PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

Report 485
Cyber Resilience

Inquiry into Auditor-General's Reports 1 and 13 (2019-20)

Joint Committee of Public Accounts and Audit

December 2020
CANBERRA

ISBN 978-1-76092-172-9 (Printed Version)

ISBN 978-1-76092-173-6 (HTML Version)

Contents

Chair's Foreword

Under the *Public Accounts and Audit Committee Act 1951*, the Joint Committee of Public Accounts and Audit examines all the reports of the Auditor-General tabled in the Parliament. The Committee periodically selects several of those reports for further detailed scrutiny.

This report reflects the Committee's inquiry into cyber resilience based on two Auditor-General reports.

Auditor-General Report No. 1 (2019-20), *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*, assessed the effectiveness of the management of cyber security risks by the Reserve Bank of Australia, the Australian Postal Corporation and the ASC Pty Ltd. The Committee was pleased to note that the Reserve Bank and ASC respectively had the highest and equal third highest level of cyber resilience of 17 entities examined by the ANAO over the past five years.

Auditor-General Report No. 13 (2019-20), *Implementation of the My Health Record System*, assessed the effectiveness of the implementation of the My Health Record system under the opt-out model by the Department of Health and the Australian Digital Health Agency.

I note that all recommendations made by the ANAO were accepted by the relevant agencies, and that work has progressed to address areas identified for improvement.

It is essential that Commonwealth entities continue their focus on managing cyber security risks and embedding a cyber resilient culture, to reach a mature cyber security posture that meets the evolving threat environment.

I would like to thank the organisations that made submissions and appeared at the public hearings for this inquiry, and Committee Members who have worked together to deliver this report.

Ms Lucy Wicks MP
Chair

Abbreviations

ADHA	Australian Digital Health Agency
ISM	Information Security Manual
ANAO	Australian National Audit Office
ASC	Australian Submarine Corporation
Australia Post	Australian Postal Corporation
JCPAA	Joint Committee on Public Accounts and Audit
Health	Department of Health
NIO	National Infrastructure Operator
OAIC	Office of the Australian Information Commissioner
PGPA Act 2013	Public Governance, Performance and Accountability Act 2013
PSPF	Protective Security Policy Framework
Reserve Bank	Reserve Bank of Australia

Members

Chair

Ms Lucy Wicks MP

Deputy Chair

Mr Julian Hill MP

Members

Ms Angie Bell MP

Senator Claire Chandler

Mr Pat Conroy MP (from 23.03.20)

Hon Dr David Gillespie MP

Hon Barnaby Joyce MP (from 27.08.20)

Senator Kimberley Kitching

Hon Dr Andrew Leigh MP (from 27.08.20)

Senator Matt O'Sullivan

Senator Rex Patrick

Ms Alicia Payne MP (until 27.08.20)

Senator Paul Scarr

Ms Kate Thwaites MP (until 23.03.20)

Mr Bert Van Manen MP (from 17.09.19 to 4.02.20)

Mr Ross Vasta MP (excluding period 17.09.19 to 4.02.20)

Senator Jess Walsh

Mr Tim Watts MP

Mr Rick Wilson MP

Mr Trent Zimmerman MP (until 27.08.20)

Committee Secretariat

Dr Joel Bateman, Committee Secretary (from 12.10.20)

Ms Stephanie Mikac, Committee Secretary (until 9.10.20)

Dr Kate Sullivan, Inquiry Secretary

Ms Carissa Skinner, Office Manager

Terms of Reference

On 5 February 2020, having considered recently tabled Auditor-General's Reports, the Joint Committee of Public Accounts and Audit resolved to conduct an inquiry into the following Auditor-General's Reports:

- No. 1 (2019-20) *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*
- No. 13 (2019-20) *Implementation of the My Health Record System*

Under section 8(1) of the *Public Accounts and Audit Committee Act 1951*, the Committee is required to 'examine all reports of the Auditor-General (including reports of the results of performance audits) that are tabled in each House of the Parliament' and 'report to both Houses of the Parliament, with any comment it thinks fit, on any items or matters in those reports, or any circumstances connected with them, that the Committee thinks should be drawn to the attention of the Parliament'.

List of Recommendations

Recommendation 1

1.73 The Committee recommends that the Attorney-General's Department provide an update on its implementation of external moderation models/benchmarking processes, to verify Commonwealth entities' reported compliance with cybersecurity requirements, including implementation timeframes.

Recommendation 2

1.77 The Committee recommends that the Attorney-General's Department:

- provide an update on the levels of cyber security maturity within Commonwealth entities and the feasibility of mandating the Essential Eight across Commonwealth entities, including the threshold of cyber security maturity required by Government to impose this mandate, and expected timeframes; and

- report back on any impediments to mandating the Top Four mitigation strategies for government business enterprises and corporate Commonwealth entities.

Recommendation 3

1.88 The Committee recommends that the Australian Government (the Attorney-General's Department) ensure that the framework of 13 behaviours and practices developed by the Australian National Audit Office (ANAO) play a greater role in the implementation and improvement of a cyber resilience culture within Commonwealth entities, including that:

- the Protective Security Policy Framework (PSPF) be amended to reflect or incorporate the behaviours and practices framework, including for auditing purposes, to maximise alignment between the PSPF and the ANAO's audit framework; and

- a dedicated section be created within the annual PSPF self-assessment questionnaire addressing the ANAO's 13 behaviours and practices that facilitate a cyber resilience culture.

Recommendation 4

1.96 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 though 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).

Recommendation 5

2.40 The Committee recommends that Australia Post provide an update on:

- progress in implementing controls in line with the Top Four and other mitigation strategies in the Essential Eight (in confidence, if required); and

- how a cyber resilience culture is being further embedded in the organisation.

Recommendation 6

3.42 The Committee recommends that the Australian Digital Health Agency (ADHA) provide an update on its 'ANAO My Health Record Performance Audit Implementation Plan' (20 February 2020), including:

- key milestones and implementation dates for each of the recommendations in Auditor-General Report No. 13 (2019-20),

Implementation of the My Health Record System, with a particular focus on recommendations 3 and 4; and

- details of the specific changes that ADHA and other stakeholders need to make to implement the recommendations.

1. Introduction

Introduction

1.1 The Joint Committee of Public Accounts and Audit (JCPAA) has a statutory responsibility to examine all reports of the Auditor-General presented to the Australian Parliament.[1]

About the Inquiry

1.2 On 5 February 2020, the Committee resolved to conduct an inquiry into cyber resilience based on the following Auditor-General Reports:

- No. 1 (2019-20), *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*
- No. 13 (2019-20), *Implementation of the My Health Record System*

Inquiry Conduct

1.3 On 7 February 2020, the Committee issued a media release announcing the inquiry and inviting submissions. The Committee also invited submissions from the audited agencies. The inquiry received ten submissions, as listed at Appendix A.

1.4 Public hearings were held on 19 May 2020 and 2 July 2020. A list of witnesses and organisations is at Appendix B.

1.5 A copy of this report, transcripts of public hearings and submissions received are available at the Committee's website at www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit.

[1] Section 8(1)(c), *Public Accounts and Audit Committee Act 1951*.

