Submission
No 2

EXAMINATION OF AUDITOR-GENERAL'S PERFORMANCE AUDIT REPORTS FEBRUARY 2018 - JULY 2018

Organisation: Department of Customer Service

Date Received: 14 August 2019

NSW GOVERNMENT | Customer Service

McKell Building – 2-24 Rawson Place, Sydney NSW 2000
Tel 02 9372 8877 | Fax 02 9372 7070 | TTY 1300 301 181
ABN 81 913 830 179 | www.customerservice.nsw.gov.au

Our reference: BN-00340-2019
Your reference: D19/23590

Greg Piper
Chair
Legislative Assembly Public Accounts Committee
Parliament of NSW

By email: pac@parliament.nsw.gov.au

Dear Mr Piper

Auditor-General's performance audit report – *Detecting and responding to cyber security incidents*

Thank for your letter dated 3 July 2019 regarding a request to provide the Legislative Assembly Public Accounts Committee with the department's response to the Auditor General's report *Detecting and responding to cyber security incidents,* tabled on 2 March 2018.

Please find attached the completed template containing the Department of Customer Service's response to the audit recommendations.

The department found the audit report useful in identifying areas of priority for uplifting cyber security across NSW Government. The recommendations informed several aspects of the whole-of-government *NSW Cyber Security Strategy*. The area responsible for actioning the recommendations is 'Cyber Security NSW'. Cyber Security NSW provides leadership and coordination to uplift whole-of-government cyber security capability and awareness, and to assist effective decision-making across the NSW cyber security ecosystem.

If you would like more information, please contact [redacted]

Yours sincerely

Glenn King, Secretary

Date: 14 August 2019

ATTACHMENT TO LETTER – IMPLEMENTATION OF RECOMMENDATIONS

Department of Customer Service

Detecting and responding to cyber security incidents

RECOMMENDATION NUMBER	RECOMMENDATION	ACCEPTED OR REJECTED	ACTIONS TO BE TAKEN	DUE DATE	STATUS (completed, on track, delayed) and COMMENT	AREA RESPONSIBLE
2018/01	DFSI should develop whole-of-government procedures, protocol and supporting systems to effectively share reported threats and respond to cyber security incidents impacting multiple agencies, including post-incident reviews and communicating lessons learnt	Accepted	1. Cyber Security NSW has established information sharing procedures and protocols.	1. Commenced 18/19 financial year. To be completed 19/20 financial year and updated as required.	1. On track.	Cyber Security NSW
			2. Post-incident review practices implemented including lessons learned workshops and reports.	2. Commenced 18/19 financial year. To be completed 19/20 financial year and updated as required.	2. On track.	
			3. Incident notification form developed for clear and consistent reporting.	3. Completed 17/18 financial year. Reviewed 18/19 financial year.	3. Completed.	
			4. Mandatory requirement 2.5 of the Cyber Security Policy requires that agencies share information on security threats and intelligence with Cyber Security NSW and cooperate across NSW Government to enable management of government wide cyber risk.	4. Completed 18/19 financial year.	4. Completed.	
			5. Cyber Security NSW will be establishing an inter-agency information sharing portal and protocol to ensure timely and secure dissemination and receipt of threat intelligence.	5. Commenced 18/19 financial year. Procurement in progress. To be completed 19/20 financial year.	5. On track.	
2018/02	DFSI should assist agencies to improve their detection and response by providing:					
2018/02.1	better practice guidelines for incident detection, response and reporting to help agencies develop their own practices and procedures	Accepted	1. Threat intelligence information is shared across NSW Government.	1. Completed 18/19 financial year and now business-as-usual.	1. Completed.	Cyber Security NSW
			2. A program of exercises in 2018 developed the first NSW Government Cyber Security Sub Plan. This is a Sub Plan to the NSW Emergency Response Plan. The plan was endorsed by the State Emergency Management Committee (SEMC) in December 2018.	2. Commenced 17/18 financial year and will be ongoing. Initial incident response plan completed 18/19 financial year.	2. Completed. Sub Plan completed 18/19 financial year. Four exercises completed and exercise program will be ongoing.	
			3. The program of exercises also developed a draft incident response plan which is currently being	3. Commenced 18/19 financial year for implementation 19/20 financial year.	3. On track.	

