Auditor-General for Australia

Australian National Audit Office

22 June 2021

Ms Lucy Wicks
Chair
Joint Committee of Public Accounts and Audit

Via email: jcpaa@aph.gov.au

Dear Ms Wicks

ANAO response to recommendation 4, JCPAA Report 485: Cyber Resilience

Following the ANAO's meeting with the Committee on 12 May 2021, I am writing in response to a number of discussion points and to provide a formal response to the recommendation in JCPAA Report 485, which is attached. As we discussed in the meeting, the approached proposed in the recommendation poses challenges both in the nature and scope of audit activity. The absence of an assurance framework over self-reporting by entities not only limits the reliance that Parliament can place on the reporting produced by the Attorney-General's department, it also limits the ANAO's ability to undertake work of the nature proposed in the recommendation.

Background

JCPAA Report 485 was presented to the Parliament in December 2020 following the Committee's inquiry into Auditor-General Reports 1 and 13 (2019–20). Recommendations were made in the report to the Attorney-General's Department (AGD) including:

- updating the Committee on verification of entities' reported compliance with cybersecurity requirements (recommendation 1);
- updating on the feasibility of mandating the Essential Eight across Commonwealth entities including GBEs and corporate Commonwealth entities (recommendation 2); and
- ensuring the framework of 13 behaviours and practices developed by the ANAO play a greater role in the implementation of cybersecurity (recommendation 3).

In March 2021, Auditor-General Report No. 32 (2020–21) was presented to Parliament. In undertaking this audit, the ANAO took a different approach to its previous cyber security performance audits in a number of respects:

- in the selected entities, the ANAO tested the maturity rating given to required controls where the entity had indicated compliance in its self-assessment report to AGD (in other words, to test whether the assessment was accurate and based on evidence);

GPO Box 707, Canberra ACT 2601
38 Sydney Avenue, Forrest ACT 2603
Phone: +61 2 6203 7300
Email: grant.hehir@anao.gov.au

- the ANAO did not assess the 13 behaviours and practices of cyber resilient cultures as the Protective Security Policy Framework (PSPF) was updated to include characteristics of a positive security culture in *Policy 2 Management structure and responsibilities*, specifically in the subsection *Foster a positive security culture*. As the policy was introduced in October 2018, the ANAO decided it was too early to audit during 2020;
- the ANAO reduced the level of detail reported on identified non-compliance, after considering advice from the Australian Signals Directorate (ASD). This was a compromise for ASD and the ANAO recognising the benefits and risks of transparency in cyber security reporting (see paragraphs 10 – 12 of Report No. 32.)

In Report No. 32 the ANAO made recommendations to AGD (as the PSPF policy owner) covering:

- reviewing existing maturity levels under the PSPF maturity assessment model to determine if the maturity levels are fit-for-purpose and effectively aligned with the Essential Eight Maturity model, having regard to ASD's proposed update to the Essential Eight Maturity model (recommendation 9);
- further improvements to the guidance on PSPF Policy 10 (recommendation 10); and
- implementation of arrangements for AGD to obtain an appropriate level of assurance on the accuracy of entities' PSPF Policy 10 self-assessment results (recommendation 11).

The report also found that "….the status of entities' cyber security posture is not transparent due to the policy and operational entities' concerns about increasing security risks following the disclosure of individual entities' cyber security maturity level. The cyber policy and operational entities have not established processes to improve the accountability of entities' cyber security posture. The current framework to support responsible Ministers in holding entities accountable within Government is not sufficient to drive improvements in the implementation of mandatory requirements" (paragraph 20).

Report No. 32 is the sixth performance audit undertaken by the ANAO on cyber security since the Top Four mandatory requirements of the Australian Government Information Security Manual (now part of the PSPF) were made mandatory in 2013. Entity compliance with the mandatory Top Four remains low.

The Auditor-General's mid-term report made the following observations with respect to cyber security:

> "The public sector operates largely under a self-regulatory approach. Policy owners — for example the Department of Finance for resource management (including procurement and grants); the Attorney-General's and Home Affairs departments for cyber security; and the Australian Public Service Commission for integrity — establish the rules of operation and then largely leave it to entities' accountable authorities to be responsible for compliance. There are almost no formal mechanisms in these frameworks to provide assurance on compliance. Often the ANAO is the only source of compliance reporting and our resources mean that coverage is quite limited. While I agree that accountable authorities must be responsible for entities' compliance, it is also clear that policy owners need to be held accountable if the regulatory frameworks they put in place for the public sector do not result in an acceptable level of compliance. For this to occur, they should at least have processes in place to identify the level of compliance and be willing to modify their regulatory approach if it is not working. Unfortunately, this has not been a common approach." (see page 4)

