Submission No 27

INQUIRY INTO CYBERSECURITY

Name: Name suppressed

Date Received: 16 December 2020

21/10/20

Chair of the Cybersecurity Inquiry
The Hon. Tara Moriarty, MLC
Parliament House
Macquarie Street
SYDNEY NSW 2000

Cybersecurity Inquiry – We need to address the root causes, not just the by-products of the hacking

Dear Tara,

Thank you for your service to the people of New South Wales, and the chance to submit a letter to you today. I have spoken to **Sophie Cotsis MP**, as she has been in the media to raise the issues of cybersecurity and negligence. I contacted her after I read the article in the SMH June 20, 2020. She suggested I send you a letter to voice my concerns.

The intention of my contact today is to be as forthright as possible from my personal view, to
1) inform you of our need for a personal outcome, and
2) address what I see of a failing system, and
3) constitutional crisis issues.

I have gone beyond the possible terms of reference for the Inquiry itself, but I hope it will still be in context, and received as so.

1) Personal outcome required

My wife and I have received official notification of our data hacked at Service NSW. The data taken was my wife's and my birth certificates, child's birth registration, our driver's licenses, and also Medicare cards. The cross reference across this data is huge, knowing our location, children's details and some ages, parent's details and occupation at the time of our birth, and our faces, signatures, etc. I have spoken to Service NSW and raised the profile of our cases, and submitted an IPC complaint form, which is underway.

The safety of ourselves and our children are at risk, depending on what these criminals are after. The information is on the black market, available to the highest bidder. Child trafficking and abductions are in the news, black market prices of children I have heard fetch a high price. We don't know what the Government will do to make us safe in regards to these complex matters.

a) **What will be done to remedy the personal safety and ID risk of ourselves and our children?**

b) **What will be done with reimbursement of time and expense costs, as a minimum?** I work for myself, and all time taken in contact and remedy of the situation is not catered for. It is overall expensive, just in outlay of time.

c) **Is there appropriate compensation for the victims of this hacking?** This needs to be pushed, because if profit is the guiding principle for NSW Government making their decisions, then financial compensation is appropriate for the victims.

d) **Should victims continue to pay for Service NSW Services?**

2) Systemic problems

The fact that the Auditor General had highlighted major issues in the NSW systems back in December 2019, with little to no action taken, is appalling. The loss of personal data, personal and family security, and our "legal fiction ID" such as signature and names and facial imagery by an exclusive Government monopoly service without responsibility is unthinkable. The Service NSW IT dept as I believe is privatised with 70%

offshore...is this a weakness by design? I believe Clayton Barr MP and others spoke very strongly against the privatisation of Service NSW about 4 years ago.

Further, the systemic issues it presents is actually consistent with the lack of heeding advice. My neighbour advised me that his gun license was hacked at the Firearms Registry, so these criminals are not just targeting one thing. I found out that Land Registry Services is privatised against all public campaigning...is that a possible target of the next hacking?

My perception is that it is not just cybersecurity, but the underlying philosophies and methodology as an undercurrent in the NSW Government to maximise profits at any and all expense, that the people of NSW would never vote for at an election or referendum. The by-product is loss of control, loss of data, treason against the voter, and a domino-effect of litigation that doesn't solve the problem if it all goes wrong.

Cybersecurity Inquiry closed before all SNSW letters sent out.

The enquiry into cybersecurity...submissions closed on 20th September 2020 but as far as I know, the SNSW letters will continue to roll out until December...avoiding the majority of the public's letters and possible submissions. Was this strategic?

a) **Why isn't the NSW Government listening to and acting in the best interest of the people?**
b) **Why does NSW Government not heed the advice and report of the Auditor General?**
c) **Why are the cybersecurity enquiry submissions closed?**
d) **What departments are next?**
e) **What can be remedied to pull things back under NSW Government control and ownership?**

3) Constitutional issues

Good Government is not happening in certain instances

Privatisation of key assets and services discourage the people of NSW, and when data breaches happen, it is like we are at war economically and without any security, and without the backup of the NSW Government...they are the ones facilitating it.

