Joint Committee of Public Accounts and Audit

Inquiry into Cyber Resilience based on the Auditor-General's Reports 1 and 13 (2019-20)

Attorney-General's Department

Hearing date: **2 July 2020**

Question date: **17 July 2020**

Question type: **Written**

Tim Watts MP asked the following question:

1. Self-reported assessments of PSPF compliance (mandatory Top 4) of non-corporate commonwealth entities, published by the AGD were:
2014-15: 32.26%
2015-16: 37.63%
2016-17: 34.41%
2017-18: 40.43%

The 2019 Cyber Security Posture Report found that "73 per cent of non-corporate Commonwealth entities reporting ad hoc or developing levels of maturity".

Why has the implementation of 'mandatory' cyber security controls been so consistently slow? (Attorney General's Department)

The response to Mr Tim Watts MP's question is as follows:

It is an ongoing process for entities to implement the requirements under the Protective Security Policy Framework (PSPF), including cyber security requirements, in the context of an evolving threat environment and their own individual risk environment and operational circumstances.

As outlined in the first annual Report to Parliament on the Commonwealth's Cyber Security Posture, in 2019, the overall cyber security of Australian Government agencies continued to improve through:

- increased capability to identify cyber security events and incidents;
- improvements in organisational cyber security practices, including cyber incident management plans and procedures;
- improved implementation of malicious email mitigation strategies across the Commonwealth; and
- increased visibility and understanding of Commonwealth systems, data holdings and networks.

To assist entities strengthen their cyber security, the Australian Government has made a substantial investment in the capabilities of the Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC) to identify emerging cyber threats and respond to cyber threats on a national scale, including tailored advice and assistance about how to mitigate cyber threats.

Tim Watts MP asked the following question:

2. In the last report issued by the JCPAA on cyber security (Report 467) Recommendation 2 provided:

"The Committee recommends that the Australian Government mandate the Australian Signals Directorate's Essential Eight cybersecurity strategies for all Public Governance, Performance and Accountability Act 2013 entities, by June 2018."

In response, the government stated:

"The Government is committed to ensuring all Commonwealth entities raise their level of cyber security and understand the risks they face. The Essential Eight represents ASD's best advice on the measures an entity can take to mitigate the threat of a cyber incident and manage their risks. However, the Government will consider mandating the Essential Eight when cyber security maturity has increased across entities." At his June 19th press conference the Prime Minister outlined an increasingly dangerous cyberspace threat environment for the Australian government; specifically highlighting that "Australian organisations are currently being targeted by a sophisticated state-based cyber actor… including all levels of government" At the July 2nd JCPAA hearing the Attorney General's Department indicated that they had considered an decided not to increase the mandatory cyber security requirements within the PSPF from the Top 4 to the Essential 8. Given Recommendation 2 of JCPAA's report on cyber resilience (Report 467), that the Essential Eight be made mandatory for all Public Governance, Performance and Accountability Act 2013 entities by June 2018, and given the increasingly dangerous cyber threat environment highlighted by the Prime Minister and the claimed improvement in the cyber maturity levels of Commonwealth entities, why was the decision made not to incorporate ASD's Essential Eight mitigations as mandatory aspects of the PSPF?

The response to Mr Tim Watts MP's question is as follows:

The issue of mandating all Essential Eight mitigations in the Protective Security Policy Framework (PSPF) remains under consideration by the Attorney-General's Department (AGD) having regard to cyber security maturity levels across entities and ASD's technical advice.

While mandating the implementation of the first four mitigation strategies (known as the Top Four), the PSPF strongly recommends the adoption of the Essential Eight (which includes the Top Four). The PSPF also mandates that entities must consider all of the ACSC strategies, including the Essential Eight, to mitigate cyber security incidents, informed by their individual risk environment. Further, from 2018-19 on, all entities must report on their implementation of the Essential Eight as part of the new PSPF maturity reporting model.

As advised at the hearing on 2 July 2020, ASD's technical advice is that the Top Four provide the greatest defence and AGD's view is that it is appropriate at this point in time to prioritise the mandatory application of the Top Four strategies.

AGD continues to keep the mandatory requirements under review and the new reporting from all entities about their implementation of the Essential Eight will assist in consideration of this issue.