Report Outline

1.6 Chapter 1 provides background on the inquiry. It also considers the Australian Government cyber security regulatory framework for Commonwealth entities, as matters relating to this area are relevant to both Audit Report No. 1 (2019-20) and Audit Report No. 13 (2019-20). At the time of the Committee's inquiry, the Australian National Audit Office (ANAO) was conducting an audit on cyber security strategies of non-corporate Commonwealth entities. The proposed audit criteria included examining whether 'the three entities responsible for cyber policy in the Commonwealth (the Australian Signals Directorate, the Attorney-General's Department and the Department of Home Affairs) have worked together to support accurate self-assessment and reporting by non-corporate Commonwealth entities, and to improve those entities' implementation of cyber security requirements under the Protective Security Policy Framework'.[2] As this audit was not completed concurrent with the Committee's inquiry, this report does not consider the findings of the audit.

1.7 Chapter 2 considers Audit Report No. 1 (2019-20), which assessed the effectiveness of management of cyber security risks by the Australian Postal Corporation, the Reserve Bank of Australia and ASC Pty Ltd.

1.8 Chapter 3 considers Audit Report No. 13 (2019-20), which assessed the effectiveness of implementation of the My Health Record system under the opt-out model by the Australian Digital Health Agency and the Department of Health.

Cyber Security Framework

1.9 Three Commonwealth entities have oversight responsibilities for cyber security—the Department of Home Affairs (Home Affairs); the Attorney-General's Department (AGD); and the Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC), within ASD.

1.10 Home Affairs is responsible for 'Australia's cyber policy coordination and setting the strategic direction of the government's cyber effort'.[3]

1.11 AGD is responsible for setting Australian Government protective security policy guidance.[4] AGD produces the Protective Security Policy Framework

[2] ANAO website <www.anao.gov.au/work/performance-audit> See also ANAO, *Submission 6.1*, p. 2.

[3] Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy Division, Home Affairs, *Committee Hansard*, 2 July 2020, p. 6.

(PSPF). The core requirements for information security are set out in policies 8 to 11 of the PSPF.[5] An October 2018 Directive reiterated the requirement for 'all non-corporate Commonwealth entities to apply the PSPF as it relates to their risk environment', with the PSPF representing 'better practice for corporate Commonwealth entities and wholly-owned Commonwealth companies'.[6]

1.12 The ACSC, within ASD, leads the Australian Government's operational cyber security capability.[7] The ACSC produces the Australian Government Information Security Manual (ISM), which is referenced in the PSPF as the key source of guidance for Commonwealth entities in applying policies 10 and 11. The PSPF requires non-corporate Commonwealth entities to implement four mitigation strategies (known as the Top Four) of eight essential mitigation strategies (known as the Essential Eight), as referenced in the ISM.

1.13 The *Commonwealth Cyber Security Posture in 2019: Report to Parliament* provides information on Commonwealth entities' cyber resilience in an aggregated form, based on information obtained through the ASD annual cyber security survey and 2018-19 PSPF maturity reporting, combined with the results of the whole-of-government Cyber Uplift.[8] The Cyber Uplift aims to 'strengthen the cyber security of Australian Government networks through enhanced technical guidance, improved verification, and increased transparency and accountability'.[9] The Cyber Uplift included ACSC teams conducting 'sprint' programs to assess and improve the cyber maturity of 25 Commonwealth entities in implementing the Essential Eight, and the creation of an ongoing forum for Chief Information Officers and Chief Information Security Officers from across entities (the CIO/CISO forum).[10]

---

[4] AGD, *Submission 7*, p. 1.

[5] PSPF Policy 8, 'Sensitive and classified information'; PSPF Policy 9, 'Access to information'; PSPF Policy 10, 'Safeguarding information from cyber threats'; and PSPF Policy 11, 'Robust ICT systems'—see AGD website, <www.protectivesecurity.gov.au>.

[6] 'Directive on the Security of Government Business', Attorney-General, October 2018—AGD website, <www.protectivesecurity.gov.au/PSPF annual reporting>.

[7] AGD, *Submission 7*, p. 1.

[8] *Commonwealth Cyber Security Posture in 2019: Report to Parliament*, March 2020, p. 4.

[9] *Commonwealth Cyber Security Posture in 2019: Report to Parliament*, March 2020, p. 5.

[10] *Commonwealth Cyber Security Posture in 2019: Report to Parliament*, March 2020, p. 5.

1.14 Each Commonwealth entity must complete the ASD annual cyber security survey and report any significant or reportable security incident at the time they occur to AGD.[11] Under the PSPF, non-corporate Commonwealth entities are also required to 'submit annual reports to their portfolio minister and AGD, detailing their implementation of PSPF requirements', including the Essential Eight.[12] As part of the 2018 PSPF reforms, annual reporting has now shifted from a compliance-based assessment model to a new maturity self-assessment model, based on a risk management approach.

Regulatory Framework Overview

1.15 Auditor-General Report No. 38 (2019-20), *Interim Report on Key Financial Controls of Major Entities* (28 May 2020), included a review of the self-assessed level of compliance with mandatory cyber security controls of 18 Commonwealth entities.[13] In its submission to the inquiry, the ANAO noted that 'the maturity levels for the majority of the entities reviewed were below the required PSPF … level of "Managing"', with 'one rated as achieving a "Managing" maturity level across all mandatory controls'.[14]

1.16 Since 2013-14, there have been five cyber based audits:

- Auditor-General Report No. 50 (2013-14), *Cyber Attacks: Securing Agencies' ICT Systems*
- Auditor-General Report No. 37 (2015-16), *Cyber Resilience*
- Auditor-General Report No. 42 (2016-17), *Cybersecurity Follow-up Audit*
- Auditor-General Report No. 53 (2017-18), *Cyber Resilience*
- Auditor-General Report No. 1 (2019-20), *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*[15]

1.17 In terms of its four cyber audits of 14 non-corporate Commonwealth entities, the ANAO identified that 'four entities (29 per cent) had complied with mandatory PSPF requirements for information security (Top Four mitigation

[11] Home Affairs, *Submission 10*, p. 1.

[12] AGD, *Submission 7.1*, p. 1.

[13] Auditor-General Report No. 38 (2019-20), *Interim Report on Key Financial Controls of Major Entities*, pp. 29-32. See also ANAO, *Submission 6.1*, pp. 5-6.

[14] ANAO, *Submission 6.1*, p. 6. From 2018-19, Commonwealth entities have reported on their PSPF compliance using a maturity model. There are four maturity levels: Ad hoc; Developing; Managing; and Embedded—Maturity Level Three, 'Managing', is achieved where an entity has implemented all Top Four strategies, p 6.

[15] ANAO, *Submission 6.1*, p. 1.

strategies)'.[16] With regard to the five audits, the ANAO stated that 'Australian Government entities' compliance with mandatory requirements of the … PSPF for information security remained low, and that the regulatory framework had not driven sufficient improvement in cyber security'.[17]

1.18 The Auditor-General noted at the 19 May 2020 public hearing that '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'.[18] However, the Auditor-General added that 'there has been a new framework put in place which has additional oversight arrangements and that may be more successful, but we are not in a position to comment on that yet'.[19] As the Auditor-General also observed, 'more recently there have been changes to the framework to try and improve that assessment':

> ASD has been running what they call 'sprint tests' across a number of entities, where they come in and do a detailed review of compliance … while we haven't finished auditing in that space, that is a step forward in the overarching framework and in the quality of review work that is going on … … …
>
> [I]f you look at the evidence from our audits, one conclusion we can draw is that the framework that was in place wasn't driving the behavioural change to ensure that the regulatory stance was robust enough. Since that time there have been changes in that stance with respect to the provision of information, more review. Some moved to verification type processes; that is an area that could be stronger … … …
>
> Internally, within government, I think that when we started down this path there was very little oversight of the internal compliance reporting with respect to the whole of the PSPF … through time, the transparency and oversight of that internal reporting has become stronger, and that's part of the change in the framework in the last year or so. There has been a bit more oversight of those things.[20]

---

[16] ANAO, *Submission 6.1*, p. 2.