NSW Constitution 1902 Section 5
The Legislature shall, subject to the provisions of the Commonwealth of Australia Constitution Act, have power to make laws for the peace, welfare, and good government of New South Wales in all cases whatsoever: **Privatisation of key assets and services and exposure of NSW people to risk is against this clause.**

Pecuniary interests and offices of profit disqualify parliamentarians

Revelations of NSW politician's pecuniary interests (corruption) seems to be fruit of the boon to privatise and subcontract, providing opportunities to obtain personal benefits through these deals. NSW Government needs to be impartial and have the welfare of NSW first and foremost on their minds, and the retention of key data under Government exclusive control.

Pecuniary interests and offices of profit under the Crown are forbidden, so what does the NSW Government see in privatising these things?

NSW Constitution 1902 Section 13.
(1) Any person who directly, or indirectly, himself, or by any person whatsoever in trust for him or for his use or benefit or on his account, undertakes, executes, holds, or enjoys in the whole or in part any contract or agreement for or on account of the Public Service shall be incapable of being summoned or elected or of sitting or voting as a Member of the Legislative Council or Legislative Assembly during the time he executes, holds or enjoys any such contract or any part or share thereof or any benefit or emolument arising from the same.

Treason against the voter

To commit treason against the voter (against their interest and representation), by exposing voters to risk, is a problem that needs Australia to stop and consider what is happening. Are we being sold out from

within? Privatisations and corporations bypass government and constitutional process, effective for international agendas.

I have seen Brad Hazzard in press interviews mention twice "New World Order" which is clearly an international banking and one-world-government agenda. Are these words and agenda being bandied around in Government meetings? I would not be surprised if this is an undercurrent to privatisation, restructuring, and bills being tabled to NSW Parliament. To residents of NSW, this is Treason and a Foreign Power. Is this the country that ANZACs gave their lives for?

NSW Constitution 1902 Section 34
If any Member of the Legislative Assembly—
(b) takes any oath or makes any declaration or acknowledgment of allegiance, obedience, or adherence to any foreign prince or power, or does or concurs in or adopts any act whereby he may become a subject or citizen of any foreign state or power, or become entitled to the rights, privileges, or immunities of a subject of any foreign state or power;

(e) is attainted of treason or convicted of felony or any infamous crime,

Governor's role in representing the Crown authority

It is my understanding that supreme in authority in NSW is our Governor, and that all bills approved by the Parliament must receive a Royal Assent via the Governor. But it also puts our Governor in a tough position where Parliament may have passed something against the best interest of the people of NSW, and the Governor almost has no other choice but to give it the assent. How do these privatisations and breach of good due process and outcome escape the monitor and address of the Governor?

I my understanding, our system puts the people as supreme (which is why we get to elect); we give our Parliamentarians the job of representing us, and the Governor and Crown give the Parliament the power to enact. It is my clear view that due process needs to be seen to be happening, with transparency, otherwise it probably isn't happening. Of high concern is the revelations of un-addressed corruption coming out in the news. I suspect that the whole system needs an unbiased and authoritative audit, with enforcement. Can we obtain help from the Governor to authorize a proper hearing and review?

Conclusion

I love Australia but I suspect we are being termited out from within. I would like to be able to give evidence if it is allowed. Please advise me if I have any course of action along these lines.

Yours sincerely,

Service NSW

Registered Post
Imprint
AUSTRALIA POST

AP Article Id:

7 September 2020

Ref Code: 1

Dear

DATA PRIVACY INCIDENT

I am writing to advise you that your personal information was exposed in a cyber security attack on the Service NSW technology network. We are very sorry that this has occurred and we are focused on assisting you to resolve any issues arising from this incident.

What happened?

An unauthorised and unknown third party accessed information contained in 47 Service NSW staff email accounts, using a phishing attack from late March 2020, which was detected in April 2020. At this stage of our investigations, we believe that the following personal information relating to you was contained in the information accessed in this phishing attack:

- **Medicare Card Details**
- **Driver Licence Details**
- **Registry of Births, Deaths & Marriages certificate**
- **Personal particulars**

Please refer to the enclosed Important Information, which sets out the practical action that we suggest you take in relation to the above categories of information.

What action have we taken?

Upon becoming aware of the cyber security attack, Service NSW immediately blocked access to the impacted email accounts to prevent any further exposure and engaged cyber security and privacy experts to help us respond to this incident. We also publicly announced the incident through a series of updates on the Service NSW website.