3. Mr Tim Watts MP asked the following question:

At the July 2nd 2020 JCPAA hearing Mr Hill asked:

"On the regulatory framework, can I focus on the ANAO's statement that its submission to this inquiry was that 'the regulatory framework had not driven sufficient improvement in cyber security'. This was a common theme of the ANAO's cyber-resilience audits. In its 2018 cyber-resilience audit of the Treasury, the National Archives and Geoscience Australia, the ANAO also stated:

These findings provide further evidence that the implementation of the current framework is not achieving compliance with cyber security requirements, and needs to be strengthened.
Then, at the last public hearing, the Auditor-General said:
We wouldn't be auditing as much as we do if we had seen a progressive improvement through time. ".." the level of work we do is a reflection of our concerns about the level of compliance within the sector. It goes not just to individual entities but to the effectiveness of the framework.

They're very strong words over a number of years about the failure of the framework, I think, to achieve the compliance the government says it's seeking. The question to AGD is: after seven years of low levels of compliance with mandatory cybersecurity requirements by Commonwealth entities, whatever you're doing or say you're doing is clearly not working, so what are you now going to do to fix the regulatory framework to drive sufficient improvement in cybersecurity?"

In response, the representative (Ms Chidgey) from the Attorney General's Department indicated that they disagreed with the premise of the question.
Given that Mr Hill was quoting from ANAO reports and evidence given by the Auditor General to this Committee, was aspects of the ANAO/Auditor General's evidence was AGD disputing?

The response to Mr Tim Watts MP's question is as follows:

AGD does not consider there is a 'failure of the framework'. The results from the 2018-19 PSPF assessment reports and the 2019 Commonwealth Cyber Security Posture Report indicate that there are improvements in entities' cyber security. AGD also notes that reforms to the PSPF were made in 2018.

4. Mr Tim Watts MP asked the following question

The recently released 2020 Force Structure Plan highlighted an increasingly dangerous cyberspace threat environment for the Australian government:

"Defence is becoming more reliant on fast, reliable and secure internet based communications. But the threat to this connectivity from malicious actors is also growing. There has been a marked increase in cyber-attacks against Australia by foreign actors and criminals"

The 2020 Defence Strategic Update then outlined $15 billion of investment over the coming 10 years in the Information and Cyber domain.

How much of this funding will go to Commonwealth departments to progress their implementation the mandatory Top 4 cyber security controls specified in the PSPF?

The response to Mr Tim Watts MP's question is as follows:

This question is a matter for the Australian Signals Directorate.

5. Mr Tim Watts MP asked the following question

Commonwealth entities have been required to undertake an annual self-assessment against the mandatory requirements of the Protective Security Policy Framework since 2013.
But in the ANAO's evidence before the JCPAA on 21st March 2019, Mr Hehir told the committee

"What our audits have found is that, when we've gone in and tested compliance with the framework and then checked that against self-reporting, there hasn't always been a strong correlation between the two things."

At that time ANAO cyber resilience audits had found that 29% of agencies audited were compliant with the ASD's Top Four mitigations, whereas 60% of departmental self-assessments found themselves to be compliant.

We put this issue to AGD in Senate Estimates in November 2019 and the Department's position was that this disparity was not a problem because these processes were:

"not directly comparable. The methodology used by the ANAO differs from the self-assessments agencies are requires to complete under the PSPF."

In the last hearing of this inquiry on 19th May 2020 JCPAA, the ANAO was unable to name any meaningful differences between the way a commonwealth entity would self-assess their compliance with ASD Top 4 Mitigations and the way the ANAO assesses this.
Could AGD please explain how these processes differ?

The response to Mr Tim Watts MP's question is as follows:

The new PSPF maturity model replaces point in time compliance reporting with ongoing monitoring of security maturity and implementation of PSPF requirements, with the reporting informed by the entity's overall security position within its specific risk environment and risk tolerances. Under the compliance model, when ANAO audited the entity on its self-rated compliance level, this could be some time after the point in time information was provided, and the entity's positon may have changed.

Further, to support more nuanced reporting, the PSPF reporting portal guides entities through a series of questions to assess and demonstrate their level of implementation for each PSPF requirement. Entities that assess themselves as *ad hoc* or *developing* are required to provide additional information on how they will improve their maturity during the coming year, before they can submit their annual report.

6. Mr Tim Watts MP asked the following question

The Auditor General's opening statement to the JCPAA cyber resilience inquiry in the previous Parliament stated:

"the implementation of the current framework is not achieving compliance with cyber security requirements and needs to be strengthened, as proposed in Recommendation no.2 of the Cyber Resilience audit."