[17] ANAO, *Submission 6.1*, p. 1.

[18] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 13.

[19] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 13.

[20] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 13, p. 14, p. 15.

1.19 At the 2 July 2020 public hearing, the Auditor-General further noted that 'we haven't really done an assessment of the technical supporting of the self-assessment framework, particularly since the new framework was established last year'.[21]

1.20 Asked about the regulatory framework, AGD stated that it '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', with reforms to the PSPF also having been 'made in 2018'.[22] As to whether further development of the regulatory framework was required to drive improvements in cyber security, AGD highlighted that 'part of the reforms to the broad PSPF … and particularly the changes to maturity reporting, are designed to better support that continuous improvement':

> We work with the ACSC on that particular technical and practical support to agencies to lift cybersecurity resilience as well. In the future, we're looking to add to the maturity reporting moderation models … Clearly, there's variability, as reflected in the cybersecurity posture report, and there are definitely areas where agencies need to do better in lifting their cybersecurity performance. By no means do we think the framework is a failure, but we will continue to work to improve cybersecurity posture.[23]

1.21 AGD provided additional information on some of the PSPF reforms, including that 'we have the first results that we're compiling from 2018-19 maturity reporting under the reformed PSPF. That will provide a more comprehensive nuanced view of cybersecurity posture and a lot more information for us to consider'.[24] In addition, ASD outlined the roles of the Cyber Uplift program, as well as the 'sprint' program and the CIO/CISO forum.[25] ASD noted that the 'sprints' informed 'a heightened awareness amongst all 25 agencies of the Essential Eight, a better practical understanding of how to apply measures and, certainly, an increased and alert posture'.[26] AGD further outlined that, 'in administering the Cyber

---

[21] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 2 July 2020, p. 13.

[22] AGD, *Submission 7.2*, p. 3.

[23] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 9.

[24] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 2.

[25] Ms Abigail Bradshaw, Head, ACSC, ASD, *Committee Hansard*, 2 July 2020, p. 7.

[26] Ms Abigail Bradshaw, Head, ACSC, ASD, *Committee Hansard*, 2 July 2020, p. 7.

Security Response Fund, which is that after-care, we have now provided additional services to those 25 core agencies to improve specific elements that were identified in the uplift and upped their maturity model'.[27] Home Affairs also pointed to its 'continuing to work on the Cyber Security Strategy', noting that 'we see a cybersecurity uplift within government as a key component of that strategy'.[28]

1.22 As to whether these initiatives would see an increase in entity compliance with the mandatory requirements of the PSPF, with this being reflected in future cyber audits, AGD observed that 'the intent of the changes we made to the PSPF and the approach to maturity reporting is that we expect it will provide a framework that will support greater improvement'.[29] Similarly, ASD emphasised, with reference to the *2019 Commonwealth Cyber Security Posture*, that there was 'evidence of continual improvement, although an acceptance that additional work would be required'—in particular, 'there was an improvement in comparison to previous years of … implementation of the Essential Eight'.[30]

1.23 The *2019 Commonwealth Cyber Security Posture* stated that 'baseline adoption of the Essential Eight across the Australian Government still requires further improvement' and 'entities' self-assessed implementation of the Top Four remains at low levels across the Australian Government', with '73 per cent of non-corporate Commonwealth entities reporting ad hoc or developing levels of maturity'.[31] AGD noted that, as outlined in the *2019 Commonwealth Cyber Security Posture*, 'the overall cyber security of Australian Government agencies continued to improve through:

- increased capability to identify cyber security events and incidents;

---

[27] Ms Jessica Hunter, Acting First Assistant Director-General, Protect, Assure and Enable, ASD, *Committee Hansard*, 2 July 2020, p. 8. ASD indicated that it would continue to conduct similar Cyber Uplift initiatives 'as part of the $1.35 billion … investment in cyber security recently announced by the Prime Minister', ASD, *Submission 9*, p. 8.

[28] Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy Division, Home Affairs, *Committee Hansard*, 2 July 2020, p. 4. See, for example, *Australia's Cyber Security Strategy 2020*, August 2020.

[29] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 4.

[30] Ms Abigail Bradshaw, Head, ACSC, ASD, *Committee Hansard*, 2 July 2020, p. 3. See also Minister for Defence, 'the [Commonwealth Cyber Security Posture] Report highlights that the overall cyber security of Commonwealth entities continues to improve', *Submission 8*, p. 1.

[31] *Commonwealth Cyber Security Posture in 2019: Report to Parliament*, March 2020, p. 9, p. 10.

- 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.[32]

1.24 The *2019 Commonwealth Cyber Security Posture* stated that 'Commonwealth entities continue to improve their cyber security'; 'in 2019, implementation of the Essential Eight across Commonwealth entities improved slightly in comparison to previous years'; and 'the Cyber Uplift program has improved entities' cyber security posture'.[33] Further, to assist entities in strengthening their cyber security, AGD noted that 'the Australian Government has made a substantial investment in the capabilities of the ASD and 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'.[34]

1.25 As announced on 30 June 2020, the Australian Government is investing $1.35 billion over the next decade through the Cyber Enhanced Situational Awareness and Response package, to enhance the cyber security capabilities, working through ASD and the ACSC.[35] As to how this initiative would improve compliance with the mandatory Top Four, ASD responded:

> by having a much better national picture of the threat—and with the fact that the threat changes the types of vectors or the type of technology being used—enabling us to send that message to all government agencies, who are all ACSC partners and recipients of our advice, much more quickly and hopefully with much more scale and technical detail, it would … have a positive impact on the resilience of government agencies … uplifting awareness, whether that's through more or better quality advice, assists all Commonwealth agencies and broader government to lift their cybersecurity hygiene … it's directed at ASD so that we can give better advice to government and the whole of economy to improve cyberhygiene writ large, which includes the capacity, through our advice and our assistance, of government agencies as

[32] AGD, *Submission 7.2*, p. 1.

[33] *Commonwealth Cyber Security Posture in 2019: Report to Parliament*, March 2020, p. 9, p. 11.

[34] AGD, *Submission 7.2*, p. 1.

[35] 'Cyber Enhanced Situational Awareness and Response package', Media statement, Prime Minister, Minister for Home Affairs, Minister for Defence, 30 June 2020.

> well as individuals and small businesses to implement the mandatory four and the Essential Eight.[36]

1.26 Another matter discussed was the June 2020 cyber incident,[37] and specific actions to drive improvements in entity compliance with mandatory cybersecurity requirements since that incident. ASD explained 'the advice that we've given and the engagement that we've had with agencies occurred both in the lead-up to the Prime Minister's statement and subsequently', and that includes 'working with every agency that may have been targeted', including 'giving specific measures of care, both technical and advisory, to agencies, not only when they have been targeted but to those that we anticipate might be at a higher level of risk because of the risk environment at the moment'.[38]

1.27 A further matter discussed at the public hearing was enforcement of compliance. Since 2018-19, entities have reported on their PSPF compliance using a maturity model, including self-assessment of their implementation level of the Top Four mitigation strategies.[39] As AGD explained, '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 this 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 position 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.[40]

---

[36] Ms Abigail Bradshaw, Head, ACSC, ASD, *Committee Hansard*, 2 July 2020, p. 20.

