information and privacy commission
new south wales

Enquiries: [redacted]
Telephone: [redacted]
Our reference: IPC19/A000384

Australia's 2020 Cyber Security Strategy
Department of Home Affairs
cybersecuritystrategy@homeaffairs.gov.au

Dear Sir/Madam

Australia's 2020 Cyber Security Strategy

The purpose of this correspondence is to provide comments on the Australia's 2020 Cyber Security Strategy discussion paper released by the Department of Home Affairs on 5 September 2019.

The following comments are provided to assist the Department in its consideration of this issue.

The Information and Privacy Commission NSW (IPC) oversees the operation of privacy laws in New South Wales. The Privacy Commissioner has responsibility for overseeing and advising NSW public sector agencies on compliance with the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act). The PPIP Act and HRIP Act establish the Information Protection Principles and Health Privacy Principles which govern the collection, use and disclosure of personal and health information by NSW government agencies and, in the case of the HRIP Act, private sector health care providers.

A strong cyber security environment is an essential pre-condition to the building and maintenance of robust and privacy protective information governance systems. Section 12 of the PPIP Act specifically imposes an obligation on NSW public sector agencies to ensure that personal "information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse ..."

As governments move forward with the digital transformation agenda the importance of a sustained focus on cyber security and privacy protection cannot be underestimated. This includes fostering the growth of a skilled and capable cyber security workforce.

As demonstrated by the most recent data released by the Office of the Australian Information Commissioner (OAIC), 60 per cent of data breach notifications received by the OAIC between April 2018 and March 2019 were the result of malicious or criminal attacks. Of these, 68 per cent were attributed to incidents resulting from common cyber threats such as phishing, malware, ransomware, brute-force attacks, compromised or stolen credentials and other forms of hacking. The remaining 32 per cent were attributed to a malicious or criminal attack were the result of theft of paperwork or a data storage device, social engineering or impersonation, or an act of a rogue employee or insider threat.[1]

---

[1] Office of the Australian Information Commissioner, *Notifiable Data Breaches Scheme 12-Month Insights Report*, 2019, pp8-10.

Data breaches are a matter of significant concern to my office. While NSW does not currently operate a mandatory reporting scheme, I strongly encourage NSW public sector agencies to report data breaches under the current voluntary reporting scheme. The most recently quarterly data indicates there has been a steady rate of reported data breaches over the past 18 months. This data can be accessed on the IPC website.

The IPC has also provided public sector agencies with resources to assist them to manage and respond to a data breach incident. This includes a data breach guidance, notification forms and a prevention checklist.

The NSW Department of Communities and Justice has recently undertaken a consultation with public sector agencies on the development of a mandatory reporting scheme in NSW and is currently considering the submissions received.

As Privacy Commissioner, I encourage NSW public sector agencies to take a proactive 'privacy-by-design' approach to all digital programs and projects. Such an approach considers privacy and security requirements from the outset. Implementing preventative measures which remove or mitigate privacy and security risks is more effective to containing costs, managing community expectation and realising policy intent than developing legislative exceptions to privacy laws or redesigning programs or digital solutions after the fact.

Tools such as Privacy Impact Assessments (PIAs) are valuable in assisting public and private organisations in managing privacy and security risks. A PIA is a systematic assessment of a project which identifies the impact that the project may have on the privacy of individuals and sets out a process or recommendations in addressing this risk. PIAs are more than a 'compliance check' against privacy legislation. Critically, PIAs allow data custodians to gain an insight into information flows within their organisation, demonstrate corporate responsibility and provide the community with the confidence that a proposed project accords with community expectations towards privacy, data security and appropriate information management.

Data sharing is another area where appropriate cyber security is a significant factor in ensuring that agencies are compliant with their privacy obligations. As agencies continue to share ever increasing quantities of personal and non-personal data with other government agencies and non-government organisations, ensuring that these partners have in place commensurate levels of cyber security protections will be vital.

The IPC is currently developing guidance for NSW public sector agencies on safe and privacy respectful data sharing, including advice on the need to ensure that the receiving agency has appropriate levels of security to safeguard any data provided.

I hope these comments will be of assistance to you. Please do not hesitate to contact me if you have any queries. Alternatively, your officers may contact [redacted] Senior Project Officer, Legal Counsel and Regulatory Advice, on [redacted] or by email at [redacted]

Yours sincerely

[redacted]

Samantha Gavel
NSW Privacy Commissioner

[redacted]