. But we are not at a point where we can say the job is done. The attention needs to remain focused on it.

The CHAIR: I have just one follow-up question to that. I think we can all accept that the job will never be done in this space because the hackers will continue their work and whoever else is trying to access our information will continue to do it. But surely, from the Audit Office's perspective, government should be at least

having some better processes in place. You have made recommendations as we have heard today and in your reports from 2018. Since then we have seen what has happened with this particular data breach from Service NSW. But you don't just look at Service NSW; you have been reviewing a number of departments. The police are investigating crime organisations allegedly organising to use data to access bushfire funding illegally. There are two parts to the question. Do you think that there should be at the very least consistent approaches from government rather than an ad hoc situation depending on what each department decides that it wants to do? Do you think that there should be mandatory notification to the public on this, given that the Service NSW breach is the biggest one that we are aware of but there was no obligation for them to tell the public about it?

Mr GOODWIN: On the first question of consistency, it is a good question because consistency comes from policy and consistency comes from application. The Department of Customer Service probably can speak to this, but at the policy level they do now have a cybersecurity policy and they do have 25 what they call mandatory requirements. One of those requirements is a self-assessment against the Essential Eight mitigation strategies. But it goes beyond that. Those other 25 deal with governance, deal with staff awareness and other security matters. That is its policy. So, I guess, from a policy perspective, there is now a consistency. Agencies are required to do those self-assessments. They are required to do that attestation and report back to Cyber Security NSW. Indeed, if you do get a cyber incident, you report that back to Cyber Security NSW. The consistency, though, at the application level is probably where focus can be put. So I would say the policy level exists. The regulators put something out.

But the reason, when you look at where people sit, agencies sit—and there are a number of agencies at level zero or level one or level two. There is an inconsistency in the application there. Now, we haven't audited as to why that sits across the large number of agencies or tabled an audit report at this point on why that exists. It is going to exist from a range of factors, being complexity of system—but it is also going to exist around leadership and priority of focus. What we are saying in the recommendation in our Central Agencies report is that there needs to be that priority focus, and that comes from a leadership and a culture perspective. That is where I take some comfort that the Secretaries Board is playing a role there in ensuring that there is a conversation around cyber. But it is true, I think, to your point that more can be done in terms of the application at agency levels around what they achieve.

The other side to the consistency is where our policies sit. So we do have a policy—the New South Wales Government—but where our policy sits vis-a-vis relative to other States at the national level, and the Commonwealth has had a policy around cybersecurity going back to I believe 2013 and that policy has evolved over time. Now that policy does recognise some aspects that the New South Wales Government policy has and the New South Wales Government policy has other aspects that they have enhanced in terms of those other 25 mandatory requirements, but they do sort of largely align. I guess the difference though between the State and the Commonwealth level is that the Commonwealth level mandates achieving certain levels of maturity, whereas in New South Wales we mandate in a self-assessment but not baselining a minimum level to be achieved. How that evolves is a policy decision for the New South Wales Government, but from a consistency level you can explore the differences that exist between the Commonwealth level and at the State Government level, particularly as Commonwealth and State government departments interact.

The CHAIR: Does your office have a view on the mandatory reporting?

Mr GOODWIN: In terms of mandatory reporting around breaches of privacy of information, I might suggest that that is probably a question better asked of the Privacy Commissioner who I believe is going to be here this morning.

The Hon. ADAM SEARLE: In the room, in fact.

Mr GOODWIN: But I think we are on the record that transparency is an important part of accountability within government.

The Hon. ADAM SEARLE: A number of the questions I have asked have been about your various reports identifying problems and how we can have confidence knowing that the agencies have addressed those. For example, I note that it is five years ago to the very day that there was an unidentified attempted hack on the mining database held by the then Department of Resources. As I sit here I have no idea whether their vulnerabilities that existed then have been addressed by that agency. So, again, what mechanisms or what oversight processes should we be putting in place to make sure that all the shortcomings that you have identified in your five or six or seven or eight reports you mentioned this morning are actually being addressed by these agencies? What is a systematic way we can provide comfort to the people of New South Wales that the deficiencies you are shining a light on are in fact being addressed in a timely way?

Mr GOODWIN: Thank you. That is a really good question and it gets to the question of incentives to make sure that the priority is being put forward into cyberspace. My own experience is that at government level, and certainly at the Commonwealth level, people are challenged with a whole range of challenges that they are dealing with and you are being asked to prioritise things, and it is probably fair to say that cyber five years ago was not at the top of the priority list. But there is much more conversation now around cyber and what we are looking for, essentially, is that it remains at the top of the priority list. In terms of getting comfort, I think there is a series of things. There is a baseline now. So the baseline is that there is a policy; that policy requires agencies to self-assess; that self-assessment is provided to a central point; and there is a requirement for accountable authorities, such as chief executives and secretaries, to provide an active station around that. But that information is not made available necessarily to the Parliament—

The Hon. ADAM SEARLE: This is my point.

Mr GOODWIN: —or to the public. There is a question around how much you do make available because what you do not want to necessarily do is outline a vector for a state actor to take advantage of. But you do want to provide some incentives in the system to ensure that leaders across the Government are focused and giving this a priority of attention. And I think there is something that we continue to work through with the Department of Customer Service in terms of how we have published the information around where the self-assessments sit at an aggregate level rather than an agency level. But there is a question around what the incentives are to make sure that leaders within the public service remain focused on cyber. But you do have a baseline and that baseline now is certainly in its second year and established.

Mr DAVID SHOEBRIDGE: The New South Wales Government has been collecting perhaps some of the most comprehensive data about our movements and our whereabouts over the last 12 months that you could imagine through the COVID-19 Service NSW app. Do you agree that there is a huge amount of data being gathered in that?

Mr GOODWIN: I am not within the department so I could not speak to the details around the metadata that is collected, but it is fair to say that if you go into a place and you are required to provide a QR code, as I was required when I came into this building—

The Hon. ADAM SEARLE: We know where you have been, Mr Goodwin.

Mr GOODWIN: Exactly.

The CHAIR: Well, the Government does; we do not.

The Hon. NATALIE WARD: And that is a good thing for contact tracing.

Mr GOODWIN: There is a lot of data being collected, but I think the context in which it is being collected is important and the rollout and the spirit of that rollout—the spirit of the rollout is important to acknowledge.

Mr DAVID SHOEBRIDGE: I understand that there is a need on a public health basis to have data and be able to trace what people's movements are in order to track down an outbreak in a pandemic; I understand that fully. I understand that there are health exemptions under the privacy principles, but what troubles me is Service NSW's privacy management plan does not address the COVID-19 app. Service NSW's privacy management plan does not address the health exemptions. What comfort can we have that that data being gathered by Service NSW is secure and is meeting the privacy and the cybersecurity requirements of the State Government?

Mr GOODWIN: We have obviously not done an audit on the data that has been collected around the COVIDSafe app and the system around that, so there are real limits on what I can say there. But equally what I would suggest is that while the department was not looking to be hacked and have the breach that occurred, there was a very focused attention in terms of resources being pulled in to deal with that and give it a priority to sort of enhance the systems. But they are going to be better placed to talk about the controls that they have around the COVIDSafe app; we have just not done an audit on that.

Mr DAVID SHOEBRIDGE: But is it true that Service NSW's privacy management plan—and I am reading from your report—does not address how it deals with health information and the exemptions of health information. It is true, is it not, that they are getting this large surge of information through the COVID-19 app?

Ms MIGOTTO: It was certainly true at the time of this report. I cannot speak to whether in the subsequent weeks they have made improvements to that.

Mr DAVID SHOEBRIDGE: But surely from an auditor's point of view when these big new data captures are being designed they should be co-designed with privacy at the same time. What we have seen yet

again from Service NSW is a bunch of new data capture happening and then later on they may tack on some privacy controls. Surely we should be looking for co-design and that is what has been missing in Service NSW.

Ms MIGOTTO: If I could just point to a section in the report that might be helpful to the Committee, and certainly something that you may wish to follow-up with the privacy Commissioner later on and is referenced in the report, which is the concept of privacy by design—which I think is a point that you are trying to get to—which is an internationally recognised principle where if you are designing systems, be it a customer service system or any system that holds personal and private information, privacy is a core element of how that system is designed. So I think it is fair to say that there was an absence of that in the systems that we saw in the Service NSW handling of personal information but that principle is certainly stepped out in our report and it is something that you may want to look to for systems that do capture large amounts of personal information in the future.

Mr DAVID SHOEBRIDGE: Given the findings in your report and the concerns that you had as at 18 December regarding Service NSW's privacy controls, what are the risks in terms of access to that data gathered by Service NSW in the COVID-19 app? But I am also thinking of the data that they gathered, for example, in border permit applications—huge amounts of quite detailed personal information. What are the risks regarding those pools of data?

Mr GOODWIN: At a general level the risks obviously are self-evident, that if a threat actor was able to get into the system they get the data. But, I am not in a position to articulate the likelihood of that because we as an office have just not audited that particular system. So, it would not be right for me to be able to provide an answer to that.

The Hon. BEN FRANKLIN: Thank you very much for being here today. I go to the final pages of your submission which in particular refers to the performance audit of 2018 in detecting and responding to cybersecurity threats. I understand that you are conducting another audit now and you may not be able to specifically address this issue. I would be grateful for any comments that you can make on one of your recommendations, number five, which was about pulling back slightly that the entire New South Wales public sector threat intelligence gathering and sharing should include formal links with Australian Government agencies and private enterprise and other States. I wonder if you can make any comments as to how that has progressed, what situation it is in now and if you have any further recommendations that you can mention? I understand that you are doing the audit now.

Mr GOODWIN: Certainly we are doing a compliance audit on how people are doing the self-assessments and a separate cybersecurity audit. I can answer that at a general level but I think the Department of Customer Service can be better placed to give you the specifics on that. But, we do now get alerts from Cyber NSW, and those alerts alert you to a particular malware or phishing attack or threat. In fact, oddly enough, just as I sat down here I received and email from my own chief information officer [CIO] staff who are responsible for cybersecurity around the Information and Privacy Commission and a new threat has been alerted to. The point is that there is now a process where those sort of alerts do come forward out to government agencies and there is a community of practice for CIOs made available to talk through those issues. We have obviously not audited how Cyber NSW interacts with the Australian Cyber Security Centre, but having had conversations with people in the department, it is self-evident that they are in those sort of conversations, but they are better placed to talk at a granular level how they occur.

The CHAIR: We are done with this portion of the hearing. Thank you very much for your time, I appreciate it.

(The witnesses withdrew.)

SAMANTHA GAVEL, Privacy Commissioner, Information and Privacy Commission NSW, sworn and examined

ELIZABETH TYDD, Information Commissioner and CEO, Information and Privacy Commission NSW, sworn and examined

The CHAIR: Welcome to both of you. You may make a brief opening statement if you wish.

Ms TYDD: I welcome the opportunity to appear before the Committee in respect of this inquiry into cybersecurity. The Government Information (Public Access) Act—or GIPA Act, as it is known—falls within the terms of reference of this inquiry as it relates to public access to digital information, including information accessed by mobile-based and online platforms**.** Robust cybersecurity and information access rights both contribute to sound information governance practices by government, but they contribute in very different ways. The Information Commissioner has responsibility for overseeing the information access right enshrined under the Government Information (Public Access) Act. These rights are realised by agencies authoring and encouraging proactive public release of government information and by giving members of the public an enforceable right to access Government information.

The role of the Information Commissioner is established in statute and mandates independent oversight of agencies in exercising functions under the GIPA Act. As an agency the Information and Privacy Commission's independence is secured by the Government Sector Employment Act. Importantly, the Information Commissioner must also independently advise agencies and citizens and monitor, audit and investigate agency decisions and performance. The proper exercise of these functions necessitates consideration outside the purview of cybersecurity and therefore my statutory functions must be distinguished from the functions of Cyber Security NSW, for example. However, as government increasingly harnesses digital information and delivers services through mobile and online platforms, new opportunities and risks arise in the legislated right to access information.

I hope to offer the Committee insights into the discrete operation of information access rights within a much broader area of cybersecurity. The New South Wales Government has led the way in the development of digital government and the implementation of new and innovative service delivery for citizens. As the New South Wales Government continues to implement its digital transformation agenda, including the use of artificial intelligence and automated decision-making, maintaining and enhancing cybersecurity capabilities of the public sector is vital to protecting the security of its information assets. My role requires a contribution to the development of public sector capabilities, systems and processes that preserve the right to access information as technology and data is applied to make informed decisions and deliver better services.

The Information and Privacy Commission is playing a leading role in expanding the capabilities of the New South Wales public sector through the production of resources, including statutory guidance, fact sheets, and importantly, the regular provision of advice to agencies and citizens regarding the preservation and exercise of rights in digital government. As government increasingly adopts digital technology it has a duty to implement administrative practices that safeguard the legislated commitment to open government and the fundamental right of access by citizens to government information. Digital government necessitates adapting existing practices to the digital environment to futureproof the right to access information.

My *Report on the Operation of the Government Information (Public Access) Act 2018 - 2019*, which is the most recent report, recognises three fundamental changes in the way government makes decisions and delivers services: digital government and data application; increasing partnerships and outsourcing arrangements, and; novel models of government that transcend traditional sectoral arrangements. The development and implementation of new technologies and new modes of service delivery have the capacity to enhance the citizen's experience of government. At the same time, these developments introduce potential new risks of harm. Maintaining the trust and confidence of citizens that their rights will be protected will contribute to the success of digital government. Thank you.

Mr DAVID SHOEBRIDGE: Given the shortness of time, if we have openings that are of a very general nature like that perhaps they could be tendered and we could incorporate them into *Hansard*.

The CHAIR: Sure. We have one more. Let us see how we go.

Mr DAVID SHOEBRIDGE: If it is of a very high level generalised nature.

The Hon. ADAM SEARLE: Indeed. Let us move on.

Ms GAVEL: I think some of this is relevant to the inquiry. I welcome the opportunity to appear before the Committee in respect of this inquiry. As Privacy Commissioner my role is focused on the promotion and

protection of privacy. My legislative functions enable me to carry out my role in a number of ways, including by assisting agencies to comply with privacy legislation, publishing guidance for agencies and an oversight role in relation to internal privacy reviews about alleged breaches of the Information Protection Principles by agencies. It is important to note that cybersecurity management across government extends beyond my jurisdiction as Privacy Commissioner, which relates to personal or health information and not to government data generally. It is also important to note that privacy protection is much broader than security alone, although good security is essential to ensuring privacy. Privacy is also about safeguarding citizens' privacy rights through requirements that include ensuring information is collected lawfully, enabling individuals to access their information and the lawful use and disclosure of information.

The Privacy and Personal Information Protection Act, or PPIP Act, and the Health Records and Information Privacy Act, or HRIP Act, govern the collection, use and disclosure of personal and health information by New South Wales government agencies and, in the case of the HRIP Act, private healthcare providers. Both impose specific obligations on New South Wales public sector agencies to ensure they put into place reasonable security safeguards to protect personal and health information. Cybersecurity is an integral part of the security safeguards which an agency should implement to satisfy the requirements of the Acts. The adoption of a strong cybersecurity environment is an essential precondition to building and maintaining robust privacy protection information governance systems. There is an important link between strong and robust cybersecurity measures and the protection of personal information. As Privacy Commissioner I support the promotion and implementation of robust cybersecurity measures by agencies.

The cyberthreat landscape includes the development of rapidly evolving technology and techniques by malicious actors. This means that managing the cybersecurity environment of New South Wales agencies will require sustained and ongoing commitment and resourcing now and into the future. It requires a whole-of-government and collective approach involving not just the Department of Customer Service, Cyber Security NSW and the technical staff within agencies, but also agency executive teams and individual staff members. We all share and have a role in contributing to a strong cybersecurity environment, including through reporting awareness, capability development and uplift. The IPC contributes to this approach in a number of ways, including through the provision of guidance and tools for agencies, consulting with agencies on digital projects that involve personal information and oversighting internal privacy reviews.