[37] 'Statement on malicious cyber act against Australian networks', Media statement, Prime Minister, Minister for Home Affairs, Minister for Defence, 19 June 2020.

[38] Ms Abigail Bradshaw, Head, ACSC, ASD, *Committee Hansard*, 2 July 2020, p. 10.

[39] There are four maturity levels: Ad hoc; Developing; Managing; and Embedded. Maturity Level Three, 'Managing', is achieved where an entity has implemented all Top Four strategies, ANAO, *Submission 6.1*, p. 6.

[40] AGD, *Submission 7.2*, p. 5. As to any differences between the way that a Commonwealth entity self-assesses compliance with the Top Four mitigations and the way that the ANAO assesses this

1.28 AGD stated that maturity model reporting should 'considerably improve the quality of the information we have on agencies' protective security posture generally'—'we're conscious that we've just had the first year of maturity reporting and are now looking at how we can improve building on the results we got from this year'.[41] AGD provided information on how these new arrangements were communicated to entities, including through guidance material and workshops.[42]

1.29 Asked whether there might be scope for a greater focus on enforcement of compliance with the Essential Eight, AGD responded: 'we have already flagged, as part of the government Security Committee … that we want to work on arrangements that would add to that self-assessment moderation option to check agencies' ratings and support them as part of that assessment process. That is something we have in our work program at the moment'.[43] The department further observed that it was exploring an 'external moderation or benchmarking process', to enable comparison between entities—'whether we do it with agencies cross-assessing each other or having central arrangements going in and assessing or moderating agencies' results is something we're working through'.[44] In providing further information about its response to a previous audit recommendation that AGD, Home Affairs and ASD work together to improve compliance with the PSPF by developing a program for verifying entities' reported compliance with mandatory cybersecurity requirements,[45] AGD similarly noted that it was 'exploring moderation models that could be adopted as part of the PSPF to moderate or review entities' security assessments for

matter as part of an audit, the Auditor-General stated that, 'in terms of the substance of testing, the criteria are the same … we're looking at whether the mandatory four are implemented. So there is no substantive difference, I don't think, in that', Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 14.

[41] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 13.

[42] Ms Liz Brayshaw, Assistant Secretary, Security Law and Policy Branch, AGD, *Committee Hansard*, 2 July 2020, pp 13-14.

[43] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 13.

[44] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 14.

[45] Auditor-General Report No. 53 (2017-18), *Cyber Resilience*, p. 8.

different PSPF requirements. This includes consideration of moderation models that include peer review, benchmarks or other arrangements'.[46]

1.30 AGD emphasised that the PSPF places particular responsibility, aligned with the PGPA Act, on the accountable authority (agency and department heads) to 'make decisions about the implementation of all of those requirements, and they're accountable for reporting on them, as well as compliance'.[47] On this point, the Auditor-General stated:

> there's been lots of commentary about how, under our framework, the accountable authority from an entity is responsible for the implementation of the policy, which is absolutely correct, but I think a key part of an accountability framework … is that the owner of the policy also needs to take responsibility for whether the policy is successful.[48]

1.31 Asked whether there might be a role for a more centralised approach, Home Affairs responded:

> One of the things that the Commonwealth is looking at is: how do you build aggregation, how do you look at scaling a response and how do you support agencies who might have less capability in terms of cybersecurity, even though they've got their own individual responsibilities? How do you actually build capacity across a large Commonwealth set of networks and a complicated network? … Despite the fact that agencies are responsible for their own cybersecurity, the government is actively looking at a whole range of different options and is actively continuing to look at its own cybersecurity posture from a policy perspective, from a protective security perspective, from an operational perspective and from support to industry and the whole-of-nation effort.[49]

1.32 At the time of the Committee's inquiry, the ANAO was conducting an audit on cyber security strategies of non-corporate Commonwealth entities.[50] The proposed audit criteria included examining whether 'the three entities

---

[46] AGD, *Submission 7.2*, p. 6.

[47] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 6.

[48] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 2 July 2020, p. 14.

[49] Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy Division, *Home Affairs*, Committee Hansard, 2 July 2020, pp. 18-19.

[50] As this audit was not completed concurrent with the Committee's inquiry, this report does not consider the findings of this audit. (JCPAA Report 467, *Cybersecurity Compliance*, recommended that 'the Auditor-General consider conducting an audit of the effectiveness of the self-assessment and reporting regime under the PSPF' (October 2017), p. vii.)

responsible for cyber policy in the Commonwealth (ASD, AGD and Home Affairs) have worked together to support accurate self-assessment and reporting by non-corporate Commonwealth entities, and to improve those entities' implementation of cyber security requirements under the PSPF'.[51] As the Auditor-General further explained at the public hearing:

> we haven't really done an assessment of the technical supporting of the self-assessment framework, particularly since the new framework was established last year. The audit we're undertaking at the moment is going to that, to some degree, because a key part of the changes that happened was to change the self-assessment framework and to put in place some arrangements to assist agencies to develop that.[52]

Cyber Security and Organisational Culture

1.33 The Auditor-General outlined that audit reports over time had provided insights into why some Commonwealth entities have more compliant frameworks than others, including an emphasis on cyber resilient culture:

> broadly, what we identify is around the prioritisation and culture developed from the leadership of organisations. Where you see a strong focus within organisations on developing cyber-resilience and a willingness to privilege investment in that area, investing in the infrastructure needed to provide greater cyber-resilience, it happens. If it's lower down the priority lists of an entity, it doesn't happen.[53]

1.34 ASD similarly noted that the *2019 Commonwealth Cyber Security Posture* emphasised 'the importance of progressing cybersecurity culture to improve the cybersecurity posture', with it being 'critical that good cybersecurity practices become part of core business'.[54] ASD has a 'range of services dedicated to supporting and improving cybersecurity culture within organisations', including through its cyber security survey.[55]

---

[51] ANAO website <www.anao.gov.au/work/performance-audit> See also ANAO, *Submission 6.1*, p. 2.

[52] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 2 July 2020, p. 13.

[53] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 2 July 2020, p. 5. See also on this point Mr Hehir, *Committee Hansard*, 19 May 2020, p. 21.

[54] Ms Jessica Hunter, Acting First Assistant Director-General, Protect, Assure and Enable, ASD, *Committee Hansard*, 2 July 2020, p. 16.

[55] Ms Jessica Hunter, Acting First Assistant Director-General, Protect, Assure and Enable, ASD, *Committee Hansard*, 2 July 2020, p. 16.

