NSW GOVERNMENT
The Honourable Victor Dominello MP
Minister for Customer Service

Our reference: MIN-00553-2021

Mr David Blunt
Clerk of the Parliaments
Parliament House
Macquarie Street
SYDNEY NSW 2000

Dear Mr Blunt

Please find attached the Government response to the report entitled *Cyber Security* by Portfolio Committee No. 1 – Premier and Finance for tabling in the Legislative Council.

The NSW Government's response is due to the Legislative Council on 26 September 2021. As this is a Sunday, you have advised the response may be provided on Monday 27 September 2021.

If you have any further queries, please contact Lauryn Bae Brokate, Executive Director, Office of the Secretary, Department of Customer Service on or at

Yours sincerely

Victor Dominello MP
Minister for Customer Service
Minister for Digital

Date: 24/09/21

Received at 12.45 pm
27 September 2021

GPO Box 5341 Sydney NSW 2001 ▪ P: (02) 8574 6607 ▪ F: (02) 9339 5526 ▪ W: nsw.gov.au/ministerdominello

Report 52 – Cyber security – Government Response

No	Recommendation	Government Response	Comment
1	That the NSW Government review the functions of Cyber Security NSW and provide it with a clearer mandate to oversee agencies' cyber security progress and ensure their compliance with the NSW Cyber Security Policy.	**Supported**	The NSW Government reviewed the functions of Cyber Security NSW, which is within the Department of Customer Service, in 2020. As a result of this review, a new Governance, Risk and Compliance function in the Policy, Awareness and Research Directorate in Cyber Security NSW was established to oversee agencies' cyber security progress and ensure compliance with the reporting obligations under the NSW Cyber Security Policy.
2	That the NSW Government move Cyber Security NSW from within the Department of Customer Service to the Department of Premier and Cabinet to provide it with more independence from service delivery agencies and increased visibility and authority.	**Not supported**	The Department of Customer Service is a central agency responsible for whole of government strategy, standards and agency accountability in relation to uplifting public sector Cyber Security. Locating Cyber Security NSW within the Department of Customer Service Digital.NSW division reflects the integrated role of cyber security in all elements of digital transformation and implementation across government, including whole of government digital policies and strategies. All clusters have identical obligations under the Cyber Security Policy. A change of cluster would not change the level of independence of Cyber Security NSW.
3	That the NSW Government review the responsibility and resourcing of the Privacy Commissioner so that the office can be more proactive in ensuring government services and systems are designed and delivered with stringent privacy protections.	**Supported in principle**	The *Privacy and Personal Information Protection Act 1998* prescribes the functions of the NSW Privacy Commissioner. These functions enable the Privacy Commissioner to be proactive. For instance, one of the Commissioner's functions is to promote the adoption of, and monitor compliance with, the information protection principles. The NSW Government acknowledges that privacy law cannot remain static and accordingly, has made a public commitment to introduce broad privacy reform. When developing privacy reforms, the NSW Government will consider this recommendation and work with the Privacy Commissioner to review the Commissioner's responsibilities and resourcing to ensure these continue to be appropriate.
4	That the NSW Government urgently address the matters identified in Finding 4 and	**Supported in principle**	The NSW Government has identified the need to establish an identity resilience service to provide a consistent,

No	Recommendation	Government Response	Comment
	implement a framework or clear process within government to properly and expeditiously deal with requests by people in the community for assistance in the event of a breach of their data.		customer-centric, proactive and "tell us once" service for customers regardless of the source of the compromise. A limited-scope pilot is under way to inform a business case for this service.
5	That the NSW Government work with industry and the education sector to develop a cyber security skills framework that includes: • the provision of a comprehensive and regularly reviewed cyber security training regime for all NSW Government employees • the requirement for cyber security professionals within NSW Government agencies to be accredited in recognised cyber security certifications • the provision of adequate tertiary cyber security qualifications to meet government and industry demand.	**Supported in principle**	The 2021 NSW Cyber Security Strategy, released in May 2021, provides for the development of a cyber security skills framework with several funded initiatives to deliver enhanced training, accreditations, certifications in high school and vocational institutes and a range of other enhanced skills development programs. In October 2020, a new directive was issued for NSW Government staff, *DCS-2020-05 Cyber Security NSW directive – Practice Requirements for NSW Government*. This Circular mandates compulsory annual cyber security training for all NSW public servants (including contractors). This requirement clarifies and builds-on the expectations of Mandatory Requirement 2.1 of the NSW Cyber Security Policy and is reflected in the 2021 version of the Policy. Agencies and departments are responsible for ensuring the delivery of training and compliance. NSW Government supports improving understanding of and access to appropriate accreditations as part of a skills framework. While there is insufficient clarity on the scope of accreditations or definition of relevant cyber security employees to commit to implementing a mandatory requirement for accreditation, the Department of Customer Service continues to work with stakeholders across the sector to ensure cyber security professionals have appropriate accreditations to fulfil the responsibilities of their specific roles. The Department of Customer Service recognises that there are many pathways to a career in cyber security as well as many different role options within this field. The Department of Customer Service further recognises the importance of ensuring that the skills of employees in cyber security roles adequately meet the requirements of the role. Work on the development of skills framework and tertiary qualifications is ongoing federally in close collaboration with