We have conducted a detailed analysis of the cyber security attack to identify the information that was exposed.

We have also reported the cyber security attack to the NSW Police, the Australian Centre for Cyber Security, the Information and Privacy Commission NSW, and the Office of the Australian Information Commissioner. Investigations into this incident are ongoing.

265178_07_V8

information and privacy commission
new south wales

Application Form **Updated September 2019**

Privacy Complaint: Internal Review Application Form

This is an application[1] for review of conduct of an agency under: (please select one)

- ☑ s53 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act)
- ☐ s21 of the *Health Records and Information Privacy Act 2002* (HRIP Act)

Your completed form must be sent to the Agency listed in Question 1 below.

1	Name and address of the agency[2] you are complaining about: SERVICE NSW GPO BOX 7057, SYDNEY, NSW, 2001
2	Your full name:
3	Your postal address: Telephone number: Email address:
4	If the complaint is on behalf of someone else, please provide their details: MYSELF, ALSO INCLUDES MY CHILDREN, MY WIFE, AND MY PARENTS What is your relationship to this person (eg. parent)? PARENT OF MY CHILDREN, HUSBAND OF MY WIFE, SON OF MY PARENTS Please include details of your authority to act or make the complaint on behalf of the person you have named above. CARER OF CHILDREN UNDER 18. WIFE WILL SUBMIT ONE HERSELF. PARENTS (NEED ADVICE) Is the person capable of making the complaint by himself or herself? ☑ yes SEE DETAILS ON ATTACHED FORM. ☑ no ☐ unsure
5	What is the specific conduct[3] you are complaining about? Describe what you believe the Agency did. *(see footnote for explanation of "conduct")* NEGLIGENCE TO PROVIDE PRIVACY PROTECTION, DESPITE AUDITOR GENERAL'S WARNING 6 MONTHS EARLIER, AND REPORTS SHOWING NSW GOVT AGENCIES ARE AT RISK. MY DATA AT SERVICE NSW WAS HACKED, ENDANGERING US
6	Please tick which of the following describes your complaint: *(you may tick more than one option)* ☑ collection of my personal or health information ☑ security or storage of my personal or health information ☐ refusal to let me access or find out about my own personal or health information ☐ accuracy of my personal or health information ☑ use of my personal or health information ☑ disclosure of my personal or health information ☑ other FAILURE TO PROTECT PRIVATE INFORMATION, DESPITE AUDIT WARNING. ☐ unsure

7	When did the conduct occur (date)? *(please be as specific as you can)* BETWEEN MARCH – APRIL 2020 (INFO FROM SERVICE NSW LETTER)
8	When did you first become aware of this conduct (date)? *(please be as specific as you can about how and when you first became aware of the conduct. Please include any action that you took at the time)* 14/9/20 REGISTERED LETTER RECEIVED FROM SERVICE NSW. REF CODE
9	You need to lodge this application within six months of the date at Q.8. If more than six months has passed, you will need to ask the agency for special permission to lodge a late application. Please explain why you have taken more than six months to make your complaint *(for example: I had other urgent priorities – list them, or while the conduct occurred more than six months ago, I only recently became aaware of my privacy rights, etc)*: JUST GOT NOTIFIED ON 14/9/20. WAS NOT MADE AWARE EARLIER.
10	What effect did the conduct have on you? IMMEDIATE CONCERN FOR PERSONAL AND CHILDREN'S SAFETY. OUR ADDRESS AND CONTACT DETAILS ARE KNOWN BY BAD PEOPLE, WITH UNKNOWN INTENTIONS HOW THEY WILL USE IT, OR OUR PERSONAL INFORMATION AND NAMES.
11	What effect might the conduct have on you in the future? UNABLE TO EASILY QUANTIFY OR (SAFETY FEARS) MITIGATE THIS RISK PERSONALLY OR FOR FAMILY, SO AS TO AVERT DANGER THAT MAY ARISE FROM IT. UNABLE TO PREVENT THE USE OF MY PERSONAL INFORMATION OR FURTHER HACKING BASED ON IT.
12	What would you like to see the agency do about the conduct? *(for example: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)* TO BE DETERMINED. AGENCY HAS A DUTY OF CARE TO FULFIL TO UNDO WHAT RISK THEY HAVE EXPOSED US TO, AND FULL COMPENSATION FOR EVERY SINGLE BREACH OF INFORMATION.