1.35 ASD also seeks to 'change the cybersecurity culture' through updating its ISM on a monthly basis 'to ensure that organisations consider cybersecurity as a hygiene component rather than a docking endpoint once a year', and by providing 'additional advice and guidance' through the CIO forums.[56]

1.36 AGD also stated that 'we think cybersecurity culture … is very important, and we've done a number of things to support improvements in culture', such as the Security Culture Community of Practice, regular CISO newsletter, biannual CIO/CISO forums and sharing of 'best practice', including the development of 'a cultural transformation strategy' to build a stronger protective security culture.[57]

1.37 Home Affairs further commented that, 'in the four years since the 2016 Cyber Security Strategy and the establishment of the Australian Cyber Security Centre in 2013, there has been a broader cultural recognition of cybersecurity more generally across government', particularly through:

> the level of engagement, the level of awareness across government of cybersecurity issues, the collaborations we've seen in some of the forums … and even on a policy level, the colocation of the Home Affairs policy team with the operational activities in the Australian Cyber Security Centre, we sit side by side. So even at a policy level, the connectivity between operations and policy is there on a day-to-day basis … the secretaries board's awareness of the issues continues to mature.[58]

Auditor-General Report No. 1 (2019-20)

1.38 Chapter 4 of Auditor-General Report No. 1 (2019-20) focused on whether the entities examined had a culture of cyber resilience by assessing performance against 13 behaviours and practices under four key headings:

- Governance and risk management
- Roles and responsibilities
- Technical support
- Monitoring compliance

---

[56] Ms Jessica Hunter, Acting First Assistant Director-General, Protect, Assure and Enable, ASD, *Committee Hansard*, 2 July 2020, p. 16.

[57] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 11, p. 16.

[58] Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy Division, Home Affairs, *Committee Hansard*, 2 July 2020, pp. 16-17.

1.39 The 'Governance and risk management' section included examination of the role of leadership from senior executives in prioritising cyber security, and the role of governance, audit and risk committees in reviewing vulnerabilities and staff security awareness.[59]

1.40 'Roles and responsibilities' included discussion of core security roles such as the Chief Information Security Officer within each entity.[60]

1.41 'Technical support' included assessing whether each entity had established a Cyber Incident Response Plan.[61]

1.42 The final section on 'Monitoring compliance' assessed whether entities were aligning with cyber security requirements, including through the engagement of external parties to validate internal reports.[62]

1.43 The ANAO assessed each entities performance against these criteria, and through reference to the Top Four strategies.

ANAO Submission 6.1

1.44 In its submission to the inquiry, the ANAO outlined key features of a cyber resilience culture. This involves the development of shared attitudes, behaviours and practices, and includes establishing effective Information and Communication Technology (ICT) general controls.[63] These controls provide a strong foundation for the development of further controls and in turn the implementation of the Top Four cyber security risk mitigation strategies contained in the ISM.[64]

Cyber Resilience and the ANAO's 13 Behaviours and Practices

1.45 The Auditor-General outlined that cyber-resilience is an agency's ability 'to continue providing services while deterring and responding to a cyber intrusion' and that 'resilience goes more to the cultural aspect and the

[59] Auditor-General Report No. 1 (2019-20), pp. 38-39.

[60] Auditor-General Report No. 1 (2019-20), p. 40.

[61] Auditor-General Report No. 1 (2019-20), p. 41.

[62] Auditor-General Report No. 1 (2019-20), p. 42.

[63] ANAO, *Submission 6.1*, p. 1.

[64] ANAO, *Submission 6.1*, p. 1.

broader frameworks in place' rather than testing of controls and cybersecurity measures.[65]

1.46 The ANAO's 13 behaviours and practices that may indicate a cyber resilience culture were identified through a 'review of relevant guidance, reports and consultation with policy and audited entities'.[66] The ANAO noted that this framework 'can be used to measure culture, but this does not necessarily mean that an organisation that exhibits these behaviours is cyber resilient'.[67]

1.47 The ANAO further stated that:

> having a good culture helps achieve compliance. The behaviours should be read in context with our assessment against the PSPF Policy 10 requirements and IT general controls … which are the other factors that were considered by ANAO for assessing cyber resilience.[68]

1.48 The 13 behaviours and practices were first published in Auditor-General Report No. 53 (2017-18).[69] These include:

Governance and risk management

1 Establish a business model and ICT governance that incorporates ICT security into strategy, planning and delivery of services.

2 Manage cyber risks systematically, including through assessments of the effectiveness of controls and security awareness training.

3 Task enterprise-wide governance arrangements to have awareness of cyber vulnerabilities and threats.

4 Adopt a risk-based approach to prioritise improvements to cyber security and to ensure higher vulnerabilities are addressed.

[65] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 12.

[66] ANAO, *Submission 6.2*, p. 2. The ANAO provided further information about the guidance, reports and organisations consulted, pp. 1-2. (The ANAO's framework reflected a recommendation of JCPAA Report No. 467, *Cybersecurity Compliance*, that, in future audits on cybersecurity compliance, the ANAO 'outline the behaviours and practices it would expect in a cyber resilient entity and assess against these', October 2017, p. viii.)

[67] ANAO, *Submission 6.2*, p. 1.

[68] ANAO, *Submission 6.2*, p. 1.

[69] Auditor-General Report No. 53 (2017-18), *Cyber Resilience*.

Roles and responsibilities

5 Assign information security roles to relevant staff and communicate the responsibilities.

6 Develop the capabilities of ICT operational staff to ensure they understand the vulnerabilities and cyber threats to the system.

7 Ensure management understand their roles and responsibilities to enhance security initiatives for the services for which they are accountable. This includes senior management understanding the need to oversight and challenge strategies and activities aimed at ensuring the entity complies with mandatory security requirements.

8 Embed security awareness as part of the enterprise culture, including expected behaviours in the event of a cyber incident.

9 Assign data ownership to key business areas, including the role to classify the data, and grant or revoke access to shared data by other entities.

Technical support

10 Develop and implement an integrated and documented architecture for data, systems and security controls.

11 Identify and analyse security risks to their information and system, including documenting ICT assets requiring protection.

12 Establish a Cyber Incident Response Plan, informed by a comprehensive risk assessment and business continuity plan, including a priority list of services (not ICT systems) to be recovered.

Monitoring compliance

13 Develop an approach to verify the accuracy of self-assessments of compliance with mandatory cyber security requirements.[70]

Measuring a Cyber Resilience Culture

1.49 Evidence taken in public hearings from lead policy entities highlighted that they found culture hard to empirically assess. In response to a question from the Committee regarding the whether culture could be measured, Home Affairs observed that 'culture is really difficult to measure. But one thing you can do is put forward vignettes about where things are working … You

[70] Auditor-General Report No. 1 (2019-20), pp. 38-42.

look at how departments of state and agencies are making changes and you can look at the culture within agencies'.[71] Similarly, AGD agreed that:

> it is very hard to empirically measure culture. But one thing that agencies do that we do in Attorney-General's Department is annual protective security training for staff … We have often asked staff to complete a series of questions that also measure the extent to which they fully appreciate the range of their protective security obligations, which … is not a perfect measure of culture but contributes to an assessment.[72]

Cyber Resilience Culture and the PSPF

1.50 The PSPF focuses broadly on assisting government entities to protect their people, information and assets through the key areas of security governance; information security; personnel security; and physical security.[73] It details how accountable authorities should encourage collective responsibility among personnel, and outlines that the Chief Security Officer should provide leadership in the area of organisational culture.[74]

1.51 The PSPF also sets out a number of aspects that indicate a 'positive security culture', including that security is prioritised by leadership; risks are identified and managed; security awareness training is implemented for personnel and contractors; incidents and breaches are managed appropriately; and security improvements are encouraged within the agency.[75]

1.52 The PSPF does not provide reference to the 13 behaviours and practices identified by the ANAO as assisting in the establishment of a cyber resilient culture.

1.53 In its submission, AGD stated that, 'while the 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

---

[71] Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy Division, Home Affairs, *Committee Hansard*, 2 July 2020, p. 17.

[72] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 17.