Currently the PPIP Act does not impose an obligation on public sector agencies to notify either the public or the Privacy Commissioner in the event of a data breach incident. In 2018 I commenced quarterly reporting of voluntary data breach notifications received from agencies. As Privacy Commissioner I strongly encourage all public sector agencies to report data breaches under the voluntary scheme and I have published a range of resources to assist agencies to manage and respond to data breaches. This includes a data guidance document, notification forms and a data breach prevention tool and checklist. During the reporting year 2019-20 I received a total of 79 breach notifications, which represents an increase of 23 per cent over the previous year. This is a sizeable increase in a scheme that relies on voluntary reporting. Noting the increase in the role of digital service provision and the rapid growth in data that accompanies this, I am a strong advocate for the implementation of a mandatory data breach notification scheme, which includes a requirement to notify both the Privacy Commissioner and the affected individuals where a data breach results in or is likely to result in a serious risk of harm to the individual.

The introduction of such a scheme would provide a significant contribution to protecting privacy and enhancing cybersecurity in New South Wales in a number of ways, including by encouraging agencies to elevate capability; to prevent, mitigate and manage the risk of data breaches; providing citizens with information needed to reduce their risk of harm following a serious data breach; and increasing citizen trust in government and agency handling of personal information and data breach incidents. I welcome the commitment made by the Attorney General last year to introduce a mandatory data breach notification scheme for New South Wales agencies. The Department of Communities and Justice [DCJ] released a discussion paper on mandatory notification of data breaches by public sector agencies in July 2019, seeking community views about how government agencies should respond to data breaches. DCJ is now developing the proposed scheme in conjunction with the Department of Community Service and the IPC. This work and the introduction of the scheme will provide a significant contribution to privacy protection and cybersecurity management in New South Wales.

The CHAIR: I am happy to start with a follow-up to the last part of your statement in terms of your view about mandatory reporting. You think that there should be mandatory reporting rather than the voluntary system that is in place now. I know you have done some work with these departments, and you mentioned the Department of Communities and Justice in terms of thinking about this, but that was almost 18 months ago from what you have said. Where is that up to in terms of what work you are doing with the Government?

Ms GAVEL: Yes. The actual consultation paper that went out for comment was 18 months ago but the work has been done on scoping and putting together a model for such a scheme over the past year. At this stage it is really for the Government to announce further developments in the scheme but the IPC has been consulted as part of that and I am certainly looking forward to further developments in bringing that scheme forward.

Mr DAVID SHOEBRIDGE: Ms Gavel, I think the question was about what consultation you had and the meaningful nature of that consultation or contribution that your office made to that. We can reasonably expect some information about that.

Ms GAVEL: Yes, certainly. We have had significant consultation with the Department of Communities and Justice and with the Department of Customer Service in regard to the model for the scheme. I suppose the model includes things like the threshold for the scheme—what should the threshold be when agencies need to report? Of course, it will go to the legislation that is required for the scheme. We have looked at other models, or certainly DCJ has looked at other models for schemes around Australia, including in particular the Commonwealth Government scheme. They already have a mandatory data breach reporting scheme in place. It makes sense to look to that as a model, because it is in place, we can look at how it is working and the lessons that we can learn from that scheme. It would also be sensible to use that as a model because New South Wales shares information with the Commonwealth and so we would have similar schemes in place for data breach notification. Those are some of the issues that we have consulted on.

Mr DAVID SHOEBRIDGE: If we are just going to mirror the Commonwealth scheme, why on earth has it taken more than 18 months and it is still not finished? If we are just going to mirror what the Commonwealth does, and that is your basic thrust from what I can tell, why do we not have anything about mandatory reporting more than 18 months after the discussion paper? How is it so hard?

Ms GAVEL: The discussion paper went out 18 months ago and there was time for the community and agencies to put forward their submissions in relation to that scheme. The submissions were taken in by DCJ and they considered the findings of those submissions. Something that was very pleasing to me as Privacy Commissioner was that the submissions were overwhelmingly supportive of such a scheme. As I said, over the past year or so we have been consulting with DCJ on the form of the scheme. I hope that work is nearing completion but, as I have said, it is for the Government to announce further developments in the scheme.

The Hon. NATALIE WARD: I think you mentioned there are different types of schemes. There is that one, but there are other options. Is that correct?

Ms GAVEL: The Commonwealth one is the only one that has been legislated in Australia at the moment. Other States and Territories are looking to whether they introduce their own schemes as well. But there are, of course, also other schemes globally that we can draw on as well.

The CHAIR: Do you and your organisation have a view on which one?

The Hon. NATALIE WARD: Do they differ?

Ms GAVEL: We consider that the Commonwealth scheme works well in the Australian context. Not to say that we would necessarily mirror it and bring in the same scheme, but there are benefits in having a similar scheme because of the way that we do share information with the Commonwealth. It does not mean that we will completely mirror it, and the Commonwealth scheme covers private entities as well, which is not something that is covered under New South Wales.

The Hon. NATALIE WARD: How do the other schemes differ?

Ms GAVEL: How do they differ? We do not have a scheme here yet. Sorry, do you mean between the Commonwealth scheme and perhaps the—

The Hon. NATALIE WARD: Yes, other individual States. I just wanted you to elaborate on the others.

Ms GAVEL: No, the Commonwealth scheme is the only scheme that has been legislated in Australia to date.

The Hon. NATALIE WARD: Sorry, I thought your evidence was that there were different schemes for mandatory reporting.

Ms GAVEL: There are different schemes around the world, sorry. There is a scheme under the European Union [EU] General Data Protection Regulation, for example, but there are other schemes as well.

The Hon. NATALIE WARD: Okay, and how do they differ from the Commonwealth scheme?

Ms GAVEL: They are focused on the type of legislation that applies in that jurisdiction. The Commonwealth scheme is focused on its legislation in terms of entities—

The Hon. NATALIE WARD: But to a lay person like me, what does that mean?

Ms GAVEL: In terms of the entities it regulates. So the Commonwealth regulates Commonwealth Government entities. They also regulate healthcare providers, so there is actually a jurisdictional overlap with New South Wales.

The Hon. NATALIE WARD: And the European schemes? Do they do the same or different?

Ms GAVEL: The European data protection scheme, it has a very broad regulatory remit, as I understand it. It is a scheme that applies across the European Union, but different countries within the union will have their own version of it.

The CHAIR: But do you and your office have a view on what should happen in New South Wales in terms of a scheme?

Ms GAVEL: We do. Yes, we do.

Mr DAVID SHOEBRIDGE: What is it?

Ms GAVEL: We have views around what the threshold should be for reporting data breaches. I think I did mention in my overview that it is about where a data breach results in or is likely to result in a serious risk of harm to the individual—that that breach should be reported to the Privacy Commissioner and also to people who are affected by the breach. Obviously, there are some complexities around some of the reporting that need to be considered. There are issues that go to—I mean, obviously for me, I think the threshold and how we set that threshold is very important because agencies need to have clarity about when they need to report a breach.

Mr DAVID SHOEBRIDGE: Serious risk of harm seems like an extremely high threshold and very subjective, and I cannot see how that would give anyone comfort that—

Ms GAVEL: Well, those are my words—

Mr DAVID SHOEBRIDGE: Just let me finish, Ms Gavel.

Ms GAVEL: —that I have used in the opening statement.

Mr DAVID SHOEBRIDGE: I do not see how that would give anyone comfort of a policy.

The Hon. NATALIE WARD: I think you interrupted the witness, actually.

Ms GAVEL: I think your question goes to when I referred to the complexities of bringing in such a scheme, this is one of the issues that needs to be worked through. Where do you set the threshold? How do you incorporate it into legislation? What kind of wording do you use? And then, once it is legislated, what kind of guidance is the IPC going to put into place for agencies to use and refer to so that they know, so that they have clarity about when they need to notify? New Zealand has actually recently introduced its own scheme and legislated for it, and they, interestingly, have put some guidance on their website that includes a tool that agencies can use to put in information about the breach, and it will give advice on what level of notification is required.

Mr DAVID SHOEBRIDGE: But they do not have the serious risk of harm threshold. They just have a basic requirement to report data breaches in New Zealand. The serious risk of harm threshold would mean—how many of the 79-odd data breaches that have been notified to your office in the last financial year would have met the serious risk of harm threshold?

Ms GAVEL: I think what is important is that, for example, the Service NSW breach would have met the serious risk of harm threshold, and that is the type of breach that we are trying to capture.

Mr DAVID SHOEBRIDGE: My question was quite specific: How many of the more than 70 data breaches you have received in the last 12 months would have met the serious risk of harm threshold?

Ms GAVEL: I have got some statistics here on our data breaches, and what I can advise is that 9 per cent of those data breaches were attributed to a form of cyber incident and the majority of breaches were caused by human error.

The Hon. ADAM SEARLE: Yes, but that does not answer Mr Shoebridge's question.

Ms GAVEL: The majority of breaches caused by human error were low-risk breaches that involved emails being sent to incorrect people, usually one incorrect person. There were some where a mailing list, for example—they might have used the "to" send feature to send the mailing list instead of the "cc" so that everyone

saw the addresses in that list. But, of course, it is important to note that it depends on the context of the information because one email can actually involve a serious risk of harm, depending on the information contained in it.

Mr DAVID SHOEBRIDGE: Ms Gavel, I do not know if that answers my question, but perhaps I will put this other proposition to you: Why have you chosen that very high threshold to advocate for rather than the existing, well-understood threshold that applies in the EU where there must be immediate reporting unless it is unlikely to result in a risk of the rights and freedoms of individuals? Why have you not adopted that far more readily understood, longstanding European standard, which would obviously put a much higher onus than the one you are advocating for as Privacy Commissioner?

Ms GAVEL: Can I just mention that the scheme has not been finalised. We are talking about a hypothetical scheme at the moment that we have been working on. When the legislation comes forward for consultation, then everybody will be able to put their views forward on what they think of that scheme, what they think of the model, what they think of the legislation, what they think of the definition for when breaches need to be notified. And that is going to be the appropriate time to put that forward.

Mr DAVID SHOEBRIDGE: Ms Gavel, you are sitting down now with the State Government, as the Privacy Commissioner, working through what the response will be, and I am asking you why you are not advocating for the European standard, which is far, far preferable, I would have thought, for the protection of privacy? Why are you not advocating for that standard?

Ms GAVEL: I am advocating for a scheme for New South Wales that will protect privacy in New South Wales and protect people in New South Wales, and, in particular, I have in my mind the Service NSW breach. That is the kind of breach where we need to protect people, and the threshold that will be set in the scheme will do that work, and that is what is important.

The Hon. BEN FRANKLIN: Could I ask a question? This is just a very brief question on the numbers while we are talking about the reporting of breaches. I think you said that there was a 23 per cent rise in the last 12 months in reporting. My question is: Do you have any sense about why that is the case? Is it because there were actually more breaches, or was it because there was more reporting of breaches, or because of the fact that more people are taking up this technology and so therefore there is going to be a necessary rise?

Ms GAVEL: I think it is to do with—obviously there are a lot of media stories around cyber breaches at the moment, and I think agencies are coming forward to tell us about breaches when they have them. And I think that is a positive thing because we actually want to know where breaches are happening.

The Hon. BEN FRANKLIN: So you think there is more reporting, rather than that there are more breaches?

Ms GAVEL: That is right, yes, because it is a voluntary scheme. Agencies are not required to report.

The Hon. BEN FRANKLIN: Understood.

The CHAIR: On what basis do you say that, given that it is a voluntary scheme? Are people telling you, are the departments telling you what the breaches are?

Mr DAVID SHOEBRIDGE: Is it the vibe?

The Hon. NATALIE WARD: Can we have one question at a time and some courtesy to the witness please?

The CHAIR: We did have one question at a time, and I would like the answer to it.

The Hon. NATALIE WARD: Both of you are tag-teaming, and the commentary from one of our colleagues I do not think is acceptable to the witnesses.

The CHAIR: Let us let the witness answer the question please.

Ms GAVEL: It is a voluntary reporting scheme, and I encourage agencies to report breaches. I certainly do that. When I present to agencies I always have a piece encouraging them to report breaches. They are not required to report breaches, but I think it demonstrates a desire to show good privacy practice when agencies do it. So I see it as a very positive thing when agencies report under the voluntary scheme.

Mr DAVID SHOEBRIDGE: Ms Gavel, that was not the question from the Chair. The question from the Chair was: On what basis—what data, what information are you relying upon to give the answer you gave to the Government that the increased reporting was just because of increased reporting rather than increased breaches. What information, what evidence do you have to justify that opinion?

Ms GAVEL: The evidence that I have is that we do not have evidence for why more agencies might report breaches. What I am looking at is the environment that we are in, where cybersecurity is a much more intense media issue. It is being picked up and talked about. Agencies are much more aware of it. Some of that would be through the work that I do and the IPC does with agencies—but also, of course, the work that other agencies do. When I am looking at complaints, generally we look at what we can show from the data and what we think might be happening. It is not something that I can necessarily show from this data, but agencies are reporting more breaches. A lot of those breaches involve sending emails to the incorrect person. Unfortunately that is a very common type of data breach.

The CHAIR: While the reporting remains voluntary instead of mandatory, given your answer and your evidence to the Committee that you think maybe it is because there is a bit more attention on this as an issue, could I put it to you that it is also possible that public attention on this issue while the scheme is voluntary would encourage no reporting? It would encourage departments to hide these breaches.

The Hon. NATALIE WARD: That is not what she said. She said they are reporting.

The CHAIR: It is a question and I would like the answer to it.

Ms GAVEL: I can only comment on the breaches that are reported to me and not the ones that are not. For example, Service NSW reported to me on the breach.

The Hon. NATALIE WARD: Chair, may I ask a question about that?

The Hon. ADAM SEARLE: Madam Chair, I have got three questions.

The CHAIR: Mr Searle and then Ms Ward.

The Hon. NATALIE WARD: I have one question on that reporting number, if I may.

The Hon. ADAM SEARLE: Alright.

The Hon. NATALIE WARD: Thank you, Chair, and thank you, Mr Searle. In your submission you have talked about, on page three, the data breach released by the Office of the Australian Information Commissioner. You have said in there that:

> … sixty five percent of data breach notifications received … between January and June 2020 were the result of malicious and criminal attacks. Most of these were attributable to incidents resulting from common cyber threats such as phishing, compromised or stolen credentials, ransomware or other forms of hacking. Thirty four percent of breaches were attributable to human error, with system faults accounting for the remaining five percent …

So, it seems that the majority are criminal, malicious attacks and that the vast minority—as you say, you have referred to some human error, but also 5 per cent of system faults.

Ms GAVEL: I will just double-check.

The Hon. NATALIE WARD: It is your submission—second paragraph, page three.

Ms GAVEL: Yes, because that is—sorry, which page was that?

The Hon. NATALIE WARD: Page three.

The Hon. BEN FRANKLIN: Second paragraph.

Ms GAVEL: No. That is the data from the OAIC, which is the Commonwealth Government information commissioner. Their data has consistently shown that cybersecurity breaches are more common for them, except for the most recent report they released, where it has actually changed and it has been human error. But for New South Wales and for our voluntary data breach reporting system, the majority are human error breaches.

The Hon. NATALIE WARD: When you say it has changed and it is human error, do you mean there is more human error than malicious criminal attacks?

Ms GAVEL: The Office of the Australian Information Commissioner [OAIC] report regularly on their mandatory data breach scheme. In their most recent report they had a higher number of human error breaches, or breaches attributable to human error, than cyber breaches.

The Hon. NATALIE WARD: In sheer number?

Ms GAVEL: That is right. But, up until that point, since the scheme commenced in 2018 they have reported more cyber breaches.

The Hon. ADAM SEARLE: Madam Chair, I have got three areas I would like to quickly explore. We have been talking about the mandatory notification scheme or a potential scheme. But, at the moment, when

people have suffered breaches of their privacy or personal data, the only remedy that seems to exist is a financial compensatory mechanism which is very hard to access. I think you have to establish actual financial loss to get that. How many people who, for example, suffered the Service NSW cyber attack actually qualified for any kind of compensation? Should we be looking at a broader scheme of remedies in privacy law here in New South Wales that might actually provide meaningful support for people whose privacy has been compromised?

Ms GAVEL: Yes, that is a good question. Look, Service NSW are coming here this afternoon and they will be able to give you information on where they have provided compensation to people. People are also able to access compensation through the tribunal, as you know, but I agree. I think there are some important lessons that are going to come out of this breach. Two that really resonate with me—one is how we look after people when this kind of breach occurs, because it is very stressful and difficult for people when they have a piece of identity information that is compromised. Unfortunately, even though Service NSW did a lot of work to put their hypercare team into place and to have ID care available for people, at the end of the day people actually have to run around and get their new driver licence, get their new birth certificate, tell the police—all those things they have to do, along with everything else and the stress of the breach.