Recommendation 2 of the June 2018 ANAO Cyber Resilience Audit stated:

In revising security reporting and cyber-related requirements under the Protective Security Policy Framework, the Attorney-General's Department, Department of Home Affairs and Australian Signals Directorate work together to improve compliance with the framework by:
a) providing adequate technical guidance to support entities to accurately self-assess compliance with the Top Four mitigation strategies and their underlying controls contained in the Information Security Manual;
b) developing a program for verifying entities' reported compliance with the mandatory cyber security requirements; and
c) increasing transparency and accountability about entities' compliance with those requirements.

The response to Mr Tim Watts MP's question is as follows:

The 2018 changes to PSPF reporting require entities to refer to evidence to support their security maturity assessment. AGD is also exploring moderation models that could be adopted as part of the PSPF to moderate or review entities' security assessments for different PSPF requirements. This includes consideration of moderation models that include peer review, benchmarks or other arrangements.

As part of the new reporting model entities are also required to provide more extensive details on forward planning and specific advice on the improvements they are proposing to implement to lift their protective security and the timeframes for implementation.

7. Mr Tim Watts MP asked the following question:

Does AGD believe that the heightened cyber threat environment highlighted recently by the Prime Minister make the need for this increased cyber security accountability more acute?

The response to Mr Tim Watts MP's question is as follows:

Cyber security is a critical part of protective security. This is why the 2018 reforms of the PSPF gave more prominence to cyber security requirements and created a new Chief Security Officer role to increase senior visibility of entity protective security settings and increase entity-level accountability. The settings in the PSPF are regularly reviewed to ensure the requirements are appropriate and fit for purpose.

8. Mr Tim Watts MP asked the following question:

Given the long history of noncompliance and the deteriorating threat environment, does AGD think cyber security is too important to continue allow Commonwealth entities to continue to mark their own homework on their compliance with these obligations?

The response to Mr Tim Watts MP's question is as follows:

See answer to question 6 above.

9. Tim Watts MP asked the following question:

In Senate estimates, when asking about Commonwealth entities' Top 4 compliance, the orchestrated response received from multiple entities read, in part:

"Publicly reporting on individual agency's compliance with the Essential 8 in response to these questions on notice would provide a single, detailed and individualised snapshot in time of the entire Federal Government's cyber security maturity and as a result may provide a heat map for vulnerabilities in Federal Government networks, which malicious actors may exploit and thus increase an agency's risk of cyber incidents."

But the Auditor General has challenged this response, stating, when appearing before the JCPAA on 19th May 2020:

"We never report a level of detail which we believe would put any particular entity at risk."

Over the past 6 years ANAO has conducted 5 public cyber resilience performance audits of 16 different Commonwealth entities examining ASD Top 4 compliance. It is currently undertaking such an audit into 9 government entities.

Why is it acceptable for the ANAO to be undertaking and publishing their audits but not for the government to implement transparent accountability mechanisms?

The response to Mr Tim Watts MP's question is as follows:

ANAO audits are conducted at a single point of time across a small sample of entities. Providing detailed information on cyber security vulnerabilities for all individual Commonwealth entities would significantly increase the risk that vulnerabilities could be exploited. The aggregation of the information would in effect provide adversaries with a heat-map of the Commonwealth's entire cyber security posture.

10. Tim Watts MP asked the following question:

How could a Member of Parliament hold a Commonwealth Entity accountable for non-compliance with mandatory cyber security requirements in commonwealth entities for which they are responsible?

The answer to Tim Watts MP's question is as follows:

While AGD is not able to advise on parliamentary processes, we understand parliamentary committees can make arrangements to receive information in private having regard to the requirements of security. The PSPF mandates that each entity must report on security each financial year to their portfolio minister. The Attorney-General's Department provides an annual report to the Attorney-General and publishes a whole of government assessment report on its website.

Tim Watts MP asked the following questions:

11. Of the 25 Commonwealth entities that were involved in the government's 'Cyber Uplift', none were assessed to have achieved their recommended cyber security maturity level. The 2019 Posture Report concluded that "these entities are vulnerable to current cyber threats targeting the Australian government".

Why did the Cyber Uplift end if none of the entities involved had reached minimum cyber security requirements?

12. Why was the Cyber Uplift unable to bring any of these entities up to minimum cyber security requirements?

13. What did this Cyber Uplift program cost? Is the ASD funded to run further Cyber Uplifts in the coming year?

14. Was funding for further Cyber Uplifts included in the Prime Minister's recent multi-billion dollar cyber security announcement?

15. The 2019 Cyber Security Posture Report indicated the creation of a 'Cyber Security Response Fund'. What is that used for?

