UNCLASSIFIED

Australian Government

Department of the Prime Minister and Cabinet

ANDREW FISHER BUILDING
ONE NATIONAL CIRCUIT
BARTON

Senator Dean Smith
Chair
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Via email to jcpaa@aph.gov.au

Dear Senator Smith,

Thank you for your email dated 6 April 2017 to Dr Martin Parkinson, Secretary of the Department of the Prime Minister and Cabinet inviting a submission to the inquiry into **Cybersecurity Compliance, based on Auditor-General's report No. 42 of (2016-17): *Cybersecurity Follow-up Audit.*** I have been asked to reply on the Secretary's behalf.

I would like to thank the committee for the opportunity to provide a submission. I would also like to recognise the genuine significance of this inquiry being held to discuss cyber security. This is the second time in just a few short weeks I have been given the opportunity to address this matter before a parliamentary committee. This demonstrates not only the level of leadership being shown by our representatives in Parliament, but also the shift in environment that has occurred, with matters of cyber security now being placed at the forefront of our minds.

Audits, such as those conducted by the Australian National Audit Office (ANAO), provide us with a level of insight into how our government held information is being protected. However, in much the same way as businesses can audit their accounts to ensure their financial position is accurate and there has been no foul play, these audits do not ensure a business is investing money in a way that will turn a profit for their investors. For

government departments, enhancing trust and confidence in the confidentiality, integrity and availability of networks and data is necessary to help Australia embrace the opportunities of the digital economy and drive economic growth. But we need to ensure we are doing so in a way that will deliver the metaphorical profit for our investors – truly protecting them to the best of our abilities from cyber security breaches.

The Department of Human Services (DHS), the Australian Taxation Office (ATO) and Department of Immigration and Border Protection (DIBP) have vast amounts of information stored within their ICT systems and significant opportunities for improving and protecting their services. Audits, compulsory mitigation strategies and parliamentary inquiries are ways the government increases protection, however; simply enforcing compliance without looking beyond this does not ensure security.

Threats

We are aware that Australian and overseas organisations, across both the public and private sectors, have been compromised both criminal and state-sponsored actors. A substantial amount of sensitive commercial and personal information has been lost and significant damage has been incurred to businesses, governments and reputations.

The Australian Cyber Security Centre's[i] (ASCS) Threat Report 2016[ii] advises that Australian government networks are regularly targeted by the full breadth of cyber adversaries, from foreign states through to criminals and issue-motivated groups. Similarly, the 2016 Australian Cyber Security Centre Survey released in April 2017 revealed that Australian critical infrastructure organisations are being targeted by cyber criminals up to hundreds of times each day.

Responding to the threats

In his foreword to the 2017 update to Australia's Cyber Security Strategy the Prime Minister, the Hon Malcolm Turnbull MP said,

> Success is not just ticking off the Strategy's initiatives, *but changing culture* [emphasis added]. Enhancing trust and confidence in the confidentiality, integrity and availability of networks and data will help us derive even greater economic value from information-driven change.[iii]

In a digital age where threats are diverse and agile, we must be at least as adaptable and nimble. A valuable part of our security framework is implementing what was the Top Four mitigation strategies, and is now the Essential Eight recommended by the ASD. **However, this must be only part of the approach.** Compliance alone does not equal security and in fact, relying on it may put us at greater risk.

Audits, such as ANAO's provide us with an important snapshot of where our agencies stand, but they do not provide the full picture. In my role as Special Adviser to the Prime Minister I have found that there is a prevailing "tick box" compliance culture which is in some respects, perversely, driven by a fear of audit failure. By looking only to these snapshots, we may create a culture of fear and thereby harm our security. That is, agencies will consider themselves safe from compromise if they have their internal ICT area and their subcontractors put in place, and uncritically follow, prescribed security procedures, such as IRAP assessments.