The Hon. ADAM SEARLE: You would accept, would you not—at least at a general level—that there should be other legal remedies for breaches of people's personal privacy and data?

Ms GAVEL: I think it is something that we need to look at because cyber breaches are going to be with us going forward. We are all putting more of our personal lives online. We expect government to be available to us online and cyber breaches are part of that landscape. So, I think these are issues that we really need to consider. Of course, we know at the Commonwealth level there is a review going on at the moment of the Commonwealth Privacy Act and one of the recommendations they are looking at is whether there should be a privacy tort for people. That review is going on this year, so it will be interesting to see the outcome of that.

The Hon. ADAM SEARLE: Yes. I think a New South Wales parliamentary inquiry might have recommended that too.

Ms GAVEL: Yes, that is right.

The Hon. ADAM SEARLE: Just as a follow-up, the New South Wales Government does a lot of outsourcing; all governments have done that. Particularly Service NSW—a lot of private third parties actually hold a lot of data belonging to government and to citizens. Those private bodies are not covered by New South Wales privacy laws as I see it. Shouldn't State-owned corporations and other corporations that are handling citizen data also be covered by a New South Wales privacy regime if they are handling information given to them by government agencies?

Ms GAVEL: Yes. Again, that is a very good question. I support measures that are going to increase privacy protection in New South Wales for citizens. Third parties providing services to government is obviously an area that needs to be looked at, but there are a number of complexities as well. For example, many of those third-party providers are covered by the Commonwealth and they also report under the Commonwealth mandatory data breach scheme. So, in putting measures in place, we need to think carefully about how we manage that so that we are not making it too complex for organisations—and also too resource intensive—so that we are able to do it in a way that is workable.

The Hon. ADAM SEARLE: We also do not want make it too complex for citizens to be able to enforce their rights to privacy and data protection. Would you accept that?

Ms GAVEL: Yes, that is right.

The Hon. ADAM SEARLE: My last question really flows from an interesting book I have been reading about privacy. A couple of the case studies I have been looking at are about the ability to take anonymised data sets and to be able to reconstruct the identities of the people whose anonymised data that was. There are two or three case studies in there where public data sets are used to, with 95 per cent accuracy, actually identify the individual citizens whose data has been anonymised. I noticed in your submission, in relation to community expectations and privacy by design notions, that there is an acceptance that de-identified information should be used to inform planning and service delivery by government. But there does seem to be this risk that even anonymised data—that veil of privacy can be pierced by people who know what they are doing. Are our privacy laws actually fit for purpose in terms of providing the necessary protection to citizens from things like this? How do we need to improve those protections?

Ms GAVEL: So, as you know, privacy law is principles-based. It does cover new technologies; that is one of the benefits of being principles-based. As you know, in a joint Committee last year I did provide some information to the Committee on enhancements that I would see. I think in this space the introduction of a

mandatory data breach scheme is an important one. In terms of the issue around anonymised data—yes, I certainly understand the risks with that. I think there is the famous Bradley Cooper taxi ride, for example, but there are many others. We work closely with agencies in relation to digital projects, to make sure that they do take a privacy by design approach, that they conduct a privacy impact assessment—if necessary, a security assessment as well—and that, if they are using anonymised data, they have measures in place to prevent that data being re-identified. And one of the reasons it can be re-identified is when you bring new datasets in. So that is a known risk that needs to be managed.

Mr DAVID SHOEBRIDGE: Ms Gavel, I think where your submission speaks about the fundamental need for privacy by design is important. Does Service NSW operate under that principle from your engagement with them—privacy by design?

Ms GAVEL: They do. I have certainly had a number of engagements with Service NSW and the COVID check-in app feature is one where the IPC consulted with the Department of Customer Service [DCS]. For example—I think you were asking some questions around that earlier—the Service app does not collect location information and nor does the COVID check-in feature. Those are important privacy protections that are built into the app. We have worked with Service on a number of projects, including the digital driver licence, and they have been very aware of the need for privacy by design in those particular projects. I mean, now it is really good because when DCS and Service come to us, they have already done their privacy impact assessment [PIA], which is very good to see. And—sorry, I have lost my train of thought.

Mr DAVID SHOEBRIDGE: I might take you back then to the COVID Safe check-in app. Your evidence is that it does not contain location data. Is that your evidence?

Ms GAVEL: That is right, yes.

Mr DAVID SHOEBRIDGE: But it contains the venue you go to. Surely the venue you go to is pretty critical location data, is it not?

Ms GAVEL: It does, but it is not following you around in the way that a lot of apps do, for example. But that information is held securely. It is only passed to NSW Health should it be needed for contact tracing purposes and it is deleted after 28 days.

Mr DAVID SHOEBRIDGE: Does the Service NSW privacy management plan detail how those kinds of health exemptions will be used? Because, as I read the Auditor-General's report, it does not.

Ms GAVEL: That is right.

Mr DAVID SHOEBRIDGE: And that obviously would be critical on this COVID safety app.

Ms GAVEL: The Auditor-General did make some comments on the Service NSW privacy management plan and the fact that a number of recent developments had not been included. They are currently updating that plan and I expect to see it very shortly.

Mr DAVID SHOEBRIDGE: Why did it take the Auditor-General to identify those defects in Service NSW's privacy management plan and not your office, given you have had ongoing contact with Service NSW throughout? Why did it take the Auditor-General to find it and why not you?

Ms GAVEL: The IPC is a small agency with a very broad remit and we have quite a number of ways that we engage with agencies and assist them. We have a limited amount of resourcing. We have a particular resourcing envelope and we need to carry out our functions within that envelope. So we really target our resources and our activities on areas where we can have real impact for agencies. We have not been following up with agencies on privacy management plans to ensure that they have updated them. That is something that we will, in light of the Auditor-General's report, be looking at—whether we need to include that into our forward work program. But privacy management plans are a requirement under legislation and agencies need to comply with that requirement.

Mr DAVID SHOEBRIDGE: The Auditor-General's report also indicates that there is a lack of clarity about roles and access to data in Service NSW. Did you run the ruler over who has access to the COVID-19 location or venue data? Did you double-check that there are controls to prevent individuals from Service NSW accessing that data within the 28 days?

Ms GAVEL: That is part of the information that we check—who has access when we engage with an agency. Those data flows and issues like who has access are covered off in a privacy impact assessment.

Mr DAVID SHOEBRIDGE: So who has access to the COVID-19 data?

Ms GAVEL: Service NSW will be able to give you information about that, but certainly part of our consultation with Service and DCS on the app is around those kinds of issues and how we build privacy protection into the app.

Mr DAVID SHOEBRIDGE: What limits did you insist upon? What reporting and checking did you insist upon for the COVID-19 app? Or do you not know?

Ms GAVEL: I have not got the information with me about the consultation that we did, but what I can tell you is that we consulted with Service NSW. We went through their PIA. We went through the security information. As the regulator, part of our role is to consult to assist them to comply with privacy law. It is not to run the ruler over it per se. It is not an audit function in the way that the Auditor-General carries out.

Mr DAVID SHOEBRIDGE: But in the process you did not even pick up that the privacy management plan that they had in place did not address the health exemptions and surely the health exemptions are core for the provision of information from Service NSW under that app to NSW Health. You did not even pick up that basic thing. I cannot understand how that did not happen, Ms Gavel.

Ms GAVEL: As I say, we consult regularly with agencies and regularly with DCS and Service on the digital projects that they are undertaking. The COVID app is one of those. That is separate to their privacy management plan. The other thing I think that is important to note from the Auditor-General report is the Auditor-General was positive about the use of privacy impact assessments by Service NSW. That is something that I would agree with and something that the IPC has worked closely with Service NSW to ensure that those things occur in the digital projects that they are undertaking.

Mr DAVID SHOEBRIDGE: How many staff do you have, Ms Gavel?

Ms GAVEL: We have around 30 staff with two commissioners. Our staff work across two streams: information access and privacy. We have had over the last five years a significant increase in reviews, advices and complaints to deal with. We are also doing a lot of work with agencies around the projects under the Digital Restart Fund and supporting the Government in the digital work that it is doing.

Mr DAVID SHOEBRIDGE: I have one final question to either of you. The Information and Privacy Commissioner—the question might be to you, Ms Tydd—dealt with a complaint in respect of allegations of serious breaches of the State's freedom of information laws regarding the shredding and destruction of documents by the Premier's office. You determined to pass that report onto the Independent Commission Against Corruption. Can you please advise on what basis you made that decision?

The Hon. NATALIE WARD: I am not sure that is within the terms of reference, but I am going to be overruled.

Ms TYDD: The nexus to the terms of reference is not readily apparent to me, but I am able to answer that the Information Commissioner may refer matters—"furnished reports" is the expression in the legislation—to a range of agencies. "Any other agency" is one of the provisions that is dealt with, so it has been publicly reported that I have furnished information both to ICAC and to the State's State Archives and Records Authority. They are agencies that can be furnished with information under the legislation by the Information Commissioner.

Mr DAVID SHOEBRIDGE: But my question is why did you exercise that discretion to do so. I do not think you have addressed that, Ms Tydd.

Ms TYDD: Both provisions operate separately and independently and thresholds have to be met. One of the thresholds is that the information is able to be received by the receiving agency. Another threshold is that it does not contain information for which there might be a conclusive presumption of an overriding public interest against disclosure [COPIAD] asserted. I know you are aware of what a COPIAD is, Mr Shoebridge—a refusal to provide information. The test is whether those thresholds have been met, first of all, and whether information may be relevant to the exercise. Whilst this is not enshrined in legislation, one of the factors I would consider is whether it is relevant to the exercise of functions by those agencies.

Mr DAVID SHOEBRIDGE: You determined, I assume, that the information that you had gathered in your report was relevant to ICAC's anti-corruption investigations. Is that right?

Ms TYDD: The Chief Commissioner is certainly on the public record and his statements around his interest in how grants operate in New South Wales is on the public record. As you are aware, the investigation did look at guidelines dealing with the grant of funds.

The Hon. ADAM SEARLE: Just following up on that referral, I think both you and the records authority reached a different view about whether or not the records legislation had been breached by the Premier's

office. Have you compared notes with the records agency as to how you each arrived at a different view about the matter?

Ms TYDD: I have not compared notes. We both operate under different statutes and a section 120 deals very differently, as I understand it, from the State records offence provision. So the offence provision—

The Hon. ADAM SEARLE: So you were not making a judgement about that.

Ms TYDD: Not at all.

Mr DAVID SHOEBRIDGE: You were looking for whether or not there had been a breach of the Government Information (Public Access) Act, which was quite a different issue.

Ms TYDD: Indeed.

The CHAIR: Thank you very much for your time today. We appreciate it.

(The witnesses withdrew.)

(Luncheon adjournment)

TONY CHAPMAN, NSW Chief Cyber Security Officer and Executive Director, Cyber Security, Department of Customer Service, sworn and examined

GREG WELLS, NSW Government Chief Information and Digital Officer, Department of Customer Service, sworn and examined

DAMON REES, Chief Executive Officer, Service NSW, Department of Customer Service, affirmed and examined

The CHAIR: Welcome back to this afternoon's session of the second day of our inquiry into cybersecurity in New South Wales. Welcome to our witnesses. You are entitled to make a brief opening statement if you wish to do so.

Mr CHAPMAN: Thank you, Chair, I will, prior to deferring to Mr Rees. Thank you for the opportunity to appear at this important inquiry. The New South Wales Government is on a mission to be a world leader in customer service, and digital initiatives and the innovative use of data have a crucial role to play. Cybersecurity is critical in ensuring the New South Wales Government provides secure, trusted and resilient services. As the New South Wales Government continues its digital transformation, maintaining and enhancing our cybersecurity capabilities is paramount.

Cyber Security NSW provides whole-of-government leadership, coordination, advice and intelligence across New South Wales government, including to small agencies and our local councils, to reduce cyber risks. We coordinate whole-of-government cybersecurity incident response, including liaison with the Australian Cyber Security Centre and other jurisdictions, by what is known as the National Cyber Security Committee. We set whole-of-government cybersecurity policies and standards and deliver training, awareness and resilience programs across New South Wales government.

Ultimately, cybersecurity is about managing risk. Each department, secretary or head of agency is responsible for the governance, control, direction and management of their organisation. They are therefore responsible for all organisational risks including cybersecurity risks. No organisation, private or public, can stop cybersecurity incidents from happening, but just like workplace health and safety incidents they can be reduced. No digital system or service can be guaranteed to be secure. We can take steps to ensure they are continuously strengthened, however, new vulnerabilities and ways to exploit systems are regularly discovered. Threat actors will always look for ways to do us harm and are consistently changing their tactics, techniques and procedures in order to achieve their desired end state. It is not a matter of if incidents will occur but when and how much their impact, harm and spread can be reduced through prevention, preparedness, early detection, response and recovery. Cyber Security NSW will continue to work across government to provide early warnings of such vulnerabilities.

In February 2019 we implemented the NSW Cyber Security Policy and an Australian-leading set of cybersecurity standards. These standards take a risk-based approach to cybersecurity. For the first time in New South Wales, government agencies are now required to annually assess their cybersecurity maturity. I am proud to say that the New South Wales Government has the most comprehensive cybersecurity maturity reporting requirements of any jurisdiction in Australia—State or Federal—and that our risk-based approach is also adopted by the Federal Government. Further, in October 2020, cybersecurity training and daily cybersecurity hygiene practices were mandated for all New South Wales government staff by the release of a Department of Customer Service circular.

Cybersecurity, however, is a journey. It is not set and forget; it cannot be completed. The threat from advanced malicious cyber activity is increasing in frequency, scale, sophistication and severity. That is why, despite our considerable achievements to date, we have ensured a commitment to continuous improvement to meet this increasing threat. Our mandatory reporting requirements allow us to measure this improvement. The announcement of $240 million in funding over three years will enable uplift of cybersecurity across New South Wales government. Cybersecurity risks cannot be mitigated through implementation of vulnerability detection and IT controls alone; it requires a combination of people, process and technical controls to succeed, which is reflected in our approach to the cybersecurity policy.

Finally, I am proud to report that Cyber Security NSW is surpassing the proportion of women in the global cybersecurity workforce. Fifty per cent of cybersecurity staff are female, with two-thirds of our senior leadership team being female. Thank you.

Mr REES: Good afternoon, Chair and Committee members, thanks for the opportunity to appear at this very important inquiry. Service NSW is an executive agency within the Department of Customer Service. Our role is to provide a one-stop shop for access to government services. Our mission is to make that as easy an

experience and as good an experience as we possibly can, whether that is through our face-to-face channels, our digital channels or serving customers by phone. We serve customers through 110 different points of presence across the State in addition to our contact centres and our digital channels. In 2020 we served approximately 87 million customer interactions across a range of services. We are very, very proud that the customer satisfaction that our citizens have with Service NSW remains very, very high, but of course last year we experienced a serious cyber incident. That is something that is deeply, deeply disappointing for ourselves and we take that very, very seriously and the impact that that has on our customers, our partners and on the services that people trust us to deliver every day.

Our response to that has very much been led by our values as an organisation and our focus on making sure we do everything that we possibly can to support any customers that may have been impacted through that, whilst ensuring that we do not create any additional risk to customers and the public through our efforts to respond. That also serves as a catalyst for us to continue our commitment to strengthen our cybersecurity defences right across the organisation. That is a job that we do not believe is ever done. Cybersecurity is a critical risk for all of our organisations and we are no exception. That risk landscape is constantly changing and we need to be continuous in our efforts to make sure that we are protecting the information that we hold and that we are providing safe, secure and reliable services to our customers. Thank you again for the opportunity to be here and I welcome any questions.

The CHAIR: Thank you. We will open it up to questions. I might start with the breach that you have referred to that occurred last year that we are aware of. Mr Rees, on what date were you first notified of the breach in your department?

Mr REES: I will find the exact date. There was a lead time between when this incident occurred and when we realised we may have been impacted by a cybersecurity incident. That lead time was approximately three weeks and so I first became aware of this in the middle of April.

The CHAIR: When did you notify the Minister?

Mr REES: We formally briefed the Minister on 13 May. On becoming aware that we may potentially have been a victim of a cyber incident in the middle of April it took us approximately three weeks to verify that that cyber breach had occurred and to understand the broad dimensions of the impact that that may represent.

