Submission: Joint Committee of Public Accounts and Audit

Re: Cybersecurity Compliance - Inquiry into Auditor-General's report 42 (2016-17) (the "2016 ANAO Report")

1. The findings of the 2016 ANAO report are disturbing on a range of levels. First as follow up on its report in June 2014, ANAO Audit Report No. 50 2013–14, *Cyber Attacks: Securing Agencies' ICT Systems* (the "2014 ANAO Report") it found continuing non compliance by the Australian Taxation Office (the "ATO") and the Department of Immigration and Border Protection ("DIBP") to fundamental problems with its cyber security protocols, procedures and practices. Secondly, the potential of a catastrophic damage arising out of a data breach involving material held by the ATO and DIBP means that the failures identified by the ANAO is a failure of both public policy and administration by both agencies.

2. As the report makes clear the ATO and the DIBP collect, store and use data, including national security data and personally identifiable information that can be used to identify, contact, or locate an individual such as date of birth, bank account details, driver's licence number, tax file number and biometric data. There is a very significant responsibility to properly secure the personal information. It should be noted that the provision of that data is generally under compulsion. That is not to say that there is resistance *per se* to the provision of that personal information or no legitimate basis for that collection. It does however highlight the fundamental need for the agencies to comply with cyber security standards. They are failing to do so.

Cultural issues highlighted in the 2016 ANAO Report

3. The ANAO made it clear that it measured the performance of the agencies against particular benchmarks, that Top Four mitigation strategies in the *Australian Government Information Security Manual*[1] and evidence of cyber resilience being described as:

> " establishing a sound ICT general controls framework[5] and effectively implementing the Top Four mitigation strategies."

4. It should be noted that cyber resilience is the beginning not the end of properly compliance with an agencies obligations. The agencies must comply with the Australian Privacy Principles under the Privacy Act 1988. It is clear from this report that neither the ATO or the DIBP are doing so. The Privacy Commissioner should investigate and require them to enter into enforceable undertakings.

5. The underlying context in the 2016 ANAO report is that the review is undertaken with reference to action taken since the 2014 ANAO report. The JCPAA published its report in March 2015 and recommended that the seven entities achieve full compliance with the Top Four mitigation strategies as soon as possible. This was followed up by the Committee recommending, in March 2015, a follow-up audit, as well as undertaking regular audits of Commonwealth entities' compliance with the Top Four mitigation strategies. Even with this ample warning the ATO and DIBP was found seriously wanting. Although they say different in their response to the 2016 ANAO Report the inference that can be drawn from their actions is that these agencies do not place a high enough priority on cyber security and, more importantly, see little real consequence in maintaining the appropriate standards. That is a concern. Where there is no incentive to comply an organisation will likely not comply to the full extent, even with the best intentions.

6. The methodology adopted by the ANAO was entirely appropriate but it is however only a starting point for a proper review of cyber security. It does not highlight what is clearly a bigger problem within the ATO and DIBP, their culture. There is a cultural problem in those agencies when dealing with privacy in general and cyber security in particular. Not only did those agencies

[1] Paragraphs 6 & 7 of the 2016 Report

not address the problems identified at least 18 months previously but what they did was last minute and incomplete.

7. The poor culture is evidenced by:

(a) the DIBP having an application whitelisting strategy but then deviating from it[2];

(b) the ATO developing an application whitelisting strategy "..during the course of this audit."[3] This is an almost undergraduate response to a significant problem. For the ATO to only address a mandatory obligation involving cyber security when the auditors are in the building is dangerously irresponsible. That bespeaks a lack of seriousness to one of its fundamental, if somewhat tedious and technical, obligations. It also demonstrates that cyber security is not ingrained into the culture of the agency. In that environment there is always something else to do;

(c) neither the DIBP or the ATO meeting their obligations in ensuring that service provider contract arrangements did not align with the Top Four mitigation strategies. That is not a matter of inability to do so but poor prioratising;

(d) both the ATO and the DI Border Protection did not effectively use their internal assurance processes to validate service provider's performance self-assessments. This is a recipe for disaster. Service providers, with poor privacy and cyber security practices, are notorious for being portals for hackers;

(e) both the ATO and the DIBP had insufficient protection against cyber attacks from external sources. That is a fundamental flaw. Given that data held by agencies are high value targets by overseas governments that is a major cause for concern. In 2015 the US Governments Office of Personnel Management was hacked and the personal information of 21.5 million people were stolen[4]. The investigation pointed to an overseas power being involved. Such data is not only valuable to steal identities

