TAB A

PORTFOLIO COMMITTEE NO. 1 – PREMIER AND FINANCE

Inquiry into Cybersecurity

Inquiry hearing: 3 February 2021
Jubilee Room, Parliament House, Sydney

QUESTIONS TAKEN ON NOTICE
WITH ANSWERS

(NSW Police Force)

Question, p34

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.

Answer

The Computerised Operational Police System (COPS) was implemented in April 1994.

Question, p35

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.

Answer

In the financial year 2013/14, NSWPF was allocated $44.8million for the COPS Modernisation Program.

To date, $39.55M has been expended to enhance and upgrade COPS across a range of areas including improved user environments and web-based functionality.

This included enhancements across a range of capabilities including, a custody management form, spatial hub, a systems upgrade and new custody systems. Other COPS improvements are increased security and search capabilities, integration of COPS into other operating systems including JusticeLink and the ACIC and improvements for the capture of information around Domestic Violence incidents.

Question, p35

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.

Answer

Based on the Integrated Police Operating System (IPOS) cost estimates, there is a net funding requirement of $308 million during the implementation of IPOS in FY2021 to FY2027. Budget projections show the $308M allocation will be fully offset in the following 10 years (FY2028 to FY2038).

The IPOS program will be cost neutral over a 17-year timeframe. Over the 17-year period, current COPS and supporting systems will be decommissioned. The maintenance costs like licencing, upgrade and hardware support will be reduced for the old systems while at the same time, the IPOS system ramps up to full functionality. This will render the offset neutral.

Question, p37,38

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?

....

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

Answer

In the financial year 2013/14, NSWPF was allocated $44.8million for the COPS Modernisation Program.

COPS Modernisation Program Phase 3 was referred to internally as the “New COPS”. The aim of Phase 3 was to modernise operational processes and systems to enable NSWPF to improve policing response, reduce administrative burden and provide faster access to information. The allocated funding was to enable NSWPF to explore and commence a replacement option for the current COPS. The NSWPF was moving towards a solution with Accenture, however the venture with Accenture was not finalised and, in 2018, the NSWPF further developed the requirements and transitioned towards the current solution to replace the COPS system.

To date $39.55M of the original $44.8M has been spent and covers the costs associated with:

- Upgrades to the COPS system to ensure it continues to meet operational requirements
- the venture with Accenture and
- the pivot to the current solution, ie the Integrated Police Operating System (IPOS).

Since 2018, $22.6M in recurrent and $1.26M in capital funding has been expended to determine a viable solution and commercial partner for an Integrated Policing Operations System (IPOS) to replace COPS (and a range of other police systems). Expenditure includes procurement engagements, due diligence, contract negotiation and award process.

Question, p39

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.

Answer

There were 14,572 reports of cybercrime through ReportCyber in 2020.

There were seven cyber-related crimes reported by NSW government and its agencies in 2020 including the Service NSW breach.

Question, p39

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.

Answer

The NSW Police Force investigates all manner of cybercrime, including cyber attacks on government agencies. This can involve organised crime and/or rogue operators from within or outside Australia. Only a small proportion is executed from within NSW.

The types of things we are seeing and investigating are outlined in the table below which contains a breakdown for 2020. Fraud, online shopping scams and online bank scams are the most common cybercrimes reported and referred.

Referrals in NSW, breakdown by type – 2020	
Business Email Compromise	10.58%
Bulk Extortion	3.7%
Donation	1.14%
Fraud	23.33%
Harassment	2.19%
Image Shared	1.14%
Online Bank	12.6%
Ransomware	0.61%
Selling	5.7%
Shopping	21.58%

Types of reported cybercrime in NSW – 2020	
Business Email Compromise	1517
Bulk Extortion	536
Bullying	219
Donation	162
Fraud	3322
Harassment	312
ID Theft	1374
Image Shared	162
Investment	58
Malware	184
Online Bank	1821
Ransomware	87
Romance	644
Selling	816
Shopping	3099

Question, p40

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.

Answer

The overall operating budget for the NSW Police Force is outlined in the Annual Reports.

There are currently 68 staff in the Squad. This consists of 60 sworn officers and 8 unsworn technical personnel. Of the 60 Sworn Officers, 58 are Detectives.

The Cybercrime Squad has three units:

- Cyber Enabled Investigations – Criminal Investigations
- Cyber Dependent Investigations – Criminal Investigations
- Advanced Capability Unity – Technical experts

Strike Force Roche is being conducted by Northern Region. It was established to investigate allegedly fraudulent claims for Bushfire Recovery Scheme in the Northern Region.

To date a total of 16 people have been charged with offences. Matters continue to be investigated with the possibility of further arrests.

Question, p41

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.

Answer

There have been **855** Court Attendance Notices (CANs) issued to **832** individuals for relevant offences since these laws were introduced in 2017 (see list of offences below).