The CHAIR: It has been reported that the police were notified. Can you tell us what timetable occurred and also if they are investigating or if they are still investigating where that is up to?

Mr REES: The formal notification for police was made on 12 May. There is an ongoing investigation being run by police into this incident.

The Hon. BEN FRANKLIN: How did you actually notify the affected customers? What was the process you went through with regard to that?

Mr REES: One of the very difficult things about dealing with this situation has been how to notify. It has been challenged by a couple of things: the first is incomplete information around the customers that are impacted, including contact information for those customers. The second thing we have been very mindful of is how to minimise the risk of scams to customers in our efforts to notify them. One of the things we observed is that when we did advise the public that we had been impacted by a breach, almost immediately, members of the public were receiving attempted scam calls off the back of that public awareness to attempt to defraud them. So from the start the goal has been to notify customers as quickly as we can but, more importantly, to notify them safely and accurately. Broadly speaking, we have taken two approaches. For the vast majority of people we have notified customers via registered person-to-person mail to make sure that we had as much confidence as possible that the right notifications were being received by the people they were intended for.

Those notification letters have two key dimensions to them. One is that they are personalised. So the letter I receive is unique to my circumstances and not the same as the letter that Mr Chapman, for example, would receive. Similarly, the guidance for what I can do to understand and manage my risk is part of those letters. There was a very small set of customers we were able to identify relatively quickly and commence notification very quickly where we perceived that, due to their circumstances, there may have been greater risk of personal harm. Those notifications commenced in May. The other key decision that we took was to notify people, wherever possible, once, with a complete picture of the impact for them. The challenge or the downside to that is that it took us longer to be able to understand that complete picture and do that notification once and holistically.

The alternative would have been to progressively notify people as the data analysis progressed, but the risk of that was that we would be going back and notifying people in drips and drabs multiple times. The advice that we received from our external experts was to say no, the best outcome for people who are impacted is to

notify them once, give them a complete understanding of what their picture is, be as clear as possible about what it means for them and provide the support mechanisms and empower the customer to access those if they choose to based on their circumstances.

The Hon. NATALIE WARD: Mr Rees—or whoever is appropriate to answer—in 2019 the Government's cybersecurity policy was implemented. Can you talk us through the requirements of that and how that aligns with the whole-of-government view? It has been implemented but how does it align with the whole-of-government view of cybersecurity?

Mr WELLS: I might start and hand to Mr Chapman to go through some more details. I think the first thing to say about the policy is that we took the best of what was available from technical controls, governance controls and other risk controls and tried to put that all together into one framework that, as you have said, we introduced in February 2019 and have now mandated annual attestation against from August 2018. So we have had a first and second round of reporting, and a third one will be coming up this year. The important thing about that policy is that it is not just about technical controls. Sometimes people think of cybersecurity as just about technical controls. Within the policy are some controls called the Essential Eight, which go to some really basic sets of hygiene that should be covered in terms of cybersecurity risk management.

But it also really importantly goes to structural components—who is responsible, who is in the organisation, what is the plan to respond and have you exercised and tested that plan. Those 25 requirements go broadly across all the dimensions that need to be taken into account when we think about cybersecurity. Mr Chapman might want to comment on some of the specifics around the policy itself, but that has enabled us, as Mr Chapman said in his opening statement, to understand the baseline of maturity across the Government, which other jurisdictions are now also copying and bringing forward. That has been a really important baseline for us to understand where we need to uplift capability. That resulted in the investment that Mr Chapman also talked about that is specific to agencies about the need to uplift capabilities in certain areas, whether that be technical, governance, et cetera. Those plans formed that announcement of investment to uplift capability across the sector. We need that to be across all agencies because everyone, as you know, is quite connected in the way we operate.

The CHAIR: In terms of the answer you just gave about how the policy—sorry, I have forgotten the wording that you used so I will probably paraphrase.

Mr WELLS: That is okay.

The CHAIR: Essentially, it was about different departments being able to have different policies and you guys overseeing it. That is essentially what happens in practice. Do you think that is an ideal way for this to occur? The real question is, because departments share information between each other, so if one has a better practice than another—and Service NSW is an example where they have a lot of private information sharing between other departments—is that really the best practice?

Mr WELLS: I will quickly address that before we get into more detail. To be really clear, there is one cybersecurity policy for the New South Wales Government. It is set and mandated across; it is not different per agency. My comment was that it is a risk-based approach that every cluster will take in terms of that same policy and where they see the need for greatest uplift: where there are gaps and where they need to increase capability in those areas. So there are not different policies. It is the one policy with the same 25 requirements across all agencies. Clusters construct from their perspective what their biggest risks are and what they need to address.

Mr CHAPMAN: Just add to that, one benefit of the approach that we have taken with the policy is that it really embeds accountability from very senior levels of government. So it is a top-down approach but, at the same time, really highlighting that cybersecurity is everyone's responsibility and it is much broader than just an IT risk; it is a business risk. In accordance with the policy, you will note various requirements to, for example, establish governance forums. We have a very well-established governance forum or framework within the New South Wales Government, which ensures buy-in from those technical officers that Mr Wells mentioned, like chief information security officers, and chief information officers all the way up to deputy secretaries, who are responsible for business risk. A few other key points are: another benefit of the approach that we have taken is that agencies are required to report what is known as their crown jewels or high-risk assets to us. For the first time the central function Cyber Security NSW has a view of what those critical and high risks are across government.

The Hon. NATALIE WARD: Just to close on that and to be clear, I think there was an assertion earlier—not in this session but in an earlier session—that there were different ad hoc responses from departments. Is that your—not negatively, but just for Hansard, can you answer to clarify that?

Mr WELLS: That is correct. There is one policy and everyone reports against that policy and attests to their responses against that policy each year in August.

The CHAIR: But each department sets its own risks. I understand that you have a consistent policy in terms of they do or the baseline policy—or however you describe it—but they determine their own set of risks and then they oversee it themselves.

Mr WELLS: I would clarify that to say that they assess from their perspective what their crown jewels are, as Mr Chapman talks about—their most important frontline systems and the data they hold about their customers. From their perspective they are accountable to run those services, provide them and hold that information. On that basis they assess their greatest risk. We have taken a risk-based approach to this. It is a very complex and broad problem. That is the approach they take and then, consistently, against those 25 requirements, we are trying to uplift everyone to a consistent standard. So some agencies—to a comment before—will have strengths in some areas and weaknesses in others. Then part of our role is to make sure that we are sharing that knowledge across the sector so that people can build capability and resilience.

The CHAIR: Some departments have more personal information about individual citizens across New South Wales than others. If each department can, within your policy—which I accept is consistent—regardless of their level of private data that is kept, determine what they see as their own risk and then determine what to do with it, who is ultimately responsible and how are protections in place for individual citizens using the Service NSW data? Other than Health I would have thought that is one of the riskiest for private citizens' information.

Mr WELLS: Yes.

The CHAIR: Are there any rules across government for how that is determined?

Mr WELLS: I would say, as Mr Chapman said in his opening statement, clusters are accountable for their own systems and the data they hold. The ultimate accountability for cybersecurity rests with clusters. Our role is to lift that capability and protection consistently across government.

The CHAIR: How much has Service NSW spent on managing the data breach from last year so far?

Mr REES: Certainly the approach that we have taken to voluntarily notify customers and the method of notification, it is not the cheap way to respond to this. We have not got a final set of figures for the total cost impact and we are working through that with our insurer at the moment. But certainly we have chosen the path that makes sure we get the right customer outcome, not the path that is going to minimise the effort and expense to achieve that.

Mr DAVID SHOEBRIDGE: When you say "our insurer", do you mean—

Mr REES: Icare.

Mr DAVID SHOEBRIDGE: That will ultimately come from State Government funds because you are self-insured?

Mr REES: You would need to direct that question to icare, I think.

Mr DAVID SHOEBRIDGE: You have not got a policy with a private insurance company. This is going to come from the Treasury Managed Fund, isn't it?

Mr REES: I think questions around how icare cover their insurance would need to be directed to icare.

Mr DAVID SHOEBRIDGE: This is your insurance policy. You can surely answer where your insurance policy is covered. It is from the Treasury Managed Fund. It is public money.

Mr REES: Icare's use of the insurance and reinsurance market would need to be directed to icare.

The Hon. NATALIE WARD: Chair, the witness has twice indicated that he is not able to answer the question. I think that we should move on because it is not within the terms of reference.

The CHAIR: No, I think the questions were fine. They were follow-up questions. The witness can determine how he wants to answer it and he did.

The Hon. NATALIE WARD: He has also indicated it is a question for Treasury, and he has also indicated twice that that is not within his purview.

The CHAIR: I have ruled on that, so we can move on. Do you have any other questions in that regard?

Mr DAVID SHOEBRIDGE: You make it sound as though there is going to be a pool of insurance to cover the loss and damage. But, Mr Rees, that pool of insurance money just comes from another pot of public money, doesn't it? What is the size of the claim?

Mr REES: I can either take the question on notice or we can direct it to icare. I am not qualified to speak to how icare will fund the insurance claim.

Mr DAVID SHOEBRIDGE: Perhaps you might take it on notice then, Mr Rees.

Mr REES: Sure.

The CHAIR: Can we just go back to the original reporting timetable that we were talking about earlier, Mr Rees. You became aware of the breach in mid-April and notified the Minister in mid-May. What was the reason for the delay?

Mr REES: There were two periods prior to us notifying the Minister. The first was a period of time before we became aware that we had a cyber incident. So that is three weeks from when the cyber incident originally occurred. The subsequent three weeks was made up of a number of things. The first is we needed to verify whether that incident had in fact occurred. The second was working out what the impact or the magnitude of that impact was once that cyber incident had occurred. So that accounted for the period of time between which we became aware that we may have had a cyber incident and the point at which we formally briefed the Minister on the incident and the materiality of the impact.

The CHAIR: That was determined by what you thought, after looking at it for those three weeks, was the material effect or the magnitude, I think as you put it. What is the criteria for determining that? If there is a breach in the department, how do you determine whether it is big enough or significant enough or not to notify the Minister?

Mr REES: It is a great question. I think ultimately it comes to judgement. There aren't a predefined set of hard and fast metrics that would determine that. So it comes to the situation and the risk that is represented by that situation. In this case, the types of things that led us to that conclusion were the number of customers that we believed may have been impacted and the nature of the types of information that may have been impacted as part of that. In our view, it was clearly material once we got that guidance from the data analysis.

The CHAIR: In terms of a follow-up from something that we touched on earlier, you mentioned that you notified some people in I think it was May and then others—I don't think we clarified when we started notifying others. Can you just tell us who the people were that were notified in May? I do not literally mean name by name, but what was the criteria for the people that you assessed as needing to be told urgently—again probably paraphrasing but I think it was the way you described it—compared to the people who were told later?

Mr REES: The criteria was where we were able to identify what we thought could be a heightened risk of harm for those individuals. We developed a harm assessment framework with external guidance to say, based on the types of information that we thought were potentially compromised, what was the relative risk of harm. There were a number of items that we were able to quite specifically search for without completing all of our data analysis in that highest category of harm. So we searched for the individuals that we could find that were impacted in that way, and we made direct contact with those customers where we were able to.

The Hon. BEN FRANKLIN: Can I just ask a quick follow-up on that specific issue? I just want to talk about the hypercare team in terms of liaising and talking to affected customers. Were they the ones who directly did it? How did that process work? Just as I have been reading through it, I have not been able to crystallise it in my mind what the difference is between the idea itself and this hypercare group.

Mr REES: The hypercare team is a team that was stood up within Service NSW. They received specialty training around privacy and how to support people that may have been impacted by a privacy breach. They were the dedicated team that we put in place to handle or to support customers that had been impacted by this cyber attack.

The Hon. BEN FRANKLIN: So they would call in?

Mr REES: That is right.

The Hon. BEN FRANKLIN: They would speak to those people directly? How many calls would that team have received?

Mr REES: In total, we have received just over 30,000 calls from customers. Of those, 17,500 were directly as a result of the incident that we experienced and were customers that needed that extra level of support from Service NSW. We did receive calls from customers who had not been impacted by our breach but were concerned, had seen the media and wanted to either understand in advance of receiving that letter whether they were impacted. In some cases we received calls from customers who had been impacted previously in other aspects of their life and actually were needing support that they had been unable to find. We, of course, supported all of those customers.

The CHAIR: I am just going to jump in quickly with a wrap-up question. Going back to the time that you were made aware of the breach and the three or four weeks between then and notifying the Minister, we have heard that there are no hard and fast rules about your requirement to do that. Essentially, that is a lot of pressure on you and your department to decide what you should be telling the Minister about what should happen. Do you think that it would be better if there were mandatory reporting requirements so that it was just automatic when this happens and it was not just on your shoulders about what to tell a Minister or not?

Mr REES: I must say, firstly, we did not experience pressure. That is part of our responsibility. But to the question around mandatory reporting, it is a complex question and there will be many different perspectives. My personal view is anything that will strengthen assurance in privacy outcomes is a good thing and it is something that Service NSW would benefit from along with other government agency organisations.

The Hon. ADAM SEARLE: Just to be clear, I think you used the words "formally notified the Minister". Was there any informal indication to the Minister or his office or any member of his staff earlier that there may have been a data breach? If so, what time period roughly would that have occurred in?

Mr REES: I think we had informal conversations with the Minister's office prior to that, but at that time I do not believe we understood the magnitude of that. The point at which we understood the magnitude of the incident was the point at which we formally briefed the Minister.

The Hon. ADAM SEARLE: When did those informal discussions take place, roughly?

Mr REES: I will need to take that on notice.

The Hon. ADAM SEARLE: Please do. In relation to the December audit report on the Service NSW data breaches in March 2020, it was a fairly tough report in terms of the state of preparedness of Service NSW. In particular, there were a number of things—for example, the double authentication that Service NSW ought to have or had agreed to implement by 30 June 2019 but had not and this contributed to the risk. Can you tell us why that particular measure had not been implemented by the set timetable, and are there other security measures that you also had not implemented when they were supposed to be? In terms of the most recent audit report with those time frames, what confidence can we have that you are going to meet those time frames in terms of closing those gaps?

Mr REES: It is a great question. The security measure you are referring to is multi-factor authentication. That was an internal goal that was set and we did not achieve that goal at the time. There were a range of things that required the replanning of that. In part, it was a change in technology and direction on a number of key elements of technology. Then also the demands on the organisation to support customers through the bushfires earlier this year also impacted the timing in which we were able to deliver that enhancement. What I would say is that that control is only one of a range of controls and that control on its own would not have prevented this incident from occurring.

The Hon. ADAM SEARLE: Sure. But again, what confidence can we have that you are going to meet—for example, I notice you were meant to do a range of things by March of this year and that is only two months away. How are you tracking on those things? Can we have confidence that these milestones will be met?

Mr REES: Yes, we have been very public in our commitment and we accept the findings of that audit report completely. We have a team mobilised to deliver against each of those commitments that we have made. We have received the required funding in order to make sure that we have got the capacity behind that to deliver those outcomes. There is a lot of work to be done. So, certainly, I view those targets as aggressive but I think they are absolutely appropriate and we are fully committed to achieving them.

The Hon. ADAM SEARLE: Is your agency investigating the data breach at the health department involving the Accellion file [audio malfunction].

Mr REES: The New South Wales Government's response to that is being coordinated through Tony Chapman, so I might defer to Tony.

Mr CHAPMAN: Yes, the New South Wales Government and Cyber Security NSW are aware of the security incident that has impacted a third party provider—Accellion, their secure file transfer called the file transfer appliance. Cyber Security NSW is coordinating a whole-of-government response with potentially impacted agencies. We are working with forensic specialists as well as Accellion to determine the extent of potential impact, and that is ongoing.

The Hon. ADAM SEARLE: Apart from the health department, what other State agencies may be at risk? Are you able to tell us?

Mr CHAPMAN: At this stage investigations are ongoing. It is a complex matter involving forensic work with external specialist providers to government.

The Hon. ADAM SEARLE: When might you have a better picture as to the risk profile and which agencies may well have had their data comprised? One week? Two weeks? One month?

Mr CHAPMAN: As I said, these are very complex matters. As Mr Rees pointed out with the Service NSW incident, we have to do assurance on that forensic work to ensure the accuracy of the information that is being provided. The approach that I take, with the support of my secretary and others, is to ensure that we are being as transparent as possible to the point of notifications. We have a MOU in place with the Information and Privacy Commission. For example, we are also working very closely on that matter with the Australian Cyber Security Centre and we have notified the New South Wales police.