[2] Ibid at paragraph 12
[3] Ibid at paragraph 12
[4] ABC News Report US government data breach: 21.5 million job seekers' social security numbers taken by hackers http://www.abc.net.au/news/2015-07-10/social-security-numbers-taken-in-us-government-data-breach/6609082

for profit but provides security services valuable information in compromising individuals as well as, through data matching, uncovering operatives working under aliases. For those in the witness protection, involved in covert operations or generally requiring some anonymity this is a significant issue;

(f) the specific instances of shortcomings,[5] being application whitelisting controls not covering all desktops and servers, systems excluded from regular security patching or security patches being delayed and outside recommended timeframes outdated software on desktops are all basic mistakes which highlight a lack of system and control over the use of equipment; and

(g) poor management of privileged access is a critical problem because it can subvert all the good work that can be done through technical processes and up to date software protection. It is the human element that is often the more vulnerable part of any cyber security operation. The misuse of privileged access increases over time where privacy and cyber security is not given a high priority. While the described policies and procedures[6] adopted by the agencies were reasonable, as far as they went, that means very little in practice if the will to enforce those practices and procedures are not present. And the will comes from a viable security culture. In my experience where the cyber security culture is poor privileged access is used as a short cut to "get things done." The short cut becomes the *de facto* policy. Often times poor culture gives rise to an attitude that a privileged access processes hinder rather than help and are for show. With that mindset it is quite easy to ignore the processes.

8. The ANAO's finding[7] that:

> " The ANAO has assessed a total of 11 entities and found that only three entities were compliant with the Top Four mitigation strategies."

is damning but not particularly surprising. It is probably better than would be expected in the private sector, where the standards are generally poor and often times totally inadequate. The reason for this poor rate of compliance is that there are few consequences for a failure to meet the appropriate standards. The

[5] 2016 ANAO Report at paragraph 2.5
[6] 2016 ANAO Report at paragraph 2.20
[7] Ibid at paragraph 3.18

risk of enforcement action is slim. The consequences in the event of any action being taken negligible when compared to the quite severe penalties for similar breaches in the United Kingdom or even in the United States, where there Federal Trade Commission has proven to be a very tough and effective regulator where it has the jurisdiction to act.

9. The ANAO is correct in posing the question as to whether the entities are prioritizing cyber resilience. The answer must be no. The ANAO's conclusion[8] that:

> " To progress towards cyber resilience entities need to improve their governance arrangements and prioritise cybersecurity."

is accurate. There is, however, no real incentive to do so. It requires time, effort and probably more money. It certainly requires a change in cultural outlook. With a (always) limited budget and a constantly demanding schedule there are always different projects to put time, effort and money into when it is well understood in the cyber security community and amongst lawyers that the Privacy Commissioner is prone to talk, but only occasion, more than act, hardly at all. There is often the view that because there has not been a data breach the current state of play is adequate. There is also a reluctance to change the way things have been done in the past. Privacy protocols and procedures are often seen as more work that adds to an already busy schedule.

Action required

10. While cybersecurity has been announced as a is a strategic priority for the Australian Government and various initiatives have been taken there remains a fundamental lack of follow through in the form of adequate legislation and, more importantly, regulation and enforcement of what legislation there is[9]. The public policy problem that has developed is that Governments over the last 30 years have established the bare minimum regulatory framework, primarily the *Privacy* Act 1988.

11. The Privacy Commissioner has been, in the main, a timid regulator. Sometimes this has been because the office is poorly resourced. But the problem runs

[8] 2016 ANAO Report at paragraph 3.23
[9] 2016 ANAO Report at paragraph 19

deeper. The office has always been a tentative regulator, even when funding has been reasonable. It has erroneously focused on education over enforcement to an extreme degree. Educate till you nauseate seems to be the office mantra. It is necessary to do both. The Australian Securities and Investment Commission in the area of Corporate Governance and the Australian Competition and Consumer Commission in the area of consumer protection have shown that a combination of education and enforcement is necessary to properly regulate. The enforcement should be public and on occasion high profile so that those who are non-compliant will have an incentive to change their ways. The Privacy Commissioner has had the powers of injunctive relief since the *Privacy* Act was enacted in 1988. This provision has been used once. That is not because Australian businesses and government are conscientious in the privacy field.