I understand that this form will be used by the agency to process my request for an internal review. I understand that details of my application will be referred to the Privacy Commissioner in accordance with: section 54(1) of the *Privacy and Personal Information Protection Act*; or section 21 of the *Health Records and Information Privacy Act*; and that the Privacy Commissioner will be kept advised of the progress of the internal review.

Your signature: _____

Date: 16/9/20

ATTACHED DOCUMENTS.
1) SERVICE NSW LETTER.
2) SMH ARTICLE (CYBER-SECURITY WARNINGS)
3) LIST OF DOCUMENTS & BREACHED INFO.

SEND THIS FORM TO THE AGENCY YOU HAVE NAMED AT Q.1

Keep a copy for your records.

For more information on the PPIP Act or the HRIP Act visit our website: www.ipc.nsw.gov.au
Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

---

1 It is not a requirement under the PPIP Act or the HRIP Act that you complete an application form. This form is designed for your convenience only. However, you must make a written request in some form to the agency for the matter to be a valid internal review.

2 The PPIP Act regulates NSW state government departments, area health services, most other state government bodies, and NSW local councils. Each of these is defined as a "public sector agency". The HRIP Act regulates private and public sector agencies and private sector persons.

3 "Conduct" can include an action, a decision, or even inaction by the agency. For example the "conduct" in your case might be a *decision* to refuse you access to your personal information, or the *action* of disclosing your personal information to another person, or the *inaction* of a failure to protect your personal information from being inappropriately accessed by someone else

Gmail

and family data privacy hacking

16 September 2020 at 09:52

To: privacy.hypercare@service.nsw.gov.au

Hello

Case manager has advised on my phone call 3:45pm 15/9/20 (ref code) that I can send a complaint about the data privacy hacking at Service NSW. Much personal detail of myself, wife, and children has been exposed to organised criminal networks who see financial value and power in our records. This brazen attack shows the lack of regard for the law, and likewise presents huge risk to myself and family on many levels.

Abductions and child trafficking is almost the largest and most profitable industry in the world, There is major concern that I and my family are in a potentially dangerous position, having our names, marriage connection, my birth certificate, parents names, our home address and children's names and our child's birth registration details among the stuff that was stolen. My signature and face photo on my license is also stolen. This creates a whole host of issues which we have not determined how to deal with,

The damning Sydney Morning Herald article on June 20, 2020 (attached to my complaint) says the Auditor General's report into the prone-ness of NSW Government data storage in December 2019 went unheeded, indicating systemic problems within departments such as inaction and carelessness. I personally have no guarantees or faith in the system if that's how bad it is.

The "one-stop-shop" taxpayer funded monopoly of Service NSW for major records and driver licenses without accountability or heeding Auditor General's warnings is unthinkable.

The immediate offer by Service NSW of replacement of cards etc and reprint of birth certificates indicates to me another systemic problem, like changing a password on an email account after the contents have been sent to criminals. It is a loss of data to Service NSW, but to me and my family it is a loss of safety forever, and Service NSW has the duty of care to remedy the true risk involved, and compensate properly for every breach of our data.

I have completed the IPC form, and included as much information as is privy to me. My case has been escalated for review at higher levels.

I look forward to hearing from you as a matter of urgency.

Yours sincerely,

IPC complaint - and family's data hacked at Service NSW.pdf
1468K

List of documents identified by at 3:45pm 15/9/20 (ref code:)

I have expanded on the information contained on the documents which is now at large.