1. A person who intentionally distributes an intimate image of another person without the consent of the person and knowing the person did not consent to the distribution or being reckless as to whether the person consented, is guilty of an offence.
2. A person who intentionally records an intimate image of another person without the consent of the person and knowing the person did not consent to the recording or being reckless as to whether the person consented to the recording is guilty of an offence.
3. A person who threatens to distribute an intimate image of another person without the consent of the other person and intending to cause that other person to fear that the threat will be carried out, is guilty of an offence.
4. A person who threatens to record an intimate image of another person without the consent of the other person, and intending to cause that other person to fear that the threat will be carried out, is guilty of an offence.

The breakdown by year is shown in the table below:

Year	CANs	Individuals with CANs
2017	56	56
2018	196	191
2019	252	246
2020	306	302
2021	45	45
Grand Total	**855**	**832**

Question, p41

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.

Answer

Strike Force Roche was established in April 2020 within the Northern Region to investigate alleged fraudulent claims for bushfire disaster relief and small business grants through government agencies.

Question, p41 - 42 – NOTE – this question contains an audio malfunction.

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.

Answer

Strike Force Raptor did not receive an audit report. Police are constantly monitoring for unusual behaviour that may indicate fraudulent behaviour. In August 2020, Strike Force Fireant was established to investigate reports that OMCG members and associates were allegedly involved in unlawfully obtaining money through a Government grant scheme intended for persons and small businesses impacted by bushfires.

As at 26 February 2021, ten people have been charged for a total of 54 offences in relation to fraud relating to the accessing of the bushfire grant funds.

Investigations are ongoing.

Question, p42

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.

Answer

The COPS has 62.6 million 'Incident' records.

Question, p42, 43

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 numbers.

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

Answer

Three officers have been charged for unauthorised/unlawful accesses to COPS within the last two financial year periods.

Question, p44

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.

Answer

NSWPF uses the SalesForce engine as an Internet facing front-end for Community Portal and the Firearms Registry. This front end is 'stateless' and as such does not store any data in the SalesForce platform itself. Instead, data is pushed back to the NSWPF protected datacentre, which is built and operated to appropriate protective security standards.

Question, p44, 45

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.

Answer

NSWPF has access to the national Face Matching Service (FMS) (announced in 2017 by the Commonwealth as the National Facial Biometric Matching Capability). The Commonwealth has provided limited access (with only Commonwealth data) for testing purposes, and to allow data to be cleansed to protect legally assumed identities and those on witness protection. The testing has enabled the NSW Police Force to evaluate the privacy, security and accountability safeguards whilst developing robust, transparent and auditable systems that will ensure appropriate use, and protect the privacy of NSW citizens.

NSW will not upload NSW data until the Commonwealth Identity-matching Services Bill has passed Commonwealth parliament.

TAB B

PORTFOLIO COMMITTEE NO. 1 – PREMIER AND FINANCE

Inquiry into Cybersecurity

Inquiry hearing: 3 February 2021
Jubilee Room, Parliament House, Sydney

SUPPLEMENTARY QUESTIONS
WITH ANSWERS

(NSW Police Force)

1. Question

Were any firearm licence details accessed or released in the phishing attack on Service NSW?

a. How many firearm licence holders were affected?

b. Have all those affected been issued a new firearms licence?

Answer

Yes.

a) 69 firearm licence holders were affected.

b) Eleven (11) affected customers have requested a licence to be reissued. Communication with the customer was conducted by the Service NSW hypercare team.

2. Question

What safeguards are in place with the Firearms Registry's Firearms and Licensing Information Management System (FLIMS) to prevent the personal details of licensed firearm owners and firearms dealers from being inappropriately accessed?

Answer

Information supplied by an applicant is batched and deposited by Service NSW behind the NSW Police mainframe environment every 24 hours.

3. Question

From 5 June 2012 to 27 June 2017 licensed firearm owners in NSW were required to provide their name and home address every time they purchased ammunition. During this time tens of thousands of records of ammunition purchases included the home address of licensed firearm owners in dealer's ammunition record books. How does the NSW Police Force propose to securely manage these highly sensitive paper records?

Answer

Firearms dealers are required to gather information about firearm and ammunition transactions. The requirement to capture the address of licence holder exists for a firearm transaction. It is incumbent on firearms dealers to ensure appropriate security measures are in place for all records they hold.

4. Question

When will firearm dealers be able to undertake Interstate Acquisitions of firearms on the Sales Force platform, instead of having to use both the Registry's paper and electronic systems?

Answer

A roadmap of future works has been developed, which will see modules being built and launched in 2022. Recognising the business and regulatory benefits of digitising interstate acquisitions, this module has been prioritised. Some scoping work has already been commenced and significant focus will be afforded to this part of the build in the second quarter of 2021.