The Hon. ADAM SEARLE: Getting back to the framework for best data protection—I think, Mr Wells, you were talking about this—there is the policy and everyone reports against the policy. Previous evidence that we heard this morning was essentially that the New South Wales regime very much relies upon self-assessment by agencies and then self-reporting. It does not, for example, unlike the Commonwealth scheme, really require a minimum level of maturity in terms of sophistication. It seems to be a lesser standard that is in place in New South Wales Government. Can you just talk us through why that is and are there plans now to move to the minimum level of sophistication or maturity in cyber preparedness across the board?

Mr WELLS: In terms of those 25 requirements that I talked about, we have actually mandated a minimum level of maturity. Without going into the individual controls, we have said three out of five at this level is where we are targeting and two out of three for this level in technical control is where we are targeting. So we have actually implemented a minimum standard that we want clusters to reach. I would say that that is stronger than a lot of the Commonwealth controls at the moment.

Mr CHAPMAN: If I may add to your point around self-attestation, Cyber Security NSW does have experts within the team that, I guess, sense check and ensure a rigorous approach to that reporting and upon receiving the additional funding will be standing up at a governance, risk and compliance function within Cyber Security NSW to ensure the accuracy of that reporting to us.

The Hon. ADAM SEARLE: How many of the citizens whose data was compromised in March 2020 have sought compensatory payments and how many have received them? Separate to that, what other measures has your agency put in place to otherwise address the breaches or the compromising of that citizen data? If you do not have the information to hand I am happy for you to take it on notice.

Mr REES: I will take the question on notice to come back with the specifics. The number of people that have requested compensation or reimbursement is low—it is in the hundreds—but I will come back to you with the exact answer.

The Hon. ADAM SEARLE: Are there persons whose accounts have been compromised who have not been notified by Service NSW?

Mr REES: We have notified everyone that we have the mechanism to notify safely. Where we do not have the contact details or reliable or up-to-date contact details for a customer we do not have an ability to notify them safely.

The Hon. ADAM SEARLE: That is simply a limitation on your capacity?

Mr REES: It is a limitation of the information that is available about the people that have been impacted by the breach. We have taken all measures we can to understand that.

The Hon. ADAM SEARLE: Can you just pause there and help me understand. Is it that they do not have an address? There is not a telephone number? You call the number and no-one answers? I am just at a loss given the information that I understand you to hold, including some of my own, how is it that you cannot contact some people?

Mr REES: The information that was impacted is highly unstructured. Working out that actually this Damon Rees is the same as this Damon Rees is a very difficult and risky part of that process. We need to be very careful of our assumptions there.

The Hon. ADAM SEARLE: To be clear, is it the case that as a result of this data breach you are simply not able to identify which individual citizens are affected? There is possibly a cohort of people who have provided their information to you whom you have not notified because you cannot say for certain that it is this person rather than that person whose data was compromised.

Mr REES: We have been through an exhaustive process to analyse the impact of data and there is a good level of confidence that the impacted individuals have been identified through that analysis. That has been a combination of automated data analysis, significant manual verification of documents and then a QA process run after that. I think we have taken all the measures we can to form a confident view of who is impacted. Not all of those individuals we have been able to identify have contact information available. The method of notification in order to not generate risk for the public is that registered person-to-person mail which relies on us to have a current physical mailing address for the individual. We did seek and were granted a section 41 from the Privacy Commissioner which enabled us to work with Transport for NSW to obtain the most up-to-date address possible for those impacted individuals.

The Hon. ADAM SEARLE: It is possible there is a group of persons who have been impacted but you are not able to safely contact them?

Mr REES: That is correct.

The Hon. ADAM SEARLE: Do you have any understanding of how many might be in that category?

Mr REES: We are still ensuring that all our customer notifications have been successfully received by customers. We get them returned to us by Australia Post where that has not been the case. Indications are, at the moment, that 70 to 80 per cent of customers that we have attempted to notify have successfully received them.

The Hon. ADAM SEARLE: Is that 30,000 or 40,000 people who might not know?

Mr REES: It would be less than that. We have 104,000 individuals that were impacted and at this point it indicates that we have been able to successfully reach 70 to 80 per cent of them.

The Hon. NATALIE WARD: I understand you have engaged with independent cyber support community services—I hope I have got that term right. Is that correct?

Mr REES: Yes.

The Hon. NATALIE WARD: Are you able to share with us who they are?

Mr REES: I can. Cybersecurity is complex, we leverage a range of external organisations—

The Hon. NATALIE WARD: You are talking to a layperson here, completely.

Mr REES: —through a range of different methods. Specifically for this particular cybersecurity incident we took advice and expertise from a range of organisations. IDCARE is a national not-for-profit that specialises in understanding identity-related impacts to customers and how best to support them. We have worked very closely with IDCARE through this. An organisation like IIS provided expert privacy advice to us and as part of that we were able to access the support of a former Commonwealth privacy commissioner, which was invaluable to helping guide our response. There have been a range of organisations involved in the technical analysis of this.

An organisation called CrowdStrike are a specialist cybersecurity organisation that were involved in understanding and verifying the cybersecurity incident. We sought support from Microsoft and their technical expertise, again, to understand the incident and provide additional assurance there. We used several external organisations to help us analyse the data that we believed was impacted, and understand what the impact to individuals had been. So a range of specialist organisations that I think were key to being able to respond. More broadly, one of the other mechanisms that Service NSW has leveraged is what is called a bug bounty program, which is really a structured method used by organisations like Google and Microsoft, and many others, to leverage public expertise and to leverage cybersecurity more broadly to identify any potential risks in a safe and controlled way.

The Hon. NATALIE WARD: So not only involved in the response but to identify other risks as well?

Mr REES: That is right.

The Hon. NATALIE WARD: Thank you, that is helpful. Is there anything else that you can add in that space? They were obviously assisted and—is that ongoing?

Mr REES: I think the other point to add there would be that this is complex, and so there has been a number of areas where we have sought multiple perspectives and assurance on the same thing and not relied on the findings of either ourselves in isolation or a single organisation. That additional level of assurance I think has been important through this response.

The Hon. NATALIE WARD: And it is an always ongoing, evolving—as I understand it—challenge?

Mr REES: That is right. The risks that unfortunately were realised in our business are not risks that are being introduced more recently through the introduction of digital services. They happened to, in that case, have been risks that relate to some of the older parts of our business. And I think it reinforces the need not to just focus on the security of the new services that are being introduced, but to ensure that constant vigilance and assurance across all of your services and all of your information on a constant and ongoing basis.

Mr DAVID SHOEBRIDGE: Mr Chapman, data transfer is one area where you have risk, isn't it, for the data to leak or for cyber attacks to happen at the point of data transfer?

Mr CHAPMAN: Absolutely, yes.

Mr DAVID SHOEBRIDGE: And you were answering some of Mr Searle's questions about one of those examples, where the protocol for data transfer itself had been compromised, and that potentially led to significant data leakages. Is that right?

Mr CHAPMAN: In relation to the Service NSW incident?

Mr DAVID SHOEBRIDGE: Correct. No, in relation to the—sorry, I forgot the name of that firm.

The Hon. ADAM SEARLE: The Health breach.

Mr DAVID SHOEBRIDGE: The Health breach. Is that right?

Mr CHAPMAN: Yes. So, essentially what Accellion File Transfer Appliance is—is a document that transmits information securely, yes.

Mr DAVID SHOEBRIDGE: And it was not secure, and that is where the data breach happened?

Mr CHAPMAN: Yes, there was vulnerabilities detected via Accellion—the provider—yes.

Mr DAVID SHOEBRIDGE: And perhaps one of the most vulnerable ways of transferring data is by email. Would you agree with that?

Mr CHAPMAN: It is one of many, yes.

Mr DAVID SHOEBRIDGE: But it is a very vulnerable one?

Mr CHAPMAN: Depending on how it is configured, yes.

Mr DAVID SHOEBRIDGE: Particularly if you do not have multi-factor authentication when you are sending emails—sorry, when you are logging on to email services. There are all sorts of risks with email transfers, aren't there?

Mr CHAPMAN: There are, yes.

Mr DAVID SHOEBRIDGE: Including human risks?

Mr CHAPMAN: Correct.

Mr DAVID SHOEBRIDGE: Would it be fair to say that if you were designing a system that wanted to protect people's privacy and have as many layers of cybersecurity as possible, you would not start with emails?

Mr CHAPMAN: Which is why agencies across New South Wales were actually, in fact, using Accellion as an alternative to email.

Mr DAVID SHOEBRIDGE: But the agency sitting right next to you now, Service NSW, continues to send large amounts of data by email. Are you aware of that?

Mr CHAPMAN: That is a matter for Service NSW's practices.

Mr DAVID SHOEBRIDGE: Well, I am going to ask you, first of all, Mr Chapman, if you are aware of that.

Mr CHAPMAN: I would have to take that on notice. I am not aware of the current update in relation to controls that may or may not have been implemented within Service NSW.

Mr DAVID SHOEBRIDGE: Mr Rees, you are aware that in the report from December last year from the Auditor-General it says Service NSW has still "not put in place any technical or other solutions to avoid Service NSW staff having to scan and email personal information to some client agencies." Has that been remedied since the December report from the Auditor-General?

Mr REES: So, Mr Shoebridge, I think one of the most important recommendations in that is removing the dependency on email for the transfer of information. I think there is three elements to that from our perspective.

The first is just to remove the capture and the storage of information in its first place wherever possible, and therefore we have got a big focus on that. One of the actions that we took last year was to remove all email held in the accounts of customer service staff that was over 60 days old. So that one action on its own reduced the amount of email held in those mailboxes by about 92 per cent. We have got further controls on top of that that are searching for specific points of information and removing them in a faster time frame.

So part one of this risk is to hold less; part two is to find a secure alternative to the transfer of information. We have a number of technologies that we are looking at there and piloting at the moment. We need to be very careful that when we make that change, we make it to a more secure alternative and that we get the processes and the human elements right around that, as well as the technology. And the third element of that, we believe, is to remove the manual handling of information altogether wherever possible; whether that is via whichever technology platform. That requires, in many cases, the fundamental digitisation of those processes end-to-end so that the information does not have to be manually handled. It is an important piece of work. It is not a quick or easy or fast piece of work, but that is the work that we are mobilising now with our partner agencies.

Mr DAVID SHOEBRIDGE: But the privacy risks of sending data by email has been explained to your agency and recognised by your agency since 2015. You say it is not a rapid fix, but you have been on notice about these data risks, particularly sending information through emails that do not have MFA, since 2015. That is true, isn't it?

Mr REES: I would need to take on notice when concerns were first raised in that space.

Mr DAVID SHOEBRIDGE: Well, the Auditor-General says since at least 2015. I assume the Auditor-General is accurate.

Mr REES: I will need to take the question on notice.

Mr DAVID SHOEBRIDGE: Alright. I asked you, Mr Rees, whether or not Service NSW is still sending personal information by email and I have not yet got your answer.

Mr REES: The Auditor-General's report lays out—and our response to that lays out—time frames for removing the dependency on email to transfer information. We are working to those time frames. Right now, yes, there is an ongoing dependency on email. The amount of email that is held is drastically reduced and the security of that platform has been strengthened. But right now, yes, there is an ongoing dependency until the rest of those plans are completed.

Mr DAVID SHOEBRIDGE: What personal information about people in New South Wales is being sent by email from Service NSW? What information is it?

Mr REES: The types of information that were impacted in the cyber incident and held by email typically related to either where there was a paper form or process that was required, so customers may need to provide personal information as part of completing that. That could range from name or date of birth or phone number, through to more sensitive pieces of information such as particulars around your driver's licence. And the other key risk we saw there was where there is a need to transfer personal information between Service and other agencies.

Mr DAVID SHOEBRIDGE: So people's driver's licence details and the information related to their driver's licence is still being sent by email from Service NSW to other government agencies? Is that right?

Mr REES: There will be a continued dependency on that until those plans that we committed to as part of the Audit Office response are complete, that is right.

Mr DAVID SHOEBRIDGE: When can people in this State be comforted that their information will be protected and no longer sent by email like this from Service NSW? Is there a deadline?

Mr REES: I think we need to be ever vigilant about the safety of our personal information. We are already working towards that, and through the course of this year we will if not eliminate then greatly reduce the dependency on email for handling of information.

Mr DAVID SHOEBRIDGE: Mr Chapman, one of the greatest risks in terms of cybersecurity is not just the infrastructure, but it is the protocols for access to infrastructure, who can access it and whether or not you can tell if somebody's private information has been accessed—so the logging of access points. Is that true?

Mr CHAPMAN: That is correct.

Mr DAVID SHOEBRIDGE: Are you aware that Service NSW still uses Salesforce and does not have protocols that actually enable it to tell who is logged in, what information has been accessed and when?

Mr CHAPMAN: I am aware that Service NSW do use Salesforce, but no, I was not aware of the latter point, no.

Mr DAVID SHOEBRIDGE: Mr Rees, why is it that Service NSW first of all still uses Salesforce, an IT program that the Auditor-General says is not fit for its current purpose of being a very large database with Service NSW? Why are you still using Salesforce?

Mr REES: Salesforce is a product used by many organisations. The key concerns identified by the Auditor-General have been remediated. We need to be—like any platform—making sure that our ongoing use of that product remains fit for purpose and continuing to strengthen both the controls but, as you flagged, also the method of our usage and our processes that sit around that.

Mr DAVID SHOEBRIDGE: The Auditor-General said there were no reviewable logs of access to Salesforce data, so that means Service NSW staff could have been accessing the data, potentially sharing it and no-one would have known. Was it true that there were no reviewable logs of access data?

Mr REES: We have a range of methods to ensure the appropriate handling of information within the organisation and we are—

Mr DAVID SHOEBRIDGE: But I asked you about that one, Mr Rees.

Mr REES: We are working to strengthen the quality and the use of logging around Salesforce.

Mr DAVID SHOEBRIDGE: Is the Auditor-General accurate when it says that you did not have—and as at December 2018, so far as I understand, still did not have—reviewable logs of access history for Salesforce?

Mr REES: That is correct.

Mr DAVID SHOEBRIDGE: Are they available now?

Mr REES: I need to take that on notice.

Mr DAVID SHOEBRIDGE: Has it been fixed since December and now?

Mr REES: We have remediated a range of risks around our use of Salesforce. I will need to take on notice the status of that particular item.

Mr DAVID SHOEBRIDGE: Salesforce is your big database, isn't it? It is your main customer relationship manager, isn't it?

Mr REES: It is one of a range of systems that we use.

Mr DAVID SHOEBRIDGE: Is it used to store information gathered from the COVID-19 app?

Mr REES: It is not used to store the contact tracing information that we gather.

Mr DAVID SHOEBRIDGE: What is?

Mr REES: That data that we gather through the COVID check-in is stored in a completely different system.

Mr DAVID SHOEBRIDGE: What system?

Mr REES: I will need to take on notice the actual technology.

Mr DAVID SHOEBRIDGE: Is it stored in Australia?

Mr REES: Yes.

Mr DAVID SHOEBRIDGE: What firm? What company? Is it outsourced?

Mr REES: I will take that question on notice.

Mr DAVID SHOEBRIDGE: Have you got privacy controls on the information under the COVID-19 app that you have worked through with the Privacy Commissioner?

Mr REES: We do. The introduction of that service had an external privacy impact assessment and the Privacy Commissioner was consulted as part of the delivery of that service.

Mr DAVID SHOEBRIDGE: Are you aware that the privacy documentation for Service NSW does not include details or information about the exemptions under the health legislation, which is what is used to share information on the COVID-19 app with NSW Health?

Mr REES: The sharing of contact tracing information from the COVID check-in to Health is covered under the privacy consent statement for that service with customers.

Mr DAVID SHOEBRIDGE: Can you provide a copy of that privacy consent statement to the Committee?

Mr REES: I will take that on notice.

Mr DAVID SHOEBRIDGE: Has Cyber Security NSW double-checked the cybersecurity levels for that COVID-19 information that is being gathered by Service NSW under their app?

Mr CHAPMAN: I would have to check, Mr Shoebridge, about the exact involvement of Cyber Security NSW.