[73] PSPF, 'Management structures and responsibilities' (v2020.1), pp. 5-6.

[74] PSPF, 'Management structures and responsibilities', (v2020.1), p. 12.

[75] PSPF, 'Management structures and responsibilities', (v2020.1), p. 12.

the ANAO's framework'.[76] As to whether the ANAO's framework might be used by entities as a guide, AGD responded:

> 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.[77]

1.54 At the public hearing, the ANAO outlined that, whilst it is not their role to mandate which framework should be utilised, it was clear that the framework currently being used 'wasn't driving the behavioural change to ensure the regulatory stance was robust enough'.[78]

1.55 In explaining how the ANAO had addressed this matter in its reporting, the Auditor-General stated that 'normally we audit against the framework set by regulators. In this case there isn't one, so we've built a framework that tries to provide through a definition of what a strong resilient culture is through to indicators of those things and then measures of them'.[79] As the Auditor-General further explained:

> What we're trying to look at in our reporting is what agencies are doing to become cyber resilient. A key focus of that is given that mandatory arrangements are a minimum standard, you would expect to see compliance. After that we look at what are the cultural aspects that build resilience? … It goes to elements that we've identified for developing an effective culture through the governance and risk framework, the roles and responsibilities being clear, the technical support arrangements and monitoring and compliance. We've built this framework so that we can build a measure or an indicator of the strength of the organisation's resilience, which is driven by

[76] AGD, *Submission 7.2*, p. 1. By way of example, AGD noted that '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', p. 1.

[77] AGD, *Submission 7.2*, pp. 10-11.

[78] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 14.

[79] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 2 July 2020, p. 17.

> culture. If you don't have a go at measuring it or defining it in a way that is measurable, it actually doesn't add much value to the conversation. To say culture is important but not what that means is not a very valuable thing to contribute.[80]

1.56 The ANAO elaborated that the 13 behaviours and practices were developed to test whether organisational leadership goes beyond simply instructing personnel on security measures to embedding cyber resilience into the 'day-to-day management and practices of the entity'.[81]

Top Four and Essential Eight Implementation

1.57 Under the PGPA Act, non-corporate Commonwealth entities are required to apply the PSPF, which states that they must mitigate common and emerging cyber threats. The framework mandates that non-corporate Commonwealth entities implement the Top Four cyber security mitigation strategies detailed in the ISM. These four mandatory strategies, in combination with a further four non-mandatory strategies, are known as the Essential Eight. It is not mandatory for GBEs and corporate Commonwealth entities to apply the PSPF or the ISM, including the Top Four. However, the PSPF and the ISM currently represent 'better practice' for such entities.[82]

1.58 JCPAA Report 467, *Cybersecurity Compliance*, recommended that the Australian Government mandate the ASD's Essential Eight cybersecurity strategies for all PGPA Act entities, by June 2018.[83] The Government response to this recommendation stated that 'the Government will consider mandating the Essential Eight when cyber security maturity has increased across entities'.[84]

1.59 Asked at the public hearing whether cyber security maturity had increased across entities since the Committee made its recommendation, AGD explained that the 'reporting model' under the PSPF had changed, 'so we can't compare the 2017-18 reporting directly with the reporting we got from

---

[80] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 2 July 2020, p. 17.

[81] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 17.

[82] 'Directive on the Security of Government Business', Attorney-General, October 2018—AGD website, <www.protectivesecurity.gov.au/PSPF annual reporting>.

[83] JCPAA Report 467, *Cybersecurity Compliance*, October 2017, p. vii.

[84] Australian Government, Response to JCPAA Report 467, April 2019, p. 5.

2018-19'.[85] However, AGD observed 'we do have information to indicate that there have been improvements, that there's clearly still room for more improvement and that there is variability across agencies'.[86] As to whether, consistent with the Government response, there would be consideration given to mandating the Essential Eight when cyber security maturity had increased across entities, AGD stated that:

> the issue of mandating all Essential Eight mitigations in the PSPF remains under consideration by AGD having regard to cyber security maturity levels across entities and ASD's technical advice … 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.[87]

1.60 In terms of the rationale for only the Top Four of the Essential Eight mitigation strategies being mandatory, ASD explained that 'decisions around what's mandatory and what's not are policy decisions'.[88] ASD further observed that the focus on the mandatory Top Four is 'informed by technical advice, and our technical advice is that those Top Four provide the greatest defence and are of greatest import'.[89] Similarly, AGD stated that 'from the perspective of the policy decision to have the Top Four as mandatory and then asking agencies to assess themselves … against the Essential Eight ... We consider that approach, with ASD and Home Affairs, as appropriate at this time'.[90] As ASD further advised, 'at this point we feel it is most focused and prioritised to have the policy reflect the mandatory requirements of the Top Four and not to do that for the full Essential Eight or indeed beyond that'.[91]

---

[85] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 11.

[86] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 11.

[87] AGD, *Submission 7.2*, p. 2.

[88] Ms Abigail Bradshaw, Head, ACSC, ASD, *Committee Hansard*, 2 July 2020, p. 5.

[89] Ms Abigail Bradshaw, Head, ACSC, ASD, *Committee Hansard*, 2 July 2020, p. 5.

[90] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 5.

[91] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 5.

1.61 As to why it is not mandatory for GBEs and corporate Commonwealth entities to apply the Top Four mitigation strategies, the Auditor-General observed:

> it's not uncommon within the Commonwealth public sector that mandated rules from the centre apply to the non-corporate sector but not to all of the corporate sector. You'll find that across a lot of areas like procurement, grants and in the PSPF. We'd think that there probably could be more consistency in how those frameworks are put in place … whether a dividing line of corporate is the right one is something that we've raised in other spaces.[92]

Transparency and Accountability to the Australian Parliament

1.62 JCPAA Report 467, *Cybersecurity Compliance*, recommended that AGD and ASD report annually on the Commonwealth's cyber security posture to the Parliament.[93] The *Commonwealth Cyber Security Posture in 2019: Report to Parliament* responds to this recommendation.[94]

1.63 The *2019 Commonwealth Cyber Security Posture* states that 'identifying the cyber security posture or vulnerabilities of individual Commonwealth entities may increase their risk of being targeted by malicious cyber actors. This Report, therefore, does not identify specific entities—all data has been anonymised and provided in aggregate'.[95] As ASD observed, the *2019 Commonwealth Cyber Security Posture* 'includes aggregated results of the status on the Commonwealth's cyber security posture … ASD does not identify the cyber security posture or vulnerabilities of individual Commonwealth entities as this may increase their risk of being targeted by malicious cyber actors'.[96] AGD similarly noted that having publicly available details on cybersecurity vulnerabilities 'itself creates a vulnerability, and the purpose of the cybersecurity posture report is to provide that information at

[92] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 12.

[93] JCPAA Report 467, *Cybersecurity Compliance*, October 2017, p. viii.

[94] *Commonwealth Cyber Security Posture in 2019: Report to Parliament*, March 2020, p. 4.

[95] *Commonwealth Cyber Security Posture in 2019: Report to Parliament*, March 2020, p. 4.