16. How much was originally allocated to the Cyber Security Response Fund?

17. How much of the money allocated to the Cyber Security Response Fund has been spent?

18. At the last JCPAA hearing the Auditor-General indicated that ASD was currently undertaking a number of "Sprint tests". What is the purpose of these tests?

19. Will the findings of these tests be made available to members of this committee?

20. Since 2016, more than 10,000 vulnerabilities have been discovered as security researchers were invited to US government bug bounties including: Hack the Pentagon, Hack the Army, Hack the Air Force, Have the Marine Corp and Hack the Defence Travel System. Has the government considered the adoption of bug bounty programs for Commonwealth government agencies?

21. Why has the Commonwealth government not used bug bounty programs to supplement the cyber security posture of Commonwealth entities?

22. Are there any centralised guidelines or policies for Commonwealth agencies concerning the use of bug bounty programs for their IT systems? If not, why not?

23. Since August 2019, the United Kingdom's National Cyber Security Centre has operated a vulnerability disclosure platform of last resort for UK government entities on the HackerOne platform. Why has the Commonwealth government not used a centralised vulnerability disclosure program to supplement the cyber security posture of Commonwealth entities?

24. Are there any centralised guidelines or policies for Commonwealth agencies concerning the implementation of vulnerability disclosure programs for their websites or IT systems? If not, why not?

The answers to Tim Watts MP's questions 11-24 are as follows:

These questions are a matter for the Australian Signals Directorate.

Joint Committee of Public Accounts and Audit

Inquiry into Cyber Resilience based on the Auditor-General's Reports 1 and 13 (2019-20)

Attorney-General's Department

Hearing date: **2 July 2020**

Question date: **21 July 2020**

Question type: **Written**

Lucy Wicks MP asked the following questions:

Questions regarding measuring a cyber-resilient culture

Home Affairs and the Attorney-General's Department both agreed that a cyber-resilient culture was difficult to measure (page 17 of the transcript).

1. AGD/Home Affairs – Have you used the ANAO's framework for a strong cyber-resilient culture in any of your reporting on a Commonwealth entities' compliance with cyber security measures and practices?
2. AGD/Home Affairs – Do you believe the ANAO's framework should be used by Commonwealth entities as a guide for building a strong cyber-resilient culture?
3. AGD/Home Affairs – How can the key lessons from the audit of the Reserve Bank, who was identified by the ANAO as having the strongest cyber-resilient culture of the entities it has audited, be applied to other Commonwealth entities in establishing a similarly strong cyber-resilient culture?

Questions regarding engaging the community and the private sector

The Commonwealth Cyber Security Posture (2019) outlines the importance of cyber resilience not only within Commonwealth entities but also among private business and society.

4. AG/Home Affairs – What role do policy owners in this space see for educating businesses and individuals on the importance of cyber resilience? What efforts are being taken to do this?

The responses to Lucy Wicks MP's questions are as follows:

1. While the Protective Security Policy Framework (PSPF) does not directly apply the ANAO's framework, the requirements in the security governance outcome of the PSPF are similar to the strategies and structures outlined in ANAO's framework. The PSPF includes requirements such as appointing a Chief Security Officer, forming a security plan and putting in place appropriate governance structures for their security environments. Entities are required to report against these requirements annually.

2. The ANAO's framework is a useful additional resource for Commonwealth entities to consider in building a strong cyber-resilient culture. The PSPF includes a range of requirements that assist entities to establish appropriate governance arrangements to

support protective security culture, of which a cyber-resilient culture is one part. The PSPF takes a holistic and integrated approach to protective security and security culture, encompassing information, people and physical security. AGD has established a Security Culture Community of Practice to enhance and strengthen security culture across Australian Government entities, and has worked with that Community of Practice to produce a Cultural Transformation Strategy to support entities with their obligation to foster a positive security culture.

3. AGD supports a number of mechanisms to enable Commonwealth entities to share and learn from good protective security practices across the Commonwealth. These include the Security Culture Community of Practice, a regular Chief Security Officer newsletter and biannual Chief Security Officer forums. In developing a strong security culture it is important that entities tailor their strategies to their different risk and operating environments and continue to evolve and improve those strategies. It is also important to recognise that a cyber-resilient culture must be part of, and integrated with, a positive protective security culture more generally, as cyber security outcomes are linked to and mutually dependent on effective security governance, personnel security and physical security.

4. This is a matter for the Department of Home Affairs as the relevant policy owner. AGD is responsible for Australian Government protective security policy. While the PSPF is directed toward Commonwealth entities, the framework and the related protective security policy website includes a range of guidance, information and tips about enhancing protective security that could be relevant to the private sector.