Mr DAVID SHOEBRIDGE: Are you aware that there is talk of, effectively, a vaccine passport being developed, Mr Chapman?

Mr CHAPMAN: Yes, I am aware of that.

Mr DAVID SHOEBRIDGE: Mr Rees, are you aware of those discussions?

Mr REES: At a high level, yes.

Mr DAVID SHOEBRIDGE: Has there been discussions about Service NSW having a role in that vaccine passport?

Mr REES: There has been public commentary around whether a tick should be available within the Service NSW application to indicate whether or not somebody has received a COVID vaccination.

Mr DAVID SHOEBRIDGE: Are you involved in developing the cybersecurity controls for a vaccine passport?

Mr REES: At this point I do not believe there is a decision around what services will proceed. If something were to progress like that then that would involve a range of people and a range of organisations assuring the cybersecurity around it.

Mr DAVID SHOEBRIDGE: Mr Chapman, have you been asked to do any advanced planning to ensure that if there is a vaccine passport using the Service NSW app that we can be confident that it will have cybersecurity controls to keep everyone's information protected?

Mr CHAPMAN: Cyber Security NSW, to the best of my knowledge, at this point in time has not. We do, however, provide advice through the information and communications technology [ICT] assurance process and advice more generally on secure by design.

Mr DAVID SHOEBRIDGE: But surely this is the exact kind of thing Cyber Security NSW is designed for. This will be a significant move—maybe an essential move—but surely you could not do that kind of work without knowing up-front that it could be secure and that Cyber Security NSW had signed off on it.

Mr CHAPMAN: Up until this point of time, Mr Shoebridge, we are, I guess, approached at disparate times for various projects, so for example the digital driver licence. If we do not have the capability internally prior to receiving the funding, we would make recommendations to the program management office about who they should engage outside of government to assist.

Mr REES: Maybe I can add to that. If an initiative like that were to go ahead, it is the type of initiative with the inherent privacy and security considerations around it where we would engage a range of external organisations from the start in the design and the delivery of that service.

Mr DAVID SHOEBRIDGE: But we are in the middle of starting the rollout of vaccines at a Federal level now. Are you saying that that basic preparation has not been done, that you have not got the advice and you do not know how a vaccine passport could be secured? Are you saying that has not happened yet, Mr Rees?

Mr REES: I can only speak to the involvement that Service NSW has rather than initiatives that maybe are being progressed more broadly. From a Service NSW perspective, the discussions that we are part of is whether an indication of whether you have received that vaccination or not should be displayed in the Service NSW app in the form of a tick, and those discussions are early and, to the best of my knowledge, have not been finalised yet.

Mr DAVID SHOEBRIDGE: Surely you could not provide advice about whether or not that information would be provided on a Service NSW app unless you had absolute confidence that people's health records could be absolutely secure.

Mr REES: That is correct.

Mr DAVID SHOEBRIDGE: What advice have you provided?

Mr REES: We have not provided formal advice yet. We are still working through what the options are in that space.

The Hon. TAYLOR MARTIN: Going back to a few of the questions that Mr Shoebridge asked earlier around where the data is stored and which entity it is that stores our data. I am glad you took it on notice. Is it a security risk to even discuss which entity stores our data if that is not already publicly known?

Mr REES: It is a good question. Mr Chapman and Mr Wells can speak to this more authoritatively than I can. It is certainly one of the risks and our goal is to be as transparent as possible both with this Committee but with the public as well, but that needs to be traded with the risk of creating public risk through providing too many specific details around the way services are delivered, the technology that is used and the way that technology is configured.

The Hon. TAYLOR MARTIN: Mr Wells?

Mr WELLS: As both Mr Rees and Mr Chapman have talked about, the process, while it is in early stages of designing what the solution is, goes through a very rigorous set of considerations about where the data sits, how it is managed, who can access it, what audit logs go with it et cetera. So all of that process is part of the design of all systems up-front. It is overseen by an ICT assurance process that is mandatory as part of all of this as well. Those controls happen as soon as you get into the details of exactly that.

The Hon. TAYLOR MARTIN: Mr Chapman, did you have more?

Mr CHAPMAN: No, nothing further to add, just to reiterate the ICT framework that Mr Wells mentioned and the fact that Cyber Security NSW provide input to that process.

The CHAIR: Has the Department of Customer Service taken the actions recommended by the Auditor-General, to be taken by July last year, to improve the security of the Registry of Births, Deaths and Marriages?

Mr WELLS: I cannot speak to the specifics of the Department of Customer Service. While we are in and part of the Department of Customer Service, we have got a whole-of-government view and a whole-of-sector role in terms of uplifting that capability, so I might need to take that on notice and come back to you.

The Hon. ADAM SEARLE: I am happy for you to do so.

Mr WELLS: But I would say that the Department of Customer Service is one of the first to access the funding to uplift capability so is committed to doing that. It has taken the incidents recently very seriously. It has stood up a program of work called Program Trust across the cluster, which involves all of us—the Commissioner for Resilience and the Cybercrime Commander—that is really taking a holistic view across customer service to uplift our capability. It is taking it very seriously.

The Hon. ADAM SEARLE: The audit report into the integrity of the births, deaths and marriages registry found that births, deaths and marriages has no direct oversight of the database and is very much reliant on third party assurance, a private company holding and maintaining that data. What is being done to address that and how many and what percentage of State agencies are also, as it were, hostage to private providers holding customer data, that is public data, given to them by State agencies?

Mr WELLS: Maybe I would start with, in order to provide the services to government those suppliers must be on something called the ICT Services Scheme. It is the way we procure services. In order to get on those panels they need to satisfy—

The Hon. ADAM SEARLE: Just pausing, that was not the question. The question was, what percentage of government agencies have the data they get from customers held by the companies?

Mr WELLS: We do not have the statistics. I can take that on notice.

The Hon. ADAM SEARLE: Please do.

Mr WELLS: What we do not have is the statistics on numbers of agencies that have components of that service provided by third parties. What I would say is that those contracting arrangements I was talking to mandate the same controls we have internally but those third-party providers must notify us of security incidents, privacy breaches on all those issues.

The Hon. ADAM SEARLE: Sure. But, given we do not know how many or what percentage have that exposure, it is fair to say we also do not know how much of that customer data given by State agencies is actually held here in Australia, or may be held on servers overseas. Is that correct?

Mr WELLS: Again, I would say it is more about the controls that are put in place with third-party providers than it is about where the data resides. That is the most important thing and that is what is mandated, again in the cybersecurity policy and from our procurement processes across—

The Hon. ADAM SEARLE: I understand. I am saying tomato, you are saying tomato.

The Hon. NATALIE WARD: Can he finish the sentence, please?

The Hon. ADAM SEARLE: Answer my question: It is fair to say we do not know what data of our citizens is actually held here, either New South Wales or Australia, and which is held overseas? That is correct, is it not? You have no idea.

Mr WELLS: Each cluster will know that, because that is the arrangement they go into with these providers.

The Hon. ADAM SEARLE: But you are the central agencies for data, are you not? Is not this the idea of having Cyber Security NSW, that you have visibility of the whole State sector?

Mr WELLS: What our role is, is to make sure that each cluster builds capability. We share intelligence, we run exercises, we build that capability across. It is not to understand where every cluster's exact data is. We do specifically look, as Mr Chapman said, for reporting around Crown jewels the most important systems and data that clusters hold and run, but it is not specifically to understand every component of that, no.

Mr DAVID SHOEBRIDGE: But there is no mandatory requirement for New South Wales residents' data, government data, to be held onshore, it could be held anywhere?

Mr WELLS: Yes. I mean, the State Records Act specifically enables data to be held anywhere, contingent on that risk assessment of how it is maintained, who can access it, etcetera, etcetera.

The CHAIR: We are at time. Thank you very much. I appreciate your time with us this afternoon.

(The witnesses withdrew.)

MALCOLM LANYON, Deputy Commissioner, Corporate Services, NSW Police Force, sworn and examined

DAVID HUDSON, Deputy Commissioner, Investigations and Counter Terrorism, NSW Police Force, sworn and examined

The CHAIR: You are welcome to make a brief opening statement if you wish.

Deputy Commissioner HUDSON: Thank you, Chair. I have a brief opening statement. Thank you and the Committee members for the opportunity to give evidence to assist this Committee's inquiry. I am joined here today by Deputy Commissioner Malcolm Lanyon, who has, amongst many other things, the responsibility of our internal information and technology systems. He therefore has the responsibility to protect our internal systems. As the Deputy Commissioner for Investigations and Counter Terrorism, I, amongst many other things, am responsible for the investigation of cybercrimes. Hence, from the outset I would like to clarify as to how we distinguish between cybersecurity and cybercrime.

Cybersecurity covers all measures to protect our systems and information stored in those systems. Cybercrime is an attack on those systems. It can either be cyber enabled or cyber dependent. Cyber enabled is a traditional crime type facilitated through a computer or the internet. Cyber dependent crimes are those committed directly against computers and computer systems. Hence, an easy analogy is that if cybersecurity is the defence, cybercrime is the attack. There is obviously a great deal of crossover and what we do in both these areas; however, I thought it was important to make this distinction early in our evidence so we do not mislead the Committee.

The CHAIR: Thank you. I appreciate that.

Mr DAVID SHOEBRIDGE: Thank you for the brief opening. The New South Wales police were given $44.8 million in the 2013-14 budget to replace the Computerised Operational Policing System [COPS]. Has it been replaced?

Deputy Commissioner LANYON: Not at this stage, Mr Shoebridge. We are currently going through a process at the moment. There has been a fairly lengthy process to acquire and ensure that we have the best system going forward.

Mr DAVID SHOEBRIDGE: But you were given $44.8 million in 2013-14. What happened to that $44.8 million?

Deputy Commissioner LANYON: That has been currently subject to a Treasury process as part of the ongoing funding for what will be the Integrated Policing Operating System [IPOS] system.

Mr DAVID SHOEBRIDGE: Have you spent it?

Deputy Commissioner LANYON: Certainly in terms of upgrading the current COPS, yes we have. And in terms of developing what will be the IPOS process. So, certainly we have invested into the current COPS to make it maintain its operational function.

Mr DAVID SHOEBRIDGE: Well, you need to, because the COP system is older than most of your constables out on the street, is it not? It is coming up to its twenty-sixth birthday.

Deputy Commissioner LANYON: It has certainly been a reliable and longstanding system within the NSW Police Force and it remains our core operating system.

Mr DAVID SHOEBRIDGE: The core IT infrastructure of the police is now, is it twenty-six or twenty-seven years old? How old is COPS?

Deputy Commissioner LANYON: I would have to take that on notice, but twenty-six or twenty-seven years would be accurate. It has certainly been a lengthy period of time.

Mr DAVID SHOEBRIDGE: And you were given $44.8 million in the budget in 2013-14 to replace it and you still have not done it?

Deputy Commissioner LANYON: That is correct, Mr Shoebridge. I think I have answered that.

Mr DAVID SHOEBRIDGE: Then you had a venture with Accenture. Do you remember the New COPS?

Deputy Commissioner LANYON: Yes, I do.

Mr DAVID SHOEBRIDGE: New COPS was meant to replace Old COPS, is that right?

Deputy Commissioner LANYON: Correct.

Mr DAVID SHOEBRIDGE: How much did the police spend on New COPS?

Deputy Commissioner LANYON: I would have to take that on notice, Mr Shoebridge.

Mr DAVID SHOEBRIDGE: Was it another $44.8 million?

Deputy Commissioner LANYON: I am sorry, I do not know off the top of my head. I will take that on notice, and I am happy to provide that to the Committee.

Mr DAVID SHOEBRIDGE: What came of New COPS?

Deputy Commissioner LANYON: New COPS was part of a transition. We are currently operating with the COPS. New COPS, or what was proposed to be New COPS, was to be the way forward for the COP system. A very lengthy process was taken to ensure that the system that we had to go forward would be the right one. New COPS has transitioned into what I will call IPOS, which will be the operating system of the organisation.

Mr DAVID SHOEBRIDGE: No, Mr Lanyon, New COPS has not transitioned in IPOS. New COPS was dumped in October 2017 because it was found it was not going to work.

Deputy Commissioner LANYON: New COPS was not dumped as such. New COPS was part of the transition across. So, basically it has been an evolution, Mr Shoebridge. It has not been one, neat step. New COPS was certainly an upgrade to what we currently had. So, the COPS operating platform has been ongoingly developed as we have gone through.

Mr DAVID SHOEBRIDGE: The new COPS was never implemented. It was paused in October 2017 and it has never been restarted. That is true, is it not?

Deputy Commissioner LANYON: That is correct, Mr Shoebridge.

Mr DAVID SHOEBRIDGE: How much was spent on the new COPS, did you say?

Deputy Commissioner LANYON: I have just said that I will take that on notice, Mr Shoebridge.

Mr DAVID SHOEBRIDGE: So after the initial $44.8 million did not go anywhere, the new COPS did not go anywhere. We are coming up to the twenty-sixth or twenty-seventh birthday of COPS and now you have gone out to market for this new thing called IPOS. What is IPOS?

Deputy Commissioner LANYON: IPOS is an operating system which would consist of what would be a computer aided dispatch system, which we currently have, and a record management system. Essentially it will be a system that will deliver the core policing functions for the NSW Police Force.

Mr DAVID SHOEBRIDGE: It is the Integrated Policing Operating System. Is that what it stands for?

Deputy Commissioner LANYON: Correct, Mr Shoebridge.

Mr DAVID SHOEBRIDGE: That is with a US company?

Deputy Commissioner LANYON: At this stage we have not entered into a contract so it would be premature to say who that would be with, Mr Shoebridge.

Mr DAVID SHOEBRIDGE: But it is going to be a cloud platform, is that right?

Deputy Commissioner LANYON: That is certainly the intention.

Mr DAVID SHOEBRIDGE: Is there a requirement that data be stored onshore?

Deputy Commissioner LANYON: There is a Protective Security Policy Framework, which I will certainly defer to Mr Hudson to talk about. Obviously before we can make a decision as to where information will be stored there is a very rigorous process to go through to ensure that.

Mr DAVID SHOEBRIDGE: We will come to that in a second. What is the current estimated cost for delivering the IPOS system?

Deputy Commissioner LANYON: If I could take that on notice. It will be a total cost of ownership over a period of approximately 15 years. If I could take that on notice I would be happy to provide that.

Mr DAVID SHOEBRIDGE: What is the ballpark, though?

Deputy Commissioner LANYON: Total cost of ownership is in excess of over $1 billion over 15 years.

Mr DAVID SHOEBRIDGE: And this is a project that is already seven years overdue, is it not? You had the budget in 2013-14.

Deputy Commissioner LANYON: I think it is probably misleading to say that nothing has been done with COPS or that the budget has not been used to develop COPS. COPS itself has been significantly upgraded over that period of time.

Mr DAVID SHOEBRIDGE: Given the reform was not delivered with the first $44.8 million, given new COPS was a dead-end, what comfort can the people of New South Wales have that the next $1 billion going on IPOS will actually finally produce something to replace the ageing COPS system?

Deputy Commissioner LANYON: I think significant comfort. The actual process that we have been through and the fact that we have put so much rigour into the process ensures that we have considered the risks. As you are well aware, there is no IT project that does not have considerable risk. One of the things that you can take comfort from is, for us to be funded for this project there are independent gate reviews which are conducted, not through the NSW Police Force but externally, to ensure that the process to acquire, the methodology that we are going through and the system that we are looking to implement is the correct system.

Mr DAVID SHOEBRIDGE: But I thought that the police shortlisted three contenders to deliver IPOS in May 2019? It was May 2019, was it not, when the three potential partners were shortlisted?

Deputy Commissioner LANYON: I believe that is correct, Mr Shoebridge.

Mr DAVID SHOEBRIDGE: Why are we still not advanced past all that and now we are in February 2021? Is it because the digital policing and operational systems director left?

Deputy Commissioner LANYON: No, that is not the reason at all. As I said, the reason is because substantial rigour has been put around the process to ensure that the system we implement is the correct one. I accept that it has taken a period of time. Ideally I would have liked it to have taken less time. But we do not wish to rush hastily into a system that is not going to be suitable for the organisation.

Mr DAVID SHOEBRIDGE: There is no risk of haste in a project that you were given almost $50 million to deliver in 2013-14 and you still have not delivered on. There is no risk of haste, is there, Mr Lanyon?