12. Since 2014 the Privacy Commissioner has had the power to bring civil penalty proceedings. He had not done so. The terms of the enforceable undertakings he has entered into have been weak by international standards and almost invariably entered into by self-reporting by a party which has suffered a data breach. The awards made under determinations have been risible and provide no deterrence to malefactors.

13. Without adequate and prompt enforcement the privacy and cyber security culture will remain poor. The consequences of such a poor culture will grow with time as more government activities are conducted on line and the internet of things becomes ubiquitous. Poor cyber security practices by agencies but also third party contractors who do work with or for the agencies will continue to pose a real and present threat to the personal information of Australian citizens and potentially effect the operation of Government.

14. Until the Privacy Commissioner is properly resourced but also staffed by those officers who are more serious about enforcing the legislation there will remain a poor cyber security culture and a culture of impunity.

15. It is also important for agencies to review their operations and implement Privacy By Design in their systems. Privacy By Design ("PbD") should be a core policy to underpin information and privacy management in the Public Sector. PbD is a methodology that enables privacy to be "built in" to the

design and architecture of information systems, business processes and networked infrastructure. It aims to ensure that privacy is considered before, at the start of and throughout the development and implementation of initiatives that involve the collection and handling of personal information. It involves a level of intentionality regarding privacy management that marks a genuine departure from common place ad hoc approaches to privacy.

16. PbD is a set of seven principles that the Information and Privacy Commissioner of Ontario, Canada, developed during the 1990s, which became a globally recognised framework for the protection of privacy. Through it privacy is embedded into the design specifications of information technologies, organizational practices, and networked system architectures.[10]

17. The seven principles of PbD:

    1. **Proactive not Reactive**: The PbD approach attempts to anticipate and prevent privacy-invasive events before they happen.
    2. **Privacy as the Default Setting:** Ensuring that personal information is automatically protected in any given IT system or business practice, so that if an individual does nothing, their privacy still remains intact.
    3. **Privacy Embedded into Design:** Privacy should be embedded into the design and architecture of IT systems and business practices that are related to information handling.
    4. **Full Functionality – Positive-Sum, not Zero-Sum:** PbD seeks to accommodate all legitimate interests and objectives in a "win-win" manner, balancing seemly opposing interests, such as security, privacy and the objectives for service delivery.
    5. **End-to-End Security – Full Lifecycle Protection:** PbD extends throughout the entire lifecycle and all aspects of the information involved from start to finish.
    6. **Visibility and Transparency:** seeks to assure all stakeholders that component parts and operations remain visible and transparent, to users and providers alike.
    7. **Respect for User Privacy – Keep it User-Centric:** Above all, it puts the interests of the individual at the forefront by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

18. If adopted at beginning of any proposal or development involving the collection, storage and use of personal information Pbd is a benefit as it ensures that privacy and cyber security risks are dealt with from the outset rather than remediated at the end of the process. By adopting PbD methodology personal information is respected and the agencies will be automatically compliant with

[10] https://www.ipc.on.ca/privacy/protecting-personal-information/privacy-by-design/

privacy laws and their cyber security obligations. As PbD becomes woven into the everyday organizational practices it becomes business as usual.

19. The agencies should also use controls and tools, such as a privacy impact assessment (PIA) to support a formal risk analysis. Risk is always present in cyber security operations. It can seldom be entirely eliminated regardless of which controls are employed. As some type and degree of risk is likely to remain privacy risk assessment must be a continuous process rather than a one off event.

20. Similarly with technology and system development, cyber security and privacy needs to be included in the non-functional requirements of system design. Unfortunately for most systems cyber security and privacy is seen as ancillary to the primary purpose of the system and is usually included only grudgingly for compliance purposes. That is both erroneous and short sighted. The inclusion of privacy protections facilitates core objectives to ensure personal information is being handled appropriately, it is being used for the purpose for which it was collected, accessed by authorised personnel only, it is protected from unauthorised disclosure, loss or destruction and it is securely retained.

21. It is important to review the governance structures covering the full life cycle of personal information from collection through to use, disclosure, protection and disposal; a secure information lifecycle management.

I am happy to expand upon the above at your convenience.

Peter A Clarke
Barrrister at Law
[redacted]