[96] ASD, *Submission 9*, p. 4.

a non-detailed entity level for members of parliament and others. Clearly, the ANAO report provides some level of information as well on entities'.[97]

1.64 In terms of individual Commonwealth entities being held accountable to the Australian Parliament for their compliance with mandatory cybersecurity measures, AGD advised that this 'might require classified forums with security classified, in-confidence arrangements … the issue with providing detail publicly on specific agencies' cybersecurity arrangements and potential vulnerabilities is that it could make them more vulnerable to cyber threat'.[98] AGD further stated that 'we understand parliamentary committees can make arrangements to receive information in private having regard to the requirements of security'.[99] AGD also noted that the 'PSPF mandates that each entity must report on security each financial year to their portfolio minister. AGD provides an annual report to the Attorney-General and publishes a whole of government assessment report on its website'.[100]

1.65 There was interest in how the ANAO takes account of sensitivities regarding the amount of detail provided in audit reports on the cyber resilience of audited entities. The Auditor-General explained that:

> Our methodology for dealing with that in the cyberspace is the same as we use for all security type information. We prepare reports that, in the first instance, include all the details of our findings. We provide it to the entity and then have a discussion with them about where they see security type issues. We usually work through to an agreed conclusion as to the level of detail that we disclose … We tend to take a collaborative stance on it. In general, my position would be that if an agency raised significant concerns, we wouldn't disclose.[101]

1.66 On this matter, AGD stated that '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

---

[97] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 15. Similarly, the Minister for Defence stated that the content of the posture report 'balances the need for transparency with the need to carefully protect the security of Government systems', Minister for Defence, *Submission 8*, p. 1.

[98] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 15.

[99] AGD, *Submission 7.2*, p. 8.

[100] AGD, *Submission 7.2*, p. 8.

[101] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 2 July 2020, p. 7. See also Mr Hehir, *Committee Hansard*, 19 May 2020, p. 16.

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'.[102]

Concluding Comment

1.67 Three Commonwealth entities have oversight responsibilities for cyber security—Home Affairs, AGD, and ASD, along with the ACSC. During the inquiry, the Committee received advice about the Australian Government protective security policy framework and guidance, including the PSPF and ISM.

1.68 With regard to the five cyber based audits since 2013-14, the ANAO stated that Australian Government entities' compliance with mandatory requirements of the PSPF for information security 'remained low', and that 'the regulatory framework had not driven sufficient improvement in cyber security'.[103] However, at the public hearings, the Auditor-General noted that 'there has been a new framework put in place which has additional oversight arrangements and that may be more successful, but we are not in a position to comment on that yet',[104] and that 'we haven't really done an assessment of the technical supporting of the self-assessment framework, particularly since the new framework was established last year'.[105]

1.69 On the new framework, AGD stated that 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',[106] and that the recent PSPF reforms and the changes to maturity reporting have been designed to 'provide a framework that will support greater improvement'.[107] AGD provided the Committee with information on the PSPF reforms, including the Cyber Uplift program and accompanying 'sprint' program; the CIO/CISO forums; and the new maturity reporting, which replaces point in time compliance reporting with ongoing monitoring of security maturity

[102] AGD, *Submission 7.2*, p. 7.

[103] ANAO, *Submission 6.1*, p. 1.

[104] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 13, p. 14, p. 15.

[105] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 2 July 2020, p. 13.

[106] AGD, *Submission 7.2*, p. 3.

[107] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 4.

and implementation of PSPF requirements.[108] The Committee further notes the release of the 2020 Cyber Security Strategy and June 2020 Australian Government Cyber Enhanced Situational Awareness and Response package.

1.70 The *2019 Commonwealth Cyber Security Posture* stated that 'baseline adoption of the Essential Eight across the Australian Government still requires further improvement' but noted that 'Commonwealth entities continue to improve their cyber security'.[109]

1.71 At the time of the Committee's inquiry, the ANAO was conducting an audit on cyber security strategies of non-corporate Commonwealth entities. The proposed audit criteria included examining whether 'the three entities responsible for cyber policy in the Commonwealth (ASD, AGD and Home Affairs) have worked together to support accurate self-assessment and reporting by non-corporate Commonwealth entities, and to improve those entities' implementation of cyber security requirements under the PSPF'.[110] As the audit was not completed concurrent with the inquiry, it does not form part of the Committee's report. The Committee will consider the audit findings in due course, and therefore does not make any specific recommendations in this area at this time.

1.72 The Committee understands that AGD is currently exploring external moderation models and benchmarking processes, to verify entities' reported compliance with cybersecurity requirements and enable comparison between entities.[111]

Recommendation 1

1.73 The Committee recommends that the Attorney-General's Department provide an update on its implementation of external moderation models/benchmarking processes, to verify Commonwealth entities' reported compliance with cybersecurity requirements, including implementation timeframes.

---

[108] AGD, *Submission 7.2*, p. 5. 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 position may have changed', p. 5.

[109] *Commonwealth Cyber Security Posture in 2019: Report to Parliament*, March 2020, p. 9, p. 11.

[110] ANAO website <www.anao.gov.au/work/performance-audit> See also ANAO, *Submission 6.1*, p. 2.

[111] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 13 and AGD, *Submission 7.2*, p. 6.

1.74 JCPAA Report 467, *Cybersecurity Compliance*, recommended that the Australian Government mandate the ASD's Essential Eight cybersecurity strategies for all PGPA Act entities, by June 2018.[112] The Government response to this recommendation stated that 'the Government will consider mandating the Essential Eight when cyber security maturity has increased across entities'.[113]

1.75 The Committee heard evidence from AGD, ASD and Home Affairs of increasing cyber security maturity levels throughout this inquiry.

1.76 In light of this, and the increasingly acute cyber security threat environment confronting Commonwealth entities, the Committee considers it appropriate that the Government revisit its response to this recommendation and update the Committee on its intended approach.

Recommendation 2

1.77 The Committee recommends that the Attorney-General's Department:

- **provide an update on the levels of cyber security maturity within Commonwealth entities and the feasibility of mandating the Essential Eight across Commonwealth entities, including the threshold of cyber security maturity required by Government to impose this mandate, and expected timeframes; and**

- **report back on any impediments to mandating the Top Four mitigation strategies for government business enterprises and corporate Commonwealth entities.**

1.78 The Committee notes that the ANAO has identified 13 behaviours and practices as key to a strong cyber resilient culture, and is auditing against this framework.[114] The Committee believes these factors provide a useful indication of the key steps agencies should take in the implementation or improvement of culture.

1.79 It is the Committee's view that there would appear to be no formal framework or implementation plans for the adoption of the 13 behaviours

[112] JCPAA Report 467, *Cybersecurity Compliance*, October 2017, p. vii.

[113] Australian Government, Response to JCPAA Report 467, April 2019, p. 5.

[114] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 2 July 2020, p. 17

and practices the Auditor General has outlined as assisting to establish a cyber resilient culture.

1.80 While the PSPF outlines the importance of fostering a positive security culture, it makes no reference to cyber resilience culture. The PSPF recommends that the maturity of an entity's security culture should be measured, and appropriate metrics should be utilised.[115] However, during the public hearing, it was clear that accountability mechanisms to ensure agencies are complying with the PSPF are limited and that each accountable authority must ensure their own compliance with mandatory frameworks.[116]

1.81 The current accountability framework for the cyber security practices of individual entities under the PSPF was described in evidence to the Committee by AGD:

> The reporting agencies provide [self-assessment reports on compliance with mandatory cybersecurity measures in the PSPF] to their own minister. Obviously, within the agency, it goes to the head of the agency. It has to be provided to their minister, and it's provided centrally as well to the Attorney-General's Department. On cybersecurity, we in turn share that with the ACSC. So it directs our efforts on working with agencies on improvements, but it has been made visible at a ministerial level as well. Then it informs the program of ongoing work to improve cyber-resilience.[117]

1.82 The Committee has long held a strong bipartisan consensus that this government accountability framework be supported by Parliamentary accountability on cybersecurity.