Invoice for registering birth $51 – eft visa

Birth registration statement for our child

- : DOB and place of birth
- Mother's name, maiden name, occupation, age, birth location
- Marriage date and location
- brother's name and age
- mobile number
- mobile number
- Our home address

Birth certificate –

Birth certificate –

- DOB and place of birth
- Father's name, surname, occupation, age, birth location
- Father and Mother's marriage date and marriage location
- Mother's name, surname, maiden name, age, birth location
- Birth certificate number

Driver's license – (front and rear)

- Full name
- Home address
- DOB
- License expiry date
- Photo ID
- Signature
- License number
- Card number
- License class
- Conditions

Medicare card

- Card number
- Expiry date
- Names and initials of myself, my wife and 3 children (5 total)
-
-
-
-
-

The Sydney Morning Herald

NATIONAL NSW CYBER SECURITY

NSW government was warned over cyber security weaknesses

By Angus Thompson
June 20, 2020 — 7.16pm

Share A A A

The NSW government was warned more than six months ago to urgently improve its cyber security in a report that found almost half of its agencies had no recommended strategies in place to prevent attacks.

NSW was on Friday revealed to have been the target of a wave of sophisticated, foreign-actor data breaches, prompting Prime Minister Scott Morrison to warn the nation to brace for further incursions.

China has denied it is behind a major increase in cyber-attacks on Australian government agencies and Australian businesses.

NSW Premier Gladys Berejiklian this week announced a $240 million boost to the state's cyber security capabilities but the opposition has called for an inquiry into the government's protections after the Auditor General delivered a damning report card into agencies' defence strategies.

"The NSW Government's failure to invest in cyber security measures has left our digital infrastructure vulnerable – potentially putting critical health and public safety systems at risk," Labor's public service spokeswoman Sophie Cotsis said.

"A parliamentary inquiry into cyber security is needed to assess whether the NSW Government is doing enough to keep our state safe," Ms Cotsis said.

The state government's cyber security policy requires agencies to assess themselves against eight essential risk mitigation strategies set by the Australian Cyber Security Centre, a branch of the Australian Signals Directorate.

Cyber Security NSW received 62 responses, each ranking themselves against a "maturity level" scale of implementation of security measures across each category.

The results of the December 2019 assessment showed recommended mitigation strategies were non-existent, or had a "maturity level zero", in 47 per cent of responses from agencies.

In a report released last week the Australia Cyber Security Centre recommended two key harm migitation strategies which, if implemented, would greatly reduce the risk of data breaches.

One strategy was to patch applications with security fixes once they become available, but the December 2019 Auditor General's report showed 37 per cent of NSW agencies admitted not doing this.

The other key strategy was using multi-factor authentication processes, but 41 per cent of NSW agencies reported not doing that either.

Diep Nguyen, a senior lecturer at the UTS School of Electrical and Data Engineering, said it was important that all government agencies implemented the high security standards to prevent exposing "weak links" that would become vulnerable to potential attackers.

"Usually all of these networks are connected to each other, so one weak point will make the whole network vulnerable," he said.

In November last year the Auditor General reported there had been more than 3300 data breaches across NSW agencies as of March 31, however no costs were recorded against those incidents.

Last month Service NSW reported to police that the email accounts of 47 of its staff members had been compromised in a cyber attack. The agency revealed the data that was illegally access had been stored in the email records of the employees.

Via email:

Our reference:
Your reference:

2 October 2020

Privacy internal review

Dear

I refer to your email in relation to Service NSW's handling of your personal information that was received by our agency on 16 September 2020 and our discussion on 2 October 2020.

In your correspondence you stated that you would like to make a complaint about the failure of Service NSW to provide privacy protection for you and your family. In particular, the conduct of Service NSW despite warnings from the Auditor-General six months earlier and reports showing NSW Government agencies were at risk. You raised concerns that your personal and health information has not been collected and stored correctly and has not been protected from unauthorised access, use, disclosure or modification.

In response to your correspondence Service NSW will be conducting an internal review under section 53 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and section 21 of the *Health Records and Information Privacy Act 2002* (HRIP Act).

As part of the internal review Service NSW will review the conduct referred to in your correspondence according to its obligations under the Information Protection Principles (IPPs) in the PPIP Act and the Health Privacy Principles (HPPs) in the HRIP Act.

Relevant privacy principles

Below is a brief summary of the IPPs and HPPs that may be relevant to the concerns you have raised.

IPP 1 (PPIPA s8) and HPP 1 (HRIPA Schedule 1, section 1) – Collection: Lawful

An agency must only collect personal information for a lawful purpose. It must be directly related to the agency's function or activities and necessary for that purpose.