This would be similar to a person assuming they will never experience poor health if they follow the guidance of government's public health initiatives. We can reduce our risks of developing cancer, heart disease, stroke or diabetes if we follow certain compliance measures, for example, avoiding cigarettes, exercising regularly, eating a healthy diet or reducing our sun exposure. But following these measures, ticking those boxes, doesn't eliminate the risk of developing one of these diseases entirely, as there are elements we cannot control or mitigate with just these measures. For example, you may decide not to smoke, under the belief that this will reduce your risk of developing lung cancer, but if you then move from a clean air environment to a polluted environment, a purely compliance based mindset may mean you fail to consider wearing a mask. In addition, some people have different risk factors and an individual may need to implement other measures beyond those recommended.

Thinking we can eliminate the risk of cyber compromise through following only measures of compliance, means we are missing the bigger picture. It means we are failing to understand the value of data, the changing risks from evolving threats or the peculiarities of unique ICT systems. With the cyber security landscape shifting rapidly and continuing to grow as a business risk for all our agencies, we need to ensure that our historical reliance on compliance does not prevent the necessary change that is needed to keep up with our environment. What we really need to create is an enhanced security *culture*.

By doing so we encourage agencies to adapt to the changing environment and educate their staff on **good cyber hygiene**. My vision is that of a strong cyber security culture that permeates all agencies, so that they habitually test their systems and arrangements to prevent complacency and enhance innovative solutions. This would sit alongside compliance measures, audits and alternative security options that may be more appropriate or effective for a given agency. Such an approach will significantly reduce risks to our systems and increase our cyber resilience. But I should note that we can never eliminate all of the risk.

So what does cyber security resilience look like?

The ACSC gives valuable guidance on what decision-makers, their advisers (and indeed Parliamentary Committees), should look for in judging an organisation's cyber resilience. That is, an organisation's ability to prepare for, withstand and recover from cyber incidents. The ACSC's advice, with which I agree, is that resilience is a whole-of-business concern, and that an organisation's ability to deal with a cyber incident is reliant on a variety of factors — not just technical controls.

The ACSC advises that more cyber-resilient organisations:

- Maintain good situational awareness by regularly seeking external information, advice or guidance on cyber security;
- Approach cyber security from a risk-reduction rather than compliance mindset, considering information security alongside other business risks;
- Have a strong security culture across the whole organisation and understand that everyone shares responsibility for cyber security, not just the IT department;
- Discuss cyber security at board level and with senior management, with regular updates on the agenda;
- Proactively identify and head off threats before they are successful; and
- Share information with trusted networks and alert other organisations to possible breaches of their own security.[iv]

We should look for all government organisations to carry out these measures as a matter of routine. This would represent the cultural change in cyber security that the government wants to see take place across government and the private sector.

There is an enormous amount of positive momentum across the community to build good cyber security resilience. In the wake of the Census review, my Office has seen agencies contact us directly to further understand how they should approach and address cyber security risk. We have also seen the conversation more broadly in government evolve quickly and significantly. At a strategic level the government established the Digital Transformation Agency with a key focus of ensuring cyber security is built into the development of government services. These are key examples of the shift in culture we are beginning to see. We need to harness this momentum to ensure we are actively responding to evolving threats, not resting on our laurels.

As Minister Tehan, the Minister Assisting the Prime Minister for Cyber Security said in his November 2016 letter to Ministerial colleagues on the importance of cyber security,

> The Prime Minister committed the Government to show leadership in addressing cyber security and, as part of this leadership, government departments and agencies must have strong cyber security practices.

It is up to both this committee and our agencies to set the tone on cyber security, the discussion and awareness is there, as demonstrated by the existence of this inquiry and audit, but it needs to go further. The Australian government should be the place the world looks to as an exemplar of good cyber security practice.

I welcome the opportunity to appear before your committee to give oral evidence.

Yours sincerely

[redacted]

Alastair MacGibbon
Special Adviser to the Prime Minister on Cyber Security

[redacted]

18 May 2017

[i] The ACSC is the co-located cyber security capabilities of the Australian Signals Directorate (ASD), the Defence Intelligence Organisation (DIO), the Australian Security Intelligence Organisation (ASIO), the Computer Emergency Response Team (CERT) Australia, the Australian Criminal Intelligence Commission (ACIC), and the Australian Federal Police (AFP).

[ii] https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf

[iii] https://cybersecuritystrategy.dpmc.gov.au/first-annual-update/prime-ministers-foreword.html

[iv] https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf