Australian Government

Department of the Prime Minister and Cabinet

ANDREW FISHER BUILDING
ONE NATIONAL CIRCUIT
BARTON

Response to Question on Notice

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

JCPAA Inquiry on Cybersecurity Compliance

Department of the Prime Minister and Cabinet (PM&C) with coordinated comments by the Digital Transformation Agency (DTA)

GENERAL COMMENTS

Nil.

SPECIFIC QUESTIONS ON NOTICE

Question 1
Regarding Submission 2 from Ian Brightwell:

1.1 One of Mr Brightwell's recommendations was to remove whitelisting from the mandatory list of strategies and focus on implementing a full set of ICT general controls to a level appropriate to the agency risk assessment. What are your thoughts on this recommendation?

1.2 Another of Mr Brightwell's recommendations is the suggestion that government Chief Information Security Officer positions not be combined within the technology delivery area and have a direct reporting line to the CEO. What are your thoughts on this recommendation? Can you please list the government agencies that have a direct CISO report to the CEO, and the government agencies that don't.

Response

1.1: PM&C:
The Australian Signals Directorate are responsible for the strategies to mitigate cyber intrusions and are best placed to respond to this question.

1.2: PM&C:
The extent of reporting of cyber security issues to senior management speaks to the security culture of our departments and is an important part of ensuring cyber security is considered as a key business risk. Whilst it is important we acknowledge the different historical structures and frequent barriers that exist within the APS structure, more of our departments should be

looking to industry as models of best practice. The recent release of Australia's first ASX 100 Cyber Health Check indicated Australia's biggest companies are increasingly ranking cyber risk as a key strategic risk requiring the focus, leadership and governance of their boards and most senior directors. All our government departments should do the same.

Question 2
Regarding Submission 3 from Macquarie Telecom:

2.1 On what basis were government agencies given exemptions from the Lead Agency Gateway Program and which agencies are they? When were they given exemptions?

2.2 Why have some agencies simply not joined the program, and which agencies are they?

2.3 Why are agencies allowed to negotiate tailored programs? Which government agencies have negotiated tailored programs and how have they been tailored? Which controls are they missing? – Please list against the agency.

Response

2.1: DTA:
Government granted one agency, the Australian Bureau of Statistics (ABS), exemption from the Program on the basis of the requirements of the *Census & Statistics Act 1905* and Section 16 of the *Australian Bureau of Statistics Act 1975*. The ABS was granted exemption from the Program in 2010.

2.2: DTA:
All Non-corporate Commonwealth Entities (NCEs) (formerly *FMA Act* agencies) are by default part of the Program. Agencies are required to seek formal opt out to no longer be in the Program. The ABS is the only agency that has sought or been granted exemption from the Program.

2.3: DTA:
The Program allows each agency to tailor their gateway requirements to meet its needs through a lead and client agency contractual arrangement. Three lead agencies offer an in-house gateway service while the remaining six lead agencies offer an outsourced gateway service provided by a commercial provider such as Macquarie Telecom. Lead agencies are responsible for acquiring, establishing and managing shared internet gateways. Security control arrangements are agreed to and managed under each of the lead and client agency arrangements. The DTA has no involvement or visibility of these contractual arrangements.

Question 3
Regarding Submission 3.1 from Macquarie Telecom:

3.1: Why aren't all government agencies required to comply with the Lead Agency Gateway program?

3.2: How can this be fixed quickly?

3.3: Should the Digital Transformation Agency set a deadline, and what should that deadline be?

3.4: Why was the Australian Bureau of Statistics given an exemption from the program?

3.5: What are your thoughts on the recommendation that the Australian Bureau of Statistics be compelled to comply with the program?

3.6: What are your thoughts on the recommendation that government agencies accelerate their transition to cloud computing?

Response:

3.1: DTA:
All Non-corporate Commonwealth Entities are by default part of the Program. There are currently no formal processes to compel non-Corporate Commonwealth Entities to comply with the Program.

3.2: DTA:
The DTA's Review of the Program will assess whether there is a need to continue the Program.

3.3: DTA:
The Review would determine the need to change compliance or for any deadlines.

3.4: DTA:
The ABS was given exemption from the Program by government on the basis of the requirements of the *Census & Statistics Act 1905* and Section 16 of the *Australian Bureau of Statistics Act 1975*.

3.5: DTA: The DTA will consider the ABS' participation in the Program as part of its proposed Program Review.

3.5: PM&C: In regards to compelling the Australian Bureau of Statistics (ABS) to comply with the Lead Agency Gateway Program, I refer to my response to Question four. If the Gateway Program is assessed as fit for purpose and will provide superior cyber security protection to that already in place, then there may be merit in compelling the ABS to comply with the program. However, doing so must also take into consideration the need for departments to individually assess and manage their unique risks and threats, and the potential for departments to become complacent once protected by a managed gateway. It is more important that departments are actively assessing and responding to the threats affecting them, than it is to apply a one size fits all approach to security.

3.6: DTA: The DTA is working in partnership with government agencies and with commercial providers to develop a Secure Cloud Strategy that will make it easier for government to take up cloud technologies.

Question 4
The Committee would appreciate if you could elaborate on the following comments made at the hearing:

"Mr MacGibbon: I have spoken to the DTA on the gateway program, now that it has transferred to them. I have asked them whether or not they think it is still best practice, given the fact that we are in 2017 and it was program that was fit for purpose at the time. I also asked what they thought good would look like for a gateway program. Again, going to my written submission to the committee, I often fear that an agency can be lulled into a false sense of security because it sits behind a gateway, for example, or it meets compliance of the top four or the Essential Eight and therefore all is good. I do not subscribe to the all-is-good category; I subscribe to the constant risk and how we reduce the likelihood of that risk being realised. I have spoken to the CEO of the DTA to ask that, now that it has transferred to the DTA, we do not just look at compliance with the existing program but we look to see whether that program is fit for it, as we move forward. Frankly, I would doubt that it is as fit for purpose today, now that we have many more mobile devices and a perimeter that is way more pervasive than it ever was a decade ago."

Response

4: PM&C:
The need to reduce the number of government internet gateways was identified as a priority under the 2009 Cyber Security Strategy. Since this time, the number of people, devices and threats to our government departments have increased exponentially. By reducing the number of gateways, the strategy proposed to "maximise efficiency, reliability and security" of our gateways. In many cases, this plan has enabled departments to consolidate resources and provided increased security. However, as I said during the committee hearing, we are always on the lookout for better ways to do business. Both criminals and state sponsored actors are constantly looking for new ways to harm us, so we must be just as agile and responsive. We must constantly test and reassess our methods to ensure what we are doing is best practice in light of our changing environment.

It is partly for this reason that the Prime Minister recently announced a new taskforce to drive fast improvement of Australia's capability and response to cyber security. In leading this taskforce, I will look to determine what 'good' actually looks like. This will include exploring approaches such as the gateway program and whether or not it remains the best possible option for protecting the valuable information our departments hold. At the same time, I have asked the CEO of the Digital Transformation Agency – Gavin Slater – to ensure this program is assessed not through compliance with the existing framework but on the framework itself, ensuring a culture of agile and responsive cyber security is what drives the agency.

4. DTA:
The Digital Transformation Agency (DTA) assumed responsibility for the Australian Government's Internet Gateway Reduction Program (the Program) from the Department of Finance in December 2016 under Machinery of Government changes announced in October 2016.

The Program was approved by the Government in 2010.

The Program was a product of government and industry understanding of internet security and technology at the time. However, it may no longer be best practice today. The DTA will undertake a review of the Program's effectiveness.

Question 5
Regarding question posed by Committee Chair Senator Smith:

How frequently does the Cyber Security Board meet?

Response

5. PM&C: A governance and agency consultation structure was developed in 2016 following the release of the Cyber Security Strategy. This includes a Cyber Security Board chaired by the Secretary of PM&C and attended by Secretaries or Agency heads of ASIO, AFP, Defence, AGD, ACIC, DFAT, Finance and DIIS. As well as a Cyber Security Priorities group that brings together senior executive level representatives from each of these agencies. We have had 15 formal meetings with the agencies involved. Meetings are scheduled to occur regularly but also happen in the event of an issue or incident such as Wanacry. The cadence of regular meetings is increasing, with planned meetings for the formal board every two months for the rest of 2017.