RECOMMENDATION NUMBER	RECOMMENDATION	ACCEPTED OR REJECTED	ACTIONS TO BE TAKEN	DUE DATE	STATUS (completed, on track, delayed) and COMMENT	AREA RESPONSIBLE
			reviewed. To be completed end August 2019.			
2018/02.2	training and awareness programs, including tailored programs for a range of audiences such as cyber professionals, finance staff, and audit and risk committees	Accepted	1. Mandatory requirement 2 of the Cyber Security Policy requires that agencies must build and support a cyber security culture across their agency and NSW government more broadly. Agencies must implement regular cyber security education for all employees, contractors and outsourced service provide the Cyber Security Policy requires agencies and departments across NSW Government to have cyber security awareness programs in plans. 2. Awareness information sheets are produced by Cyber Security NSW including 'top 10 tips', 'questions Board and risk committees should ask about cyber security' and 'navigating cyber security for CEOs and Secretaries'. 3. Cyber Security NSW is piloting a cyber security risk awareness programs for executives with 75 executives to be trained by September 2019. 4. Access to a technical skills training portal has been provided for cyber security personnel within NSW Government to uplift their capabilities. This provides personnel with the ability to practice and refine their skills in preparation for new accreditations. 5. Cyber Security NSW regularly presents at meetings, forums and committees to uplift cyber security across NSW Government. This includes audit and risk committees, communities of practices, Joint Cyber Security Centre events, conferences, and staff meetings and leadership meetings across departments and agencies.	1. Commenced 17/18 and will be ongoing. 2. Completed 18/19 financial year – production of updated awareness information sheets will become business-as-usual. 3. Commenced 19/20 financial year. To be completed end September 2019. 4. Commenced 19/20 financial year. The portal will be reviewed by 30 June 2020. 5. Commenced 17/18 financial year. This is now business-as-usual.	1. On track, progress to be assessed post-attestation due on 31 August 2019. 2. Completed. 3. On track. 4. On track. 5. Completed – now business-as-usual.	Cyber Security NSW
2018/02.3	role requirements and responsibilities for cyber security across government, relevant to the size and complexity of each agency	Accepted	1. Section 2 of the Cyber Security Policy outlines the role requirements and responsibilities for cyber security across government and Mandatory Requirement 1.1 enforces this.	1. Completed 18/19 and incorporated into Cyber Security Policy which came into effect on 1 February 2019.	1. Completed.	Cyber Security NSW

RECOMMENDATION NUMBER	RECOMMENDATION	ACCEPTED OR REJECTED	ACTIONS TO BE TAKEN	DUE DATE	STATUS completed, on track, delayed and COMMENT	AREA RESPONSIBLE
			2. A Director-level position description for cyber security responsible officer (or Chief Information Security Officer equivalent) was distributed to members of the ICT and Digital Leadership Group (consisting of the Chief Information Officers from all NSW Government clusters). 3. Principles to attract, retain and retrain staff in cyber security roles is being prepared by NSW Government through 'skills pathway principles'. This includes the development of standard capabilities for cyber security roles.	2. Completed 17/18 financial year. 3. Commenced 18/19 financial year. To be completed 19/20 financial year.	2. Completed. 3. On track.	
2018/02.4	a support model for agencies that have limited detection and response capabilities	Accepted	1. Proposal for vulnerability management service to be developed.	1. Commenced 19/20 financial year. To be considered 19/20 financial year.	1. On track.	Cyber Security NSW
2018/03	DFSI should revise the Digital Information Security Policy and Event Reporting Protocol by:					
2018/03.1	clarifying what security incidents must be reported to DFSI and when	Accepted	1. NSW Cyber Incident Response Plan clearly outlines and defines incidents and their reporting requirements. Incident notification form has been developed for clear and consistent reporting.	1. Completed 19/20 financial year.	1. Completed.	Cyber Security NSW
2018/03.2	extending mandatory reporting requirements to those NSW Government agencies not currently covered by the policy and protocol, including State owned corporations	Accepted in part	1. The Cyber Security Policy only extends to all agencies listed in schedule 1 of the *Government Sector Employment Act 2013*.	1. Completed for all NSW Government agencies 18/19 financial year.	1. Despite being outside the remit of Cyber Security NSW, State owned corporations, local councils and universities are encouraged to report.	Cyber Security NSW
2018/04	DFSI should develop a means for agencies to report incidents in a more effective manner, such as a secure online template, that allows for early warnings and standardised details of incidents and remedial advice	Accepted	1. Cyber Security NSW will be establishing an inter-agency information sharing portal and protocol to ensure timely and secure dissemination and receipt of threat intelligence.	1. Commenced 18/19 financial year. Procurement in progress. To be completed 19/20 financial year.	1. On track.	Cyber Security NSW
2018/05	DFSI should enhance NSW public sector threat intelligence gathering and sharing including formal links with Australian Government security agencies, other states and the private sector	Accepted	1. NSW Government is actively participating in and integrated in Commonwealth initiatives through active membership on the National Cyber Security Committee, National Cyber Security Operations Committee and the National Exercises Steering Committee. All committees consist of representatives from all state and territory cyber security functions and the Australian Cyber Security Centre.	1. Completed.	1. Completed. 2. On track.	Cyber Security NSW

RECOMMENDATION NUMBER	RECOMMENDATION	ACCEPTED OR REJECTED	ACTIONS TO BE TAKEN	DUE DATE	STATUS (completed, on track, delayed) and COMMENT	AREA RESPONSIBLE
			2. NSW cyber risk is in part mitigated through sharing of intelligence with the Australian Cyber Security Centre and contributing to the Cyber Incident Management Arrangements (CIMA) endorsed by the Council of Australian Governments in December 2018, and the accompanying operational arrangements under development. 3. Cyber Security NSW has regular representation at the Joint Cyber Security Centre. This representation has increased stakeholder engagement particularly with the Commonwealth and the private sector.	2. Completed 18/19 financial year and will be ongoing. 3. Completed.	3. Completed.	
2018/06	DFSI should direct agencies to include standard clauses in contracts requiring IT service providers to report all cyber security incidents within a reasonable timeframe	Accepted	1. Mandatory requirement 3.4 of the Cyber Security Policy requires that all agencies and departments ensure cyber security requirements are built into early stages of projects and the system development life cycle, including agile projects. 2. Cyber Security NSW has incorporated cyber security risk into the ICT Assurance Framework (ensuring secure-by-design).	1. Commenced 18/19 financial year and ongoing. 2. Completed 18/19 financial year.	1. On track. This is a requirement under the NSW Cyber Security Policy. 2. Completed.	Cyber Security NSW
2018/07	DFSI should provide assurance that agencies have appropriate incident reporting procedures by:					
2018/07.1	extending the attestation requirement within the Digital Information Security Policy to cover procedures and reporting	Accepted	1. The NSW Cyber Security Policy (which replaced the Digital Information Security Policy) requires reporting entities to provide a yearly report on their compliance (via a maturity reporting template). This attestation requires agencies to confirm they have a cyber incident response plan in place that is integrated with the security components of business continuity arrangements and has been tested over the previous 12 months. Mandatory Requirement Category 5 requires agencies to report against the requirements outlined in the policy and other cyber security measures.	1. Completed 18/19 financial year.	1. Completed.	Cyber Security NSW

RECOMMENDATION NUMBER	RECOMMENDATION	ACCEPTED OR REJECTED	ACTIONS TO BE TAKEN	DUE DATE	STATUS (completed, on track, delayed) and COMMENT	AREA RESPONSIBLE
2018/07.2	reviewing a sample of agencies' incident reporting procedures each year.	Accepted	1. Cyber Security NSW to review samples of small, medium and large agencies' incident reporting procedures.	1. To be completed 19/20 financial year.	1. Delayed. Cyber Security NSW will review a small sample 19/20 financial year.	Cyber Security NSW