JCPAA recommendation 4, Report 485: ANAO considerations

In its report on Cyber Resilience, the Committee made the following recommendation to the ANAO:

> "The Committee recommends that the Australian National Audit Office (ANAO) consider conducting an annual limited assurance review into the cyber resilience of Commonwealth entities, with the cost

to be met by the responsible policy agencies or Government. The review should examine and report on the extent to which entities have embedded a cyber resilience culture through alignment with the ANAO's framework of 13 behaviours and practices. The review should also examine the compliance of corporate and non-corporate entities with the Essential Eight mitigation strategies in the Information Security Manual and be conducted for 5 years, commencing from June 2022 (to enable time for implementation)."

The ANAO considers continued transparency through reporting to Parliament is positive. The system-level transparency that might result from an audit of the nature contemplated in the recommendation would contribute to that. In saying that, it is clear that auditing and reporting alone is not driving improvement in compliance with the government's cyber security policy. Non-corporate Commonwealth entities have not been held to account for not meeting the mandatory cyber security requirements under PSPF Policy 10. The current framework to support responsible Ministers in holding entities accountable within government is not sufficient to drive improvements in the implementation of mandatory requirements. Recommendation 13 in Report No. 32 suggested that the government strengthen arrangements to hold entities to account.

As discussed in the recent meeting, JCPAA recommendation 4 poses a number of practical challenges from an audit perspective:

1. There is likely to be cyber security risk concerns raised by ASD – ASD accepted the revised description of the findings in Report No. 32 as it covered a small number of entities and entities were addressing the issues identified by the ANAO in the course of the audit. Non-material issues were also removed from the published report. ASD has advised that a system-level report would pose cyber risks that it believes would be unacceptable. Given ASD is the technical expert, it is best placed to assess those risks and therefore difficult for the ANAO to take a different view.

The JCPAA could seek a classified briefing from AGD and ASD on the system-level reports that each produces, noting that AGD does not verify the accuracy of self-assessments, and ASD's is based on a combination of an annual survey and detailed reviews.

2. The scope proposed in the recommendation is challenging given that only Non-corporate Commonwealth entities are mandated to apply the PSPF. Auditing Corporate Commonwealth entities would need to be against the frameworks they adopt – this increases cost in auditing.

The JCPAA made a recommendation in its Report 485 to AGD which included "…report back on any impediments to mandating the Top Four mitigation strategies for government business enterprises and corporate Commonwealth entities". The ANAO notes AGD's response to this recommendation. The JCPAA may wish to seek advice from the Department of Finance on requiring compliance with policies of the Australian Government for corporates and GBEs.

3. The number of entities subject to the policy creates a scope challenge.

There are 98 non-corporate entities subject to the policy (excluding the ANAO). Auditing, even on a limited assurance basis, the evidence provided to AGD by 98 entities is resource intensive. It is possible to seek assistance from ASD to identify those entities, for example, where cyber poses a material risk based on the nature of their business. It is likely that auditing even a reduced population (such as 40 entities) would be costly (for example, the cost of the 2019–20 Defence Major Projects Report (MPR) which reviewed 25 projects was $2 million) and would likely raise additional concerns from ASD because of the increased cyber security risk posed by reporting on findings of a large number of entities.

4. The absence of assurance over material reported by entities to AGD in their self-assessments means that audit procedures would need to be conducted across the population of entities' self-assessments (whole or risk-based sample) to assure accuracy.

A more efficient and effective way for the ANAO to provide assurance is to do so on a report that is compiled centrally (eg. by AGD) that assesses the accuracy of the information being provided by the entities as part of PSPF self-assessment. This would be a similar approach to the MPR.

Auditor-General Report No. 32 recommends the implementation of arrangements for AGD to obtain an appropriate level of assurance on the accuracy of entities' PSPF Policy 10 self-assessment results (recommendation 11). AGD agreed in principle to that recommendation. The ANAO notes AGD's update to the JCPAA Report No. 485 (recommendation 1) that an approach to improve the accuracy of self-assessments will be determined by the second half of 2021.

The JCPAA could consider seeking further representations from AGD on its intention to pursue the Auditor-General recommendation in the context of its own recommendation 2. In doing so, the JCPAA could consider whether the policy owner (AGD) is regularly assessing the success of the policy and providing advice on policy improvements in accordance with the Attorney-General's Directive on the security of government business (which accompanies the PSPF) which says:

> "The Australian Government, through my Department with oversight of the Government Security Committee, will continue to assess emerging security risks and develop and refine protective security policy that promotes efficient secure delivery of Government business."