No	Recommendation	Government Response	Comment
			state and territory governments, including the NSW Government, and the outcome of this work will impact what role NSW Government will play moving forward.
6	That the NSW Government review its Cyber Security Policy to provide clarity around mandatory standards and set a benchmark that all NSW Government agencies must adhere to.	**Supported**	The Department of Customer Service reviewed the Cyber Security Policy for the FY2021 reporting year to provide clarity of several expectations laid out in *DCS-2020-05 Cyber Security NSW directive – Practice Requirements for NSW Government*. The Department of Customer Service will continue to review the policy for future reporting periods including minimum benchmarks and standards.
7	That the NSW Government work with industry to determine the most appropriate model for cyber security standards for both NSW Government agencies and cyber security businesses within New South Wales.	**Supported**	On 1 February 2021, NSW Government released a Recommendations Report from the NSW Cyber Security Standards Harmonisation Taskforce that will help strengthen NSW's cyber capabilities.
8	That the NSW Government investigate avenues for it to improve the security of Internet of Things devices, particularly those adopted or deployed by its agencies.	**Supported**	The NSW Government Internet of Things (IoT) policy includes cyber security requirements for use of Internet of Things devices. The IoT Policy and NSW Cyber Security Policy are reviewed as part of standard policy review cycles and the changing threat landscape and evolving requirements which may need to be addressed are considered as part of this. Cyber Security NSW will examine potential IoT related changes to the Cyber Security Policy for 2022 and beyond. The Department of Customer Service and NSW Government agencies work closely with their Federal and State equivalents on the ongoing implementation of IoT, including the security and safety of associated IoT devices and systems.
9	That the NSW Government urgently establish a mandatory data breach notification scheme applicable to all NSW Government agencies and its contracted service providers.	**Supported in principle**	The NSW Government has released an exposure bill, the *Privacy and Personal Information Protection Amendment Bill 2021* (the 'Bill'), which proposes to strengthen privacy protection in NSW, including by creating a Mandatory Notification of Data Breach (MNDB) Scheme. If passed through Parliament, the MNDB Scheme will commence 12 months after assent. This allows enough time for NSW public sector agencies and the Information and Privacy Commission to put in place a

No	Recommendation	Government Response	Comment
			range of mechanisms to ensure compliance. The Commonwealth Government is currently reviewing the *Privacy Act 1988* (Cth) and the NSW Government will engage with the Commonwealth on key issues, including the issue of NSW Government contracted service providers.
10	That the NSW Government develop a strategy to enhance sovereign cyber security capability which includes building the industry, establishing principles for procuring services onshore and working with agencies to identify what data should be stored offshore.	**Noted**	The NSW ICT Sovereign Procurement Taskforce will develop strategies and policies to diversify our ICT/digital partnership ecosystem. The NSW Cyber Security Strategy's objectives include increasing the NSW Government's cyber resiliency as well as helping NSW cyber security businesses grow and enhance cyber security skills and workforce. The Strategy includes $7.4 million of programs to implement these goals. The NSW Government Information Classification, Labelling and Handling Guidelines support NSW Government agencies to procure appropriate services.
11	That the NSW Government: • provide further financial support to local councils to enhance their cyber security capabilities • develop a plan in consultation with Local Government NSW to ensure local councils meet the cyber security standards identified for NSW Government agencies.	**Noted**	The Department of Customer Service is providing local councils with support across all functions, including incident response, cyber security maturity uplift, training and awareness, risk and audit. This support is part of a boost in funding to the Department of Customer Service over three years. Office of Local Government (OLG) is responding to NSW Audit Office audit recommendations regarding the cyber security maturity of local councils. The Department of Customer Service is working with OLG and local councils, supporting them as they implement the recommendations.
12	That the NSW Government develop a strategy to improve the cyber safety of citizens that includes: • education and awareness measures • consumer protection measures • advice and support services.	**Supported in principle**	The Australian Cyber Security Centre in the Commonwealth Government raises awareness and provides education to citizens in Australia. The education and awareness measures for citizens are led by the Commonwealth Government, through cyber.gov.au website/hub.-The NSW Government is working proactively with the Commonwealth Government on a co-branded awareness campaign to ensure a consistent approach nationally to avoid confusion and duplication. Ensuring the cyber safety of citizens with consumer protection measures is part of Australia's Cyber Security Strategy 2020 under the *Clarify cyber security obligations*

No	Recommendation	Government Response	Comment
			for Australian businesses initiative. NSW Government works closely and collaboratively with its Federal counterparts to provide feedback on the national approach. The nationally agreed approach is to utilise the cyber.gov.au website/hub as the primary source of truth for citizens and businesses seeking advice on cyber security issues. NSW citizens are directed to this service.