IPP 2 (PPIPA s9) and HPP 3 (HRIPA Schedule 1, section 3) – Collection: Direct

An agency must only collect personal information directly from you, unless you have authorised collection from someone else, or if you are under the age of 16 and the information has been provided by a parent or guardian.

IPP 3 (PPIPA s10) and HPP 4 (HRIPA Schedule 1, section 4) – Collection: Open

An agency must inform the you that the information is being collected, why it is being collected, and who will be storing and using it. You must also be told how you can access and correct your personal information, if the information is required by law or is voluntary, and any consequences that may apply if you decide not to provide it.

IPP 4 (PPIPA s11) and HPP 2 (HRIPA Schedule 1, section 2) – Collection: Relevant

An agency must ensure that your personal information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

IPP 5 (PPIPA s12) and HPP 5 (HRIPA Schedule 1, section 5) – Storage: Secure

An agency must store your personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

IPP 6 (PPIPA s13) and HPP 6 (HRIPA Schedule 1, section 6) – Transparent

An agency must provide you with details regarding the personal information they are storing, why they are storing it and what rights you have to access it.

IPP 11 (PPIPA s18) and HPP 11 (HRIPA Schedule 1, section 11) – Disclosure: Restricted

An agency can only disclose your information in limited circumstances if you have consented or if you were told at the time they collected it that they would do so. An agency can also disclose your information if it is for a directly related purpose and it can be reasonably assumed that you would not object, if you have been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

IPP 12 (PPIPA s19) – Disclosure: Safeguarded

An agency cannot disclose your sensitive personal information without your consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

HPP 14 (HRIPA Schedule 1, section 14) – Transferrals and linkage: Controlled

Only transfer health information outside New South Wales in accordance with HPP 14.

Who is conducting the internal review?

The reviewing officer is myself, , an Advisor employed by Service NSW. My position does not normally involve processing customer transactions for Service NSW and I was not involved in any matter relating to the conduct that is the subject of your application.

I am therefore performing my role as a reviewing officer who is substantially removed from any matter relating to the alleged conduct which is the subject of this application.

Completion date and review rights

Following your agreement, this privacy internal review will be completed **by 29 November 2020**, which is 60 days from the date your Proof of Identity check was completed at the Service Centre. Your complaint was received by Service NSW on 16 September 2020. However, as discussed, I request your consent for a two-week extension to conduct the review considering the delays encountered with the Proof of Identity checks.

On completion of the review you will be notified within 14 days of:

- the findings of the review (and the reasons for those findings)
- the actions proposed to be taken by the agency
- your right to have those findings, and the agency's proposed agency, reviewed by the NSW Civil and Administrative Tribunal (NCAT).

If the review is not completed by 29 November 2020 you are entitled to make an application to NCAT for administrative review of the conduct concerned.

Further information

If you would like to discuss this letter or the progress of the review, or submit any further relevant material, please contact me on or at GRP.Privacy&Complaints@customerservice.nsw.gov.au.

Your correspondence in relation to Service NSW's handling of your personal information and my draft review report will also be provided to the NSW Privacy Commissioner for the purpose of their oversight role under the PPIP Act. You can find more information about privacy complaint handling on the website of the Information and Privacy Commission: https://www.ipc.nsw.gov.au/privacy/citizens/make-complaint.

Yours sincerely

Advisor, Governance
Privacy & Complaints Review
Department of Customer Service

I AGREE TO THE ABOVE, ALSO TO NOTE THE COMPROMISE OF PERSONAL SAFETY FOR MYSELF AND ALL OTHERS ON MY IPC COMPLAINT FORM, AND LOSS OF EXCLUSIVE USE OF MY LEGAL FICTION, FACE, AND SIGNATURE. THAT SITUATION WILL NEED TO BE REMEDIED. REFER TO IPC COMPLAINT & EMAIL & ATTACHED DOCUMENTS SENT TO PRIVACY.HYPERCARE@SERVICENSW.GOV.AU ON 16 SEPT 2020 9.52AM.