Deputy Commissioner LANYON: Mr Shoebridge, before you asked me about comfort. What I can say is, because of the detail we have gone into in the process I have great comfort that we are on the right track to move forward.

Mr DAVID SHOEBRIDGE: And our grandkids will have it in place, is that right, Mr Lanyon? When can we expect it to be delivered?

The Hon. BEN FRANKLIN: Point of order—

Mr DAVID SHOEBRIDGE: I withdraw that.

The Hon. BEN FRANKLIN: I would still like to make my point of order, if that is okay. I appreciate you withdrawing the comment, but my point of order is this: Like all members I am in favour of robust questioning, but this is beginning to tend towards incivility and I ask potentially that the member restrain a little from the tone he is using.

The Hon. ADAM SEARLE: It was pretty tame.

The Hon. BEN FRANKLIN: That is why my point of order was pretty tame too.

The Hon. TAYLOR MARTIN: It was dialling up.

Mr DAVID SHOEBRIDGE: Come on. It's Grandparents Day.

The Hon. ADAM SEARLE: Have you been downstairs?

The Hon. BEN FRANKLIN: The comment was withdrawn.

The Hon. NATALIE WARD: Also it was not $50 million. It was $44.8 million. That is nowhere near $50 million.

The Hon. BEN FRANKLIN: I am putting a line in the sand at the moment.

The CHAIR: Noted.

Mr DAVID SHOEBRIDGE: We will wind it back. What is your deadline for finally replacing the COPS system? Is it going to get its thirtieth birthday? Are we going to have a cake for it?

Deputy Commissioner LANYON: Mr Shoebridge, without wanting to run around your question, as I have said we are yet to finally enter into the contract for it. The contract will obviously specify those time lines.

I would prefer to come back to you once we have entered the contract with that information. Can I say the intent of the organisation is to implement the system as quickly as possible and to do so in a way that is sustainable and a good system. That is what we are aiming for.

Mr DAVID SHOEBRIDGE: Delaying the implementation of this comes with real costs, though, does it not? Just last year another $50 million was handed to IBM to keep the COPS system on life support. That is right, is it not?

Deputy Commissioner LANYON: As to the exact amount I will certainly come back to that, but it is essential that the COPS system remains functional. Irrespective of which system we implement, there will be a transition. We will be required to maintain the COPS system. I agree with you that the sooner we can implement IPOS the better.

Mr DAVID SHOEBRIDGE: But it comes at a real cost, because the COPS system now is so antiquated that IBM basically has the NSW Police Force over a barrel. They are the only ones who can maintain this fairly ancient infrastructure. I have it on good authority that there was a contract last year for another $50 million to IBM to keep it ticking over. Is that about right for the ballpark?

Deputy Commissioner LANYON: Mr Shoebridge, I have said to you that I am happy to take the cost on notice and come back to you with that. I do not disagree with you. The longer that it takes to enter into the contract, the more we are required to maintain the COPS system and hence our need to move this forward quickly.

Mr DAVID SHOEBRIDGE: But the police have entered into a contract with IBM. You say quickly, Mr Lanyon, but the police have entered into a contract with IBM to keep the COPS system running until 2024. That will be the thirtieth birthday of COPS, is that right? There is a contract with IBM to keep COPS running until 2024.

Deputy Commissioner LANYON: It is essential that the organisation has surety about its main operating system. There will be a period of transition even implementing a new system. With a system that is so complex you cannot just switch immediately from COPS to IPOS anyway, so there is a need to maintain the COPS system.

Mr DAVID SHOEBRIDGE: I say again, there is no risk of an immediate switch. This process started in 2013-14.

The Hon. TAYLOR MARTIN: There is risk with an immediate switch. That is what the Deputy Commissioner is saying.

Mr DAVID SHOEBRIDGE: Well, I am saying that there is no risk of an immediate switch. The project was commenced in 2013-14. We are eight years in and there is at least another three years to go because you have this contract with IBM.

Deputy Commissioner LANYON: And what I said before as part of my evidence, Mr Shoebridge, is that we are moving as quickly as possible to get into the IPOS program. I think you would be critical if you felt that we did not exercise due diligence as part of that procurement process. We are working through that. In any event the vendor must be able to implement the system. There will be a period of time that we will be required to maintain the COPS system until IPOS is functional. Even when it is functional, it is a staged approach for that to come in.

Mr DAVID SHOEBRIDGE: Mr Lanyon, will you provide on notice the full cost to date for whatever was spent out of the 2013-14 budget, then the new COPS and then whatever has been spent on the new IPOS project?

The Hon. NATALIE WARD: This is an estimates question about expenditure; it is not cybersecurity.

Mr DAVID SHOEBRIDGE: Could you provide that on notice so that we have a sense of how much this change to the IT security of the police is costing us?

The Hon. TAYLOR MARTIN: The Greens are worried about the budget for once.

The Hon. NATALIE WARD: We have been ably assisted about this particular topic area and I do not quibble with that, but now we are straying into the estimates area and I do not know that it is assisting this inquiry into cybersecurity to be honest.

Mr DAVID SHOEBRIDGE: I press the question. The cost of doing cybersecurity and the cost of IT transfer—if that is not relevant, I do not know what is.

The Hon. NATALIE WARD: Well and truly canvassed.

Mr DAVID SHOEBRIDGE: If the Government thinks the cost of IT projects is irrelevant, that is a matter for it.

The Hon. NATALIE WARD: I ask you to withdraw that. No-one has said that. I just believe that we have well and truly canvassed this question. I ask that we move on.

The CHAIR: That is fine. The question has been asked and it is relevant. The point is taken. You have been asked to take this question on notice. Is that something you are prepared to do?

Deputy Commissioner LANYON: I can certainly take that on notice.

The Hon. NATALIE WARD: Thank you for coming along and assisting the Committee. I want to ask about the Service NSW breach in particular, as much as COPS is interesting. Can I ask about that particular incident? I understand there were vulnerabilities in the system. I understand that is the case, but despite that can I ask you to comment on the criminal aspect? Ultimately this was a criminal act. There may have been some vulnerabilities, but ultimately this was a criminal act that I understand you are investigating. Can you inform the Committee about that investigation, without breaching what you are not able to tell us, but just generally about the investigation?

Deputy Commissioner HUDSON: I can answer that. The investigation is still ongoing. We have made some referrals to the Australian Federal Police [AFP], and we are waiting for some outcomes from that before we can progress further, but the investigation is still current and it is being investigated under Strike Force Seebree by the Cybercrime Squad.

The Hon. NATALIE WARD: I should have said at the outset it is being assumed to be a criminal act. It is not assumed to be any other—

Deputy Commissioner HUDSON: We believe there was malicious intent, which would make it a cybercrime. That is the distinguishing factor. Some data breaches are caused by human error. It certainly was not the case in this. It was malicious actors.

The Hon. NATALIE WARD: And it is an ongoing investigation. When do you think that might be arriving at a decision?

Deputy Commissioner HUDSON: We are reliant upon some information being returned to us from the Australian Federal police, so I think we have a fairly good handle on possibly what happened, but obviously we are waiting for information to come back to confirm that.

The Hon. NATALIE WARD: And this is not the only one. There are cyber attacks, I assume, happening all the time that you are asked to investigate. Is that correct?

Deputy Commissioner HUDSON: Cybercrime, dependent upon whether it is cyber-dependent or cyber-enabled, is on the increase. I think last year we had over 12,000 incidents reported to us. At the moment they are escalating about 7 to 8 per cent per month. Our Cybercrime Squad, because of that, from its infancy in 2017 when it was part of the fraud squad—it was an adjunct to the fraud squad, we created a standalone unit—staffing in that unit since that time has grown from 12 to 65, along with a lot of technical capability that we bring with that. I think we are the largest standalone cybercrime unit in Australia, including the AFP, and we have got some very smart people in that unit. I think, importantly, they are not just technical experts; they are detectives as well. So there is a mixture of those—unsworn technical experts, sworn technical experts and some very smart detectives.

The Hon. NATALIE WARD: And this is an evolving thing. It is not something like your traditional crime investigation; it is an ongoing, changing, evolving thing from various different worldwide entities at any one time. I do not think I am stating the obvious. I think the challenge for us and for policing, is it not, is that this is such an evolving framework.

Deputy Commissioner HUDSON: It is continually moving, and those with malicious intent will continually try to breach systems for profit, and that is basically the aim. It seems we develop a capability or cybersecurity experts create a capability to obviate a threat or negate a threat; criminals will try to find a way through that.

The Hon. NATALIE WARD: To my final point: Like any crime, you can do the best you can. In lay terms I can have a burglar alarm, I can have a dog and a fence and all the best intentions in the world. If someone wants to break into my house, they will do their very best to get around those and break into my house. I guess the equivalent in cyber is that with all the best intentions of government and everything that we can put in place, there are still vulnerabilities potentially that, should they want to, these criminals can get around. Would you agree with that?

Deputy Commissioner HUDSON: I totally agree. I think from our organisation, our internal perspective, we were an early adopter of the PSPF, Protective Security Policy Framework, when it was adopted by New South Wales Government from the Commonwealth, and that was because we deal with Commonwealth agencies significantly—the Australian Federal Police, the intelligence agencies—and overseas law enforcement agencies as well. So we had to be assured, and they had to have some assurance with us when sharing information that we were dealing with it appropriately. So we were very early adopters of information classification protocols, which includes technology, and I think we have been engaged with that since 2015.

All our staff are baseline vetted, security vetted to protected level, to access certain types of information. And, depending upon duty type, other people such as Deputy Commissioner Lanyon and myself are security vetted up to top secret, depending on the level of information we access, but we have to go through that process. A lot of it is governance around that process. The first step in protective security is governance of it. I chair a protective security governance committee, which meets quarterly for the NSW Police, where we look at cybersecurity, we look at personal security, we look at physical security for the organisation. And we hold the heads of different departments accountable for that and really drive that security framework and template through our organisation because if we are vulnerable then other agencies might refuse to deal with us.

The Hon. NATALIE WARD: You may or may not be able to answer this but just in your experience a percentage of that may well be systemic, it might be the systems that are in place, but a large percentage may well be human error. We have heard other evidence about the break-up of reporting federally about the different components, but sometimes it can just simply be human error for all the best systems in the—

Deputy Commissioner HUDSON: The last data I saw was that 32 per cent of data breaches are human error.

The Hon. NATALIE WARD: We have all done it—clicked on something that came through that we thought was an innocent attachment or something.

Deputy Commissioner HUDSON: Yes, and sent something probably inappropriate quite innocently. And that is a third of all data breaches. And as I said, to actually commit a cybercrime or a criminal act, you need some malicious intent, so they are investigated but obviously not prosecuted.

The CHAIR: How many of the cybercrimes that you are investigating or have investigated—I think you said 12,000 over the course of the last year—are against or have been against the New South Wales Government or its agencies?

Deputy Commissioner HUDSON: I would have to take that on notice. Obviously we are aware of—and through Cyber NSW we have matters reported to us and we are maturing that relationship all the time in relation to what the police involvement is in the sub-plan under the emergency management Act in relation to a cyber response. I think there is a meeting as soon as this Friday between Cybercrime and Cyber Security in relation to that, maturing that relationship and that communication flow. They have a very good relationship but it needs to be probably more formal and better articulated, so they are working through that. But the exact number of attacks on New South Wales Government, I would have to take that on notice. Obviously, I am aware of the Service NSW one, which we are still investigating, and one other which we are not investigating. It was not reported to us through that conduit.

The CHAIR: Thanks, and I am very happy for you to take it on notice. That is fine. Do you have a rough idea of a percentage of how much of the cybercrime that you investigate would be related to the Government?

Deputy Commissioner HUDSON: A small percentage. It is not significant compared to the broader context of what we do.

The CHAIR: I ask this question in two parts. The cyber attacks against government agencies that you would be looking at, compared to any sort of cybercrime, what are the types of things that you are seeing occurring? You talk about malicious acts. Are these from outside of Australia? Are they rogue operators? Is it organised crime? What are the types of things that you are seeing and investigating?

Deputy Commissioner HUDSON: From the opening, I made a distinction between cyber-enabled and cyber-dependent. Cyber-dependent crimes would be more of the attack on the systems that the Government would attract: the potential for malware, for denial-of-service attacks, the potential for hacking offences. Theft of information is always open. As I said, I would have to get back to you with details of the exact nature. There are many attempts, even our own systems. Phishing attacks—I think we were up to 200 a week at one stage on our systems—and if security protocols are in place the attacks are rejected. It is only when somebody actually gets through.

From a main attack point of view—I was speaking to Deputy Commissioner Lanyon before. I think we were 58 last year significant attacks on our systems, but none of them got through. Part of preventing an attack—and this is matters we are discussing with Cyber NSW—the way to stop an attack is to lock the people up that are doing it. The police have an integral role in that. You are right, though: Many of the attacks come from offshore. Many of them are computer-generated attacks, denial-of-service attacks, phishing attacks on different systems. So it is a fairly broad area, but I would have to come back to you with better detail on that.

The CHAIR: Yes, that is fine. Just one more question in this area: I note the comment about the percentage of general cybercrime compared to attacks on Government, but how could you be assisted in taking down the people who are doing it, to paraphrase how you put it? There is no requirement for people to report these things. I would imagine there are phishing expeditions on all of our devices and banking and all the rest of it all the time, and most of the time people would not report it. So are there ways that the Government can assist the police to do better with this so it is not growing at the exponential rates that we are hearing?

Deputy Commissioner HUDSON: The majority of reports that are made to the New South Wales police come from a Commonwealth system, ReportCyber, which has had a soft launch. It is a reiteration of the Australian Cybercrime Online Reporting Network, ACORN, which has moved to ReportCyber now. I am told that that will be promoted through the Commonwealth with a hard launch later on this year. We are receiving several hundred reports per month through that system, as well as other conduits: through our community portal and through our face-to-face at a police station reports. There are a number of different avenues for people to report crime. Having said that, we believe the reporting rate is quite low. It is always difficult to investigate a volume crime type, which this is becoming, when you only have part of the picture of it.

We probably need a better picture of what is happening through increased reports, which will give us, certainly, trends and better focus in relation to what our investigative efforts should focus on. So, we will be promoting that as well. Having said that—and in answer to your previous question about government attacks—out of the 12,700 cyber incidents over the past 12 months, less than 10 per cent of those are cyber-dependent crimes, which is an attack on a system. Most of them are cyber-enabled crimes. So, fraud or identity theft—those traditional crime types that are just facilitated through the use of a computer or the internet. Of the matters reported to us, the rate of cyber incidents targeting government agencies would be quite small. I am aware that most of them are private enterprise.

The Hon. ADAM SEARLE: Deputy Commissioner Hudson, in relation to the Cybercrime Squad—I think you said it comprises 65 persons at present.

Deputy Commissioner HUDSON: Yes.

The Hon. ADAM SEARLE: Are you able to tell us—if not, please take it on notice—how that is broken down by, if you like, police investigative personnel versus technical personnel?

Deputy Commissioner HUDSON: The squad is split up into three streams. I think currently there are 12 technical experts and we are employing three others at the moment, who are unsworn. Almost all of the others are designated detectives, but those designated detectives have interests and skills in IT, which has attracted them to that squad.

The Hon. ADAM SEARLE: Okay. And what is the overall budget for the function?

Deputy Commissioner HUDSON: I would have to take that on notice. It is obviously a component of our State Crime Command. The budget for the State Crime Command is allocated and it is a sub-allocation through that process, but I would have to take that on notice.

The Hon. ADAM SEARLE: That is okay. Is that squad conducting Operation Roche, which deals with the access to bushfire grants? Is that an investigation that is currently being undertaken?

Deputy Commissioner HUDSON: I am fairly sure that is being conducted by Financial Crimes, but I would have to take that on notice. It is a different squad of State Crime.

The Hon. ADAM SEARLE: I am happy for you to do so—and also, if you are able to, tell us on notice where that investigation is up to.

Deputy Commissioner HUDSON: Yes.

The Hon. ADAM SEARLE: I think you talked about the remit of the Cybercrime Squad being cyber-dependent or cyber-enabled and you have been talking about a range of offences which are in the nature of attacks on systems of various forms of fraud. Where does the unauthorised distribution of intimate images using technology for it? Is that also in the cybercrime unit or is that dealt with by some other part of the police?

Deputy Commissioner HUDSON: In relation to child exploitation?

