Enquiries: Siobhan Jenner
Tel: (02) 8019 1603
Our ref: A11/0362

Mr Michael Coutts-Trotter
Director General
Finance & Services
McKell Building
2-24 Rawson Place
SYDNEY NSW 2000

Dear Mr Coutts-Trotter

Thank you for your undated letter to this Office addressed to Dr Elizabeth Coombs regarding the News South Wales Government Information and Communication Technology (ICT) strategy, which was received by this Office on 12 September 2011. Dr Coombs will not commence her appointment until 7 November 2011. The following advice is provided in accordance with my powers under sections 36()(a),(d),(g) and (j) of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act).

I note your advice that the proposed ICT strategy is part of a response to the NSW Auditor General's audit report *Electronic Information Security* (the EIS report). I share the Auditor General's concerns about the lack of consistent implementation of electronic information security policies across the NSW public sector (as required by the Premier's Memorandum M2007-04 Security of Electronic Information), particularly as the EIS report specifically identifies risks to sensitive personal information, not just government data[1]. I have therefore couched the following advice in terms of the obligations imposed upon NSW public sector agencies by the PPIP Act (while canvassing best privacy practice for an ICT) rather than addressing the Discussion Paper (DP) questions directly, as in my view, privacy legislation and best practice privacy protection should form the cornerstone of a sound ICT strategy. In addition this approach is likely to be of benefit in relation to the stated aim in the DP that an electronic security policy should canvass other matters such as 'service delivery, the storage and exchange of information within Government' and 'transactions between Government and the community'.

Privacy and Personal Information Protection Act 1998

As you know the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) requires that NSW public sector agencies comply with twelve Information Protection Principles (IPPs) in their dealings with personal information. One key issue in developing an ICT policy, particularly a policy which governs transactions between individuals and Government is whether the information at issue is or is likely to be personal information. The definition of 'personal information' in the PPIP Act is:

[1] In this regard I note that in 2009 this Office was advised by the Department of Commerce that the Jobs NSW website had been 'accessed by unknown persons who obtained email addresses of registered users' after which some Jobs NSW clients received SPAM emails.

> information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion[2].

In my experience, while agencies have little difficulty recognising personal information where the identity of an individual is apparent, they sometimes have greater difficulty in recognising personal information where the identity of an individual 'can be reasonably ascertained' from information or an opinion. In my view agencies should adopt a risk management approach (which is discussed below in the context of Privacy Impact Assessments); ensuring that the information they collect, hold use and disclose is potentially personal information and treat it as subject to the IPPs in the PPIP Act.

Once agencies have formed the view that their ICT systems hold (or potentially hold) personal (and/or health) information they are required to protect that information. In this regard section 12 (IPP 5) provides that agencies must ensure:

> …
>
> (a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and
>
> (b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and
>
> (c) **that the 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**, [emphasis added] and
>
> (d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.[3]

In order to satisfy the requirement in subsection (c), agencies should have undertaken an assessment or possibly a Privacy Impact Assessment (PIA) (discussed below) to determine their holdings of, and transactions with personal (and health) information particularly where that information is electronic information or which might be digitised in future. Agencies should review and tailor their security policies to ensure that the information is protected (to the standards required by Premier's Memorandum M2007-04 Security of Electronic Information and with relevant NSW Government ICT policies) to protect it against loss, unauthorised access, use, modification, disclosure and all other misuse. It is possible that agencies may need to go beyond the security standards in commercial or government standards, particularly where there is a high volume of transactions outside the agency and/or the information is particularly sensitive, such as health information. These protections should be articulated in agencies' ICT policies and procedures and should not only include technical requirements but should articulate the means by which employees will be trained in implementing the technical requirements and the

[2] Section 4 of the PPIP Act.
[3] The *Health Records and Information Privacy Act 2002* (HRIP Act) contains a similar requirement in relation to health information – see Health Privacy Principle 5).

policies underpinning the technical requirements. ICT policies and procedures should form part of the agency's Privacy Management Plan which describes how it will comply with the IPPs[4].

Privacy Impact Assessments

In my view Government sector-wide projects such as ICT policies which involve the collection, storage, access to, use or disclosure of personal (and possibly health) information should be preceded by a Privacy Impact Assessment (PIA). A PIA is an assessment of real or perceived potential impacts of the project or legislation upon an individual. The PIA process is similar to a risk assessment but it should map existing and proposed personal (and health) information flows[5]. A PIA can form part of an ICT risk assessment or policy or it can operate in tandem with ICT assessments or policies. Once information flows have been mapped a PIA should identify the potential risks to the security of that information. The PIA should review the sensitivity of the information and identify whether increased heightened security controls are required (such as encryption). The PIA should also assess the likelihood of a security breach, identify possible IT countermeasures and indicate whether affected individuals should be notified. The PIA should identify staff training needs regarding the legal requirements not only in relation to personal and health information but in relation to record keeping, good administrative practice and corruption prevention. The PIA should reference the ICT business rules relating to the collection, storage, use and disclosure of personal and health information and should identify clear audit mechanisms which identify data viewing as well as data transactions. The PIA should include contingency plans in place to identify security breaches or improper disclosure and include breach notification procedures to enable affected individuals to take remedial action[6].

Future-proofing security arrangements

I note that the Auditor General's Report, Electronic Information Security, (Volume One) issued in 2011 reports that its audits in that year of two agencies which were certified to ISO27001 'showed no major security flaws'[7], however the audit found that there were some weaknesses in the electronic information security, such as database applications not being secured in web applications, failures to terminate remote access sessions and to encrypt transmission between data systems and remote applications. This is evidence that compliance with an ICT standard will not always be sufficient protection against risk.

---

[4] As required under section 33 of the PPIP Act. That provision also requires agencies to describe how they will comply with the Health Privacy Principles in the *Health Records and Information Privacy Act 2002* (HRIP Act).

[5] A PIA should generally start with the question: 'Does the individual need to be identified at all?' In this regard the HRIP Act recognises that where it is lawful and practicable organisations should enable individuals to transact or receive health services anonymously. (HPP 13)

[6] For more detailed guidance about conducting a PIA see the website of the Australian Information Commissioner http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html)or the Privacy Victoria website: http://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessments-guide

[7] At page 74.

The EIS report noted that 'the level and sophistication of external threats is increasing[8]' which means that the methods by which personal information may have been considered sufficiently secure at the time of the commencement of the PPIP Act would be likely to be considered wanting today. As noted above it is expected that agencies will implement and comply with an ICT standard as a first step to the protection of ICT data. As noted on page 3 of the DP, it is possible that agencies might need to go beyond a data security standard and consider whether they require bespoke security protections for personal information. I note that this is canvassed in the DP in the discussion about a 'prescribed approach' which may need to include particular security guidance in some cases enforceable rules relating to:

- Limits and security protocols for wireless communications
- Asset disposal, particularly the sale of computers
- Disclosures of personal and health information outside NSW
- The use of cloud computing
- The use of contractors
- The posting of information which could identify an individual on the world wide web or on intranet systems
- Inventory and security of portable storage devices
- Encryption of sensitive information in email, portable storage devices and telephone messaging
- IT security systems such as firewalling and systems to detect, prevent and defeat malware, botnets, sniffing and phishing.

If required my Office is able to provide further assistance and advice in developing the NSW ICT strategy. If you have any queries regarding this advice please contact Ms Jenner of this Office on the above number.

Thank you again for the opportunity to make submissions and I trust my comments will be of assistance in developing the New South Wales Government ICT strategy.

Yours sincerely

John McAteer
Acting Privacy Commissioner
Information and Privacy Commission

[8] EIS report at page 14.