NOTES FROM MY RESEARCH SINCE 16/9/20

* SERVICE NSW IT IS 30% ONSHORE, 70% OFFSHORE. PROBLEM BY DESIGN. (CLAYTON BARR MP)
* NEIGHBOUR ADVISED HIS GUN LICENSE HACKED @ FIREARMS REGISTRY.
* CYBERSECURITY SUBMISSIONS CLOSED @ NSW PARLIAMENT ON 20 SEPT 2020. WITHOUT ADVERTISEMENT. SERVICE NSW LETTERS TO BE ISSUED UNTIL DECEMBER. COMPLAINT OPPORTUNITY WINDOW FAR TOO SMALL.
* WHOLE SITUATION LEAVES ME VERY CONCERNED AT THE LOSS OF CONTROL AND OWNERSHIP AND RESPONSIBILITY OF NSW GOVT TO PROTECT CITIZENS. COVERING OF TRACKS AND AVOIDANCE OF RESPONSIBILITY.
* FURTHER PRIVATISATIONS AND PRONE-NESS TO HACKING ACROSS OTHER NSW GOVT SERVICES, OR SUBCONTRACTED SERVICES LIKE LAND REGISTRY SERVICES. WHO IS NEXT? IMPLICATIONS AND RISKS ARE PERSONALLY BORN BY NSW CITIZENS.

SUPPLIED TO ME BY CLAYTON BARR MP'S OFFICE STAFF ON MY VISIT ON 25/9/20 AT APPX 11:00 AM. I AM ADVISED BY THE STAFF THAT SERVICE NSW LOTTERIES MAY CONTINUE UNTIL DECEMBER 2020. SUBMISSIONS CLOSED ON 20/9/20. WAS THIS ADVERTISED?

LEGISLATIVE COUNCIL

PORTFOLIO COMMITTEE NO. 1 – PREMIER AND FINANCE

Inquiry into Cybersecurity

TERMS OF REFERENCE

1. That Portfolio Committee 1 – Premier and Finance inquire into and report on cybersecurity and digital information management in New South Wales, and in particular:

   (a) The number of cybersecurity incidents and data breaches involving NSW Government agencies;

   (b) The monitoring and response to cybersecurity incidents and data breaches across the NSW Government;

   (c) The policies and procedures underpinning the management of digital information by the NSW Government;

   (d) Systems management within NSW Government agencies including outages, backups and cyber security;

   (e) The financial costs and other impacts of cybersecurity incidents, data breaches and outages involving NSW Government agencies;

   (f) Expenditure on cybersecurity, digital services and digital infrastructure across the NSW Government;

   (g) The management of public access to digital information under GIPA and similar processes including coverage of mobile based and online platforms;

   (h) Contractual arrangements between the NSW Government and providers of digital services and infrastructure, including:
      (i) Provisions relating to cybersecurity generally; and
      (ii) Reporting obligations and the monitoring of cybersecurity incidents;

   (i) The extent and impact of outsourcing of government information systems, including:
      (i) Outsourcing to entities which are owned overseas;
      (ii) The risks involved with outsourcing government information systems.

   (j) The support provided by the NSW Government to local councils and other organisations in relation to cybersecurity;

(k) The NSW Government's response to cybercrime in the community generally; and

(l) Any other related matter.

Committee membership

Hon Tara Moriarty MLC	Australian Labor Party	*Chair*
Hon Robert Borsak MLC	Shooters Fishers and Farmers Party	*Deputy Chair*
Hon Ben Franklin MLC	The Nationals	
Hon Taylor Martin MLC	Liberal Party	
Hon Adam Searle MLC	Australian Labor Party	
Mr David Shoebridge MLC *	The Greens	
Hon Natalie Ward MLC	Liberal Party	

* Mr David Shoebridge MLC substituted for Ms Abigail Boyd MLC on 6 August 2020 for the duration of the inquiry

Cybersecurity

This inquiry was established on 6 August 2020 to inquire into and report on Cybersecurity.

Date	Milestone
06 Aug 2020	Self-referred
20 Sep 2020	Submissions closed
29 Oct 2020	Hearing - Macquarie Room, Parliament House, Sydney
20 Nov 2020	Hearing - Macquarie Room, Parliament House, Sydney

} 1.5 MONTHS. WHERE WAS THIS ADVERTISED? N.W.S. S.NSW LETTERS UNTIL DECEMBER 2020?