The integrity of the assessment and advice should be supported by accurate information, otherwise there is a risk that the PSPF may not be effective nor efficient in supporting the security delivery of Government business.

5. The funding model proposed in the recommendation is not consistent with the ANAO's funding model.

The implementation of the recommendation would require additional funding via an appropriation or agreement. This could be achieved through AGD developing a model to support the activity.

6. Limited assurance procedures do not result in a report which informs the Parliament about the actual implementation of cyber security requirement.

In undertaking a limited assurance review of the implementation of PSPF Policy 2 (which provides guidance on the characteristics of a positive security culture) and PSPF Policy 10 (the Top Four), the ANAO could look at evidence which supported self-assessments of "managing" to see if the reporting was accurate and conclude that nothing has come to attention that indicates the results cannot be relied upon. The ANAO notes that AGD will recommend to the Attorney-General to update PSPF Policy 10 to additionally mandate the remaining four mitigation strategies within the Essential 8. The above approach would still be applicable. Current ANAO work in cyber security in both financial statements audits (IT controls) and in performance audits indicate that the ANAO is likely to find issues with the accuracy of self-assessments. In the event that accuracy issues are found, the ANAO would conclude that the report could not be relied upon, but would not report on whether entities actually do meet the requirements of the PSPF. Alternatively, the ANAO could take additional audit procedures where an issue of accuracy is identified, effectively moving to reasonable assurance (the standard audited against in Report No. 32's assessment against PSPF Policy 10). The cost to proceed with either of these approaches on a reasonable sample or total population is very high. A team of appropriate size and capability to undertake the scale and effort of the work is not currently available to the ANAO.

ANAO preferred approach

Improvements in the framework have occurred with mandatory central reporting of entity self-assessments to AGD. As yet, no quality assurance procedures are in place within AGD to assess the accuracy of reported information. The ANAO notes AGD's update to the JCPAA Report No. 485 (recommendation 1) that an approach to improve the accuracy of self-assessments will be determined by the second half of 2021.

A review undertaken by the ANAO over any quality assurance processes implemented by AGD would provide information and assurance to the Parliament on whether entities' self-reporting on the implementation of PSPF Policy 2 and 10 core requirements is accurate.

The review would assess if entities had provided appropriate evidence to AGD to monitor and implement PSPF Policy 2 and 10 requirements. If there is insufficient evidence to conclude on the appropriateness of measures in place, additional review procedures would be performed to assess whether PSPF requirements had been implemented effectively.

AGD would be required to provide a report and supporting information on:

- entity self-assessments;
- verification and assurance activities and results;
- accountability and governance;
- security risks and issues;
- schedule and financial performance;
- learning and development;
- lessons learned; and
- security plans.

The review would include an assessment of the assurance processes in place by AGD as per an overarching guideline endorsed by the JCPAA, and be performed in accordance with the ANAO Auditing Standards specified by the Auditor-General under the *Auditor-General Act 1997*.

A response to recommendation 4 in JCPAA report 485 is attached.

Yours sincerely

[redacted]

Grant Hehir
Auditor-General

JCPAA Report 485: Cyber Resilience

ANAO response to recommendation 4

The ANAO supports increased transparency to the Parliament of entity compliance with the PSPF, in particular cyber security compliance, acknowledging that this needs to be balanced with the potential risk of increased cyber security threat through public reporting. However, the ANAO does not see an audit of the type suggested in the recommendation as the most effective way of achieving this outcome.
The ANAO has undertaken six performance audits of cyber security since the mandatory requirements came into effect in 2013. ANAO audits continue to find low compliance with cyber security requirements.

The regulatory framework for compliance with the mandatory and recommended cyber security policies of the government currently has no internal assurance mechanism to assess the effectiveness of the policy's implementation by entities. It is only the external auditing work of the ANAO which verifies for Parliament and government the accuracy and reliability of performance reporting by entities in this policy area. The policy framework does not contain sufficient incentives or disincentives to drive improvements in performance.

In its most recent performance audit, Auditor-General Report No. 32 (2020-2021) *Cyber Security Strategies of Non-Corporate Commonwealth Entities* the ANAO made recommendations to the policy owner, Attorney-General's Department (AGD), including that the department implements arrangements to obtain an appropriate level of assurance on the accuracy of PSPF Policy 10 self-assessment results. AGD agreed in principle to this recommendation.

Should AGD implement such assurance arrangements, the ANAO considers that the auditing of assurance of the policy would have merit given the poor performance of the sector over many years in both implementation of the policy and accurate reporting of implementation. The extent of coverage of such an audit approach would take account of AGD's work to verify reporting. The extent of reporting of such an audit would also be cognisant of potential risk within the sector as advised by the Australian Signals Directorate (ASD).