The Hon. ADAM SEARLE: I was thinking more about the so-called revenge porn legislation that was introduced in 2017 and updated last year—about the unauthorised distribution of intimate images without people's consent. That is certainly cyber-enabled or technology-enabled, but is that investigated by this squad or it is it in some other part of the police?

Deputy Commissioner HUDSON: Depending upon the actual circumstances of it—depending on how clear cut—it could be investigated by the Sex Crimes Squad with Cybercrime assistance. But certainly, depending upon the level of technical capability, it could be investigated purely by the Cybercrime Squad.

The Hon. ADAM SEARLE: Okay. So, if it is just a case of, say, a former intimate partner taking intimate images and circulating them to his friends without the consent of the person who is the subject of the pictures, that would be the Cybercrime Squad's remit?

Deputy Commissioner HUDSON: They would have input into it. Most likely it would be investigated by the Sex Crimes Squad, who have responsibility for that revenge porn type of incident, with the technical expertise provided by the Cybercrime Squad. The Cybercrime Squad, apart from their own standalone investigations, also assist police area commands and districts and other State crime squads—and, indeed, the Counter Terrorism and Special Tactics Command in relation to their investigations as well—because they have that technical expertise.

The Hon. ADAM SEARLE: It might be a little bit off topic and I am happy for you to take this on notice—those revenge porn laws that were enacted in 2017. Can you tell us on notice how often they have been enforced by police—the number of prosecutions that have resulted from that? I am happy for you to take that on notice. I do not expect you to know.

Deputy Commissioner HUDSON: That should be easily obtainable but I do not have it with me.

The Hon. ADAM SEARLE: Thank you, Deputy Commissioner. Those are my questions.

Mr DAVID SHOEBRIDGE: Going back to the Operation Roche—the investigation into the potentially fraudulent access to bushfire recovery funds. What is the name of that operation, Deputy Commissioner Hudson? Otherwise it is going to get confusing.

Deputy Commissioner HUDSON: I do not have that in front of me. I am aware of the investigation. I do not have the specific strike force name; I will go with "Roche", if that is what you say.

Mr DAVID SHOEBRIDGE: I think it is, but I am going on memory, at this point. When was it commenced?

Deputy Commissioner HUDSON: It was last year—I think early last year—but I would have to take that on notice. It was shortly after the scheme was put in place.

Mr DAVID SHOEBRIDGE: It was following concerns that had been raised that outlaw motorcycle gangs and other organised crime figures had been seeking to inappropriately access the funds. Is that right?

Deputy Commissioner HUDSON: To a degree. We have taken this position since we have investigated a number of Commonwealth schemes in relation to child care: When any scheme is put in place, we believe that there will be those out there trying to take advantage of that. We have seen that through the compulsory third party insurance scheme when we investigated a number of people. I think we determined that out of the 13,000 claims made on that scheme, 7,000 were fraudulent for the compulsory third party scheme, which resulted in a reduction in premiums for compulsory third party insurance across the State.

That investigation tipped us into child care fraud—a Commonwealth program—which we investigated through Strike Force Mercury and arrested a number of operators and people associated with day care centres. Following that experience, government schemes will attract those who will try and find loopholes and vulnerabilities in those systems. So, we were quite alert to that when the scheme was announced. But outlaw motorcycle gangs and those associated with those individuals were certainly those who we believed would try and target that system.

Mr DAVID SHOEBRIDGE: And they did, did they not?

Deputy Commissioner HUDSON: Correct.

Mr DAVID SHOEBRIDGE: Do you have any idea of [audio malfunction] were targeted and unlawfully accessed by criminal elements?

Deputy Commissioner HUDSON: I would have to take that on notice.

Mr DAVID SHOEBRIDGE: Was there an audit undertaken by the relevant government agency and provided to police?

Deputy Commissioner HUDSON: In relation to those availing themselves—

Mr DAVID SHOEBRIDGE: Of the bushfire recovery funds.

Deputy Commissioner HUDSON: I am not 100 per cent sure of that. I will take that on notice.

Mr DAVID SHOEBRIDGE: Alright. And, if you could, give any details about the audit, if it existed—and I understand it did—and when or if it was concluded and provided to police.

Deputy Commissioner HUDSON: Yes. We will take that on notice.

Mr DAVID SHOEBRIDGE: And do you have any details of if there have been any prosecutions?

Deputy Commissioner HUDSON: There have been prosecutions out of that investigation.

Mr DAVID SHOEBRIDGE: Can you give any details about them?

Deputy Commissioner HUDSON: I can, on notice. I do not have those details with me.

Mr DAVID SHOEBRIDGE: Alright. The COPS system itself has, I think, in excess of 40 million private records. Is that right? You might know, Mr Lanyon; I am not saying you counted them.

Deputy Commissioner LANYON: I would have to take the exact number on notice, Mr Shoebridge.

Mr DAVID SHOEBRIDGE: But it is in the order of 40 million?

Deputy Commissioner LANYON: It is a significant number of records.

Mr DAVID SHOEBRIDGE: Yes. I think, Mr Hudson, you said that if organisations are going to trust the police to do the investigations about cybersecurity breaches, they need to be satisfied that you, yourself, have proper cybersecurity controls in place. That is true, is it not?

Deputy Commissioner HUDSON: Correct.

Mr DAVID SHOEBRIDGE: You would be aware of the LECC report that was delivered last year that showed there were not those rigorous controls in terms of access to the COPS database. False entries had been made by police and inappropriate and unlawful access had been obtained in the COPS database for unlawful reasons by police. You would be aware of that report that was handed down in March of last year by the LECC.

Deputy Commissioner HUDSON: I do not recall that report specifically, to be perfectly honest.

Mr DAVID SHOEBRIDGE: It was Operation Dukono.

Deputy Commissioner HUDSON: It does not strike a bell with me, Mr Shoebridge. But I can say that those—if data has been compromised internally—one of the considerations we are making as an organisation at the moment is whether we consider an insider threat program for the New South Wales police as has been done by many overseas departments. But there are offences created and offences caused by serving police or administrative officers accessing information inappropriately.

Mr DAVID SHOEBRIDGE: So you have not yet got an insider threat program, although there are 16,000 people who have access to the COPS database.

Deputy Commissioner HUDSON: We monitor our systems, but we are proactively looking for not just threats to—no other law enforcement agency in Australia has an insider threat program to my knowledge. We investigate matters through our professional standards command. We do regular audits of all accesses. I think everyone is audited at least once a year in relation to their access to the COPS system. There is a "reason for access" field on COPS. When you look someone up, you have to actually put down the reason as to why you have accessed that person and why you have accessed that information. All that information is audited regularly by the local command or the command that owns the officer involved. Sometimes through that process and sometimes through other investigations errant behaviour is detected in relation to access to systems or information. Those instances are investigated as a criminal investigation and prosecuted if required.

Mr DAVID SHOEBRIDGE: How many police have been prosecuted in the last two financial years for illegally accessing the COPS database?

Deputy Commissioner HUDSON: I am aware of several, but I would have to take the exact number on notice, unless Mr Lanyon, who currently has professional standards, is aware. I am unaware of the exact number.

Deputy Commissioner LANYON: I take the number on notice please, Mr Shoebridge. I will come back to you with that.

Mr DAVID SHOEBRIDGE: But let us be clear, there is no systemic, proactive program in place to identify, for example, surges of access to someone's data or inappropriate access to someone's data in the COPS database. You have not got a system-wide insider threat approach.

Deputy Commissioner HUDSON: We have an—which is about to be digitised—audit process in relation to how we audit the accesses of individuals but, bearing in mind as you quite rightly said, it is our main operating system. It is accessed probably by every police officer in the State several times a day for many reasons. All of our event information is contained within that system. All of our intelligence information is contained within that system at different levels requiring different levels of access security, but it is a vast system that, as you quite rightly said, was implemented in 1994 and has been built upon with numerous records since then.

Mr DAVID SHOEBRIDGE: Mr Hudson, are you telling me that there are paper audits of access to a database that has 40 million plus records in it? Are you really telling me it is a paper-based audit process?

Deputy Commissioner HUDSON: At the moment, yes.

Mr DAVID SHOEBRIDGE: How on earth can you do an effective paper-based audit process of a database with 40 million records on it? That is not achievable, is it, Mr Hudson?

Deputy Commissioner HUDSON: We are not auditing the records on the system. We are auditing the people that access the system.

Mr DAVID SHOEBRIDGE: Yes, but on your evidence police are accessing it multiple times a day—16,000 police and you have got 50,000 records a day. You could not possibly even scratch the surface of auditing access to that if you are relying upon a paper-based auditing system.

Deputy Commissioner HUDSON: That is why the "reason for access" for each access to the system has to be documented on the system and the audit is of those reasons for accesses.

Deputy Commissioner LANYON: Mr Shoebridge, I will add to Mr Hudson's evidence there. Even an automated process would not detect 100 per cent of what you are considering to be inappropriate accesses. The reason for doing it the way we do and auditing each officer is because it becomes quite apparent on the pattern of use by each officer as they do that. There is a very rigorous audit program that goes through each officer to look at their reasons for access.

Mr DAVID SHOEBRIDGE: But, Mr Lanyon, as you would well know because you have experience in looking at the database, the best way of identifying those kinds of patterns is not printing out people's access and then having a look at it under a lamp. The best way of doing it is putting some programs in place so you see suspicious patterns of access. You do not have that available on the COPS database right now.

Deputy Commissioner LANYON: I do not disagree with you at all and certainly IPOS gives us that ability to do that. That is why, when the IPOS system is implemented, we will have a far greater program of being able to do that. But at the moment the current computer access audits are effective in identifying usage patterns and have regularly identified persons when they do the wrong things.

Mr DAVID SHOEBRIDGE: Is there a system in place to correct false entries in the COPS database?

Deputy Commissioner LANYON: When they are identified? Is that what you asking?

Mr DAVID SHOEBRIDGE: Yes.

Deputy Commissioner LANYON: There certainly is. If an entry is identified to be erroneous, there certainly is a process to redress it.

Mr DAVID SHOEBRIDGE: I may have asked this earlier so I apologise if I am coming back to it. The current contracting or tender requirements for the IPOS, the integrated policing operating system—will it require that the data—these millions and millions of records of New South Wales residents' activities—is retained onshore?

Deputy Commissioner LANYON: It will require that the information is stored in accordance with the PSPF and appropriate systems. It is a cloud-based program and we would be looking to hold those records onshore.

Mr DAVID SHOEBRIDGE: Is it a requirement?

Deputy Commissioner LANYON: Can I confirm that and come back to you?

Mr DAVID SHOEBRIDGE: Alright. There is access to the New South Wales Firearms Registry through firearms dealers across New South Wales. What are the cyber security checks in place to ensure that that access to hundreds of dealers across New South Wales is secure?

Deputy Commissioner HUDSON: Are you talking in relation to the current trial we are going through with dealers through the dealer portal through the Salesforce product?

Mr DAVID SHOEBRIDGE: Correct.

Deputy Commissioner HUDSON: Yes, we are looking to change the system we deal, the main operating system and the way an individual applies for a firearms licence as well as a number of other components. The first component of that has been the dealer portal through Salesforce. That comes under our NSW Police Force operating system so the same governance is place around that system as around every other system in the IT world that we have in all systems.

Mr DAVID SHOEBRIDGE: Have you reviewed the Auditor-General's very critical findings about Service NSW's use of Salesforce database, talking about the vulnerabilities and the security concerns with Salesforce in their December 2020 report on Service NSW?

Deputy Commissioner HUDSON: I have read that. And I have taken that—because we are driving the project. Obviously one of the things I am also responsible for is the Firearms Registry, so we are driving that transformation of the digital platforms to get a better user experience for the 240,000 firearms licence holders in New South Wales. I have read that report.

Mr DAVID SHOEBRIDGE: I am asking about the data security, though.

Deputy Commissioner HUDSON: I have read that report. I have taken it up with the IT people that are building the system for us and they assured me the same things cannot happen.

Deputy Commissioner LANYON: Mr Shoebridge, can I just add to that? As part of any new operating system that we bring into the organisation, part of the architecture of that is that the Chief Information Security Officer for the organisation is part of the process so that information security is taken into account as part of introducing any operating system.

Mr DAVID SHOEBRIDGE: Well, perhaps, Mr Hudson, I will give you the opportunity to provide some additional comfort on notice about how those concerns raised by the Auditor-General about the use of sales force and its lack of security have been addressed by NSW Police on this project.

Deputy Commissioner HUDSON: Yes, I will take that on notice.

Mr DAVID SHOEBRIDGE: Have you used the capability yet?

Deputy Commissioner HUDSON: Have I personally used the—

Mr DAVID SHOEBRIDGE: No, the capability, which is that Federal database of facial recognition. It is called the capability; it is a pretty Orwellian nasty title but that is the name of it, the Federal integrated facial recognition database.

Deputy Commissioner HUDSON: The facial matching services, is that what you are talking about, the Commonwealth project?

Mr DAVID SHOEBRIDGE: Correct. It is called the capability. I did not come up with the name; some Orwellian bureaucrat federally did.

Deputy Commissioner HUDSON: Not in my world it is not, but anyway I will take your word for it, Mr Shoebridge. I have not used it. We have not as an organisation—we are still waiting for the Commonwealth legislation to pass before we provide any data to the system. I am aware that a number of other jurisdictions have uploaded data to the system; it is available to be used and we would use it if required. I am aware that some Commonwealth data is on the system as well as, I think, three States' data is on the system at this stage. We are not providing data until the Commonwealth legislation goes through.

Mr DAVID SHOEBRIDGE: Can I just indicate I endorse that approach? Of course, we would not provide our data until there was a legislative framework to protect it and I appreciate that, but you do have access to it.

Deputy Commissioner HUDSON: Yes.

Mr DAVID SHOEBRIDGE: And that is some Commonwealth data and some data from other States.

Deputy Commissioner HUDSON: Yes.

Mr DAVID SHOEBRIDGE: Has it proven useful?

Deputy Commissioner HUDSON: I have to take that on notice and get back to you because our biometric data is not loaded onto it. Our use of it would be negligible at this stage.

Mr DAVID SHOEBRIDGE: I can understand the limitations, because you have got a bunch of data here and unless you are linking it to that it is going to have limits.

Deputy Commissioner HUDSON: And we have used facial recognition for over 10 years in New South Wales and other systems with our charge photographs, so it is not new to us. Our charge photographs would probably give us better outcomes than a national system that does not have our State-based photographs contained within it at this stage.

Mr DAVID SHOEBRIDGE: My last question is about the potential cybersecurity risk from domestic-based terrorism. We have seen the internet used in other jurisdictions to promote mass attacks. The most recent would be the attack on the Capitol in the United States. What, if any, risks do you see in the cybersecurity space coming from particularly right-wing domestic terrorism?

Deputy Commissioner HUDSON: The use of the internet is of concern not just in terrorism but broader crime issues, so we have specialists that monitor that frequently or continually in relation to radicalisation, in relation to whether it be extremist, right-wing ideology or Islamic ideology, looking for those people that may be radicalised and escalating behaviour into a possible attack. We monitor that frequently. We monitor different environments to see established escalating behaviour and also monitor individuals, especially those on the high-risk terrorism offenders scheme, to establish if there is any possibility of an ongoing threat. In the terrorism space it is all about minimising the threat at the earliest opportunity. I think last year we saw the arrest of two brothers down south whose behaviour online was escalating in relation to right-wing extremism and we arrested those individuals at the earliest opportunity. Late last year we arrested a youth from Albury who was making online threats as well and his behaviour online was escalating.

So without being a cybersecurity issue, it is more of a cyberthreat and cyber crime. We use that as a tool to monitor the environment. The assessments from our intelligence agency say that the main focus of a possible attack will be simple weapons not cybersecurity incidents, so we are looking at vehicles, knives, guns, and that is the intelligence assessment that it has been that since 2014 when security levels escalated.

Mr DAVID SHOEBRIDGE: So as of yet, that kind of online organising, if I could put it neutrally, has not yet drawn its focus, at least systemically, towards cybersecurity? That is not where you see the threat coming, from that kind of online extremism?

Deputy Commissioner HUDSON: No, it does not eventuate in a cybersecurity threat; it more garnishes support for some more physical-type action.

The CHAIR: If there are no other questions, thank you. We very much appreciate your time this afternoon.

(The witnesses withdrew.)

The Committee adjourned at 15:57.