1.83 JCPAA Report 467, *Cybersecurity Compliance*, emphasised that, 'as a strategic priority, it is crucial that Commonwealth entities be accountable to the Australian Parliament' on cybersecurity'.[118]

1.84 On this basis, the Committee recommended that AGD and ASD 'report annually on the Commonwealth's cybersecurity posture to the Parliament, such as through the Parliamentary Joint Committee on Intelligence and Security'.[119]

---

[115] PSPF, 'Management structures and responsibilities' (v2020.1), p. 12.

[116] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 16.

[117] Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group, AGD, *Committee Hansard*, 2 July 2020, p. 12.

[118] JCPAA Report 467, *Cybersecurity Compliance* (October 2017), p. 13.

[119] JCPAA Report 467, *Cybersecurity Compliance* (October 2017), p. 13.

1.85 The Government agreed to this recommendation and in response published the first *Commonwealth Cyber Security Posture* report in 2019. However, the publication of this report highlights the challenges inherent between the benefits of public accountability of the cyber security practices of individual departments and the potential for the publication of vulnerabilities within Commonwealth entities to exacerbate existing security risks. The Government has sought to resolve this tension in the *Commonwealth Cyber Security Posture* report by publishing information on an aggregated basis only.

1.86 The *Commonwealth Cyber Security Posture in 2019: Report to Parliament* responds to a previous JCPAA recommendation that AGD and ASD report annually on the Commonwealth's cyber security posture to the Parliament. The Committee appreciates the sensitivities involved in reporting on the cyber security posture of individual Commonwealth entities, in terms of potentially increasing their risk of being targeted by malicious cyber actors. The Australian Parliament has a number of mechanisms to receive information on the cyber security position of individual Commonwealth entities, to ensure transparency and accountability while having regard to security requirements, including through: ANAO cyber audits on individual entities tabled in the Parliament; security classified, in-confidence briefings; and in-camera parliamentary committee arrangements. The Committee also notes that each Commonwealth entity must report on security each financial year to their portfolio minister, with AGD publishing a whole of government assessment report on its website.[120] The Committee will continue to monitor the effectiveness of the Commonwealth cyber security posture reporting to the Parliament.

1.87 The Committee notes that Commonwealth entities range significantly in size and risk profile and the mandating of specific cyber security strategies must be tailored to, and conscious of, those differences.

Recommendation 3

1.88 The Committee recommends that the Australian Government (the Attorney-General's Department) ensure that the framework of 13 behaviours and practices developed by the Australian National Audit Office (ANAO) play a greater role in the implementation and

[120] AGD, *Submission 7.2*, p. 8.

improvement of a cyber resilience culture within Commonwealth entities, including that:

- **the Protective Security Policy Framework (PSPF) be amended to reflect or incorporate the behaviours and practices framework, including for auditing purposes, to maximise alignment between the PSPF and the ANAO's audit framework; and**

- **a dedicated section be created within the annual PSPF self-assessment questionnaire addressing the ANAO's 13 behaviours and practices that facilitate a cyber resilience culture.**

1.89 The Committee considers that greater transparency in the implementation of a cyber resilience culture within corporate and non-corporate Commonwealth entities is required.

1.90 The Committee recommends that this be achieved through an annual limited assurance review into the cyber resilience of entities, undertaken by the ANAO on behalf of the Parliament.

1.91 The ANAO could work with each relevant entity to review and report back on the extent to which they have developed cyber resilience. The Committee recognises the concerns raised in evidence to the inquiry highlighted that individual vulnerabilities within Commonwealth entities could exacerbate existing cyber security risks. In light of this, the Committee proposes that published limited assurance reviews provide no more granular public information than is published in existing ANAO cyber resilience audits. The published report can also provide advice on identified impediments to agencies implementing the 13 behaviours and practices and the Essential Eight mitigation strategies, noting that the provision exists for confidential reporting to Ministers and the JCPAA where required.

1.92 Compliance of corporate and non-corporate entities with cyber security measures could be assessed against the Essential Eight mitigation strategies in the ISM, with a particular focus on the Top Four strategies. Cyber resilience culture should also be assessed according to the ANAO's 13 behaviours and practices as outlined above.

1.93 During the period of this inquiry, the Auditor-General released his Mid-Term Report, reflecting on key issues in public sector accountability that have characterised his time in the role so far.

1.94 The Committee notes that this Mid-Term Report highlighted that:

> the category which consistently has the most number of financial audit findings raised relates to the information technology control environment, with the most common area relating to weaknesses in security management. These findings are consistent with the conclusions in performance audits of cyber security, which have also consistently identified non-compliance. With cyber security being an area of government priority for many years, these findings are disappointing.[121]

1.95 The Auditor-General continued:

> 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.[122]

Recommendation 4

1.96 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 though 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).

[121] ANAO, *Auditor-General's Mid-Term Report* (2020), p. 5.

[122] ANAO, *Auditor-General's Mid-Term Report* (2020), p. 5.

2. Auditor-General Report No. 1 (2019-20)

Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities

Entities Audited: Australian Postal Corporation

ASC Pty Ltd

Reserve Bank of Australia

Introduction

2.1 The Reserve Bank of Australia (Reserve Bank) is a corporate Commonwealth entity. The Australian Postal Corporation (Australia Post) and ASC Pty Ltd (ASC; formerly the Australian Submarine Corporation) are government business enterprises (GBEs).[1]

2.2 Under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), non-corporate Commonwealth entities are required to apply the Australian Government Protective Security Policy Framework (PSPF), which states that they must mitigate common and emerging cyber threats. The framework mandates that non-corporate Commonwealth entities implement

[1] In line with the requirements for performance audit of GBEs under the *Auditor-General Act 1997*, the Committee provided approval for the ANAO to examine the cyber resilience of Australia Post and ASC.

the Top Four cyber security mitigation strategies detailed in the Australian Government Information Security Manual (ISM). These four mandatory strategies, in combination with a further four non-mandatory strategies, are known as the Essential Eight.[2] It is not mandatory for GBEs and corporate Commonwealth entities to apply the PSPF or the Top Four mitigation strategies from the ISM.[3] However, the PSPF and the ISM currently represent 'better practice' for such entities.[4]

Audit Rationale

2.3 The audit was undertaken to 'enable comparison with GBEs and corporate Commonwealth entities, and provide information to help strengthen the regulatory framework and improve cyber resilience of Commonwealth entities'.[5]

Audit Objective and Criteria

2.4 The audit objective was to assess the effectiveness of the management of cyber security risks by Australia Post, ASC and the Reserve Bank. To form a conclusion against this objective, the ANAO adopted three high-level criteria:

- Have entities managed cyber security risks in line with their own risk arrangements? Have entities managed cyber security risks in line with key aspects of the ISM? Do entities have a culture of cyber security resilience?[6]

Overall Audit Conclusion

2.5 The audit found that the Reserve Bank and ASC had 'effectively managed cyber security risks' but that Australia Post had 'not effectively managed cyber security risks, and should continue to implement its cyber security

[2] The Top Four mitigation strategies are: application whitelisting; patching applications; patching operating systems; and restricting administrative privileges. The other four mitigation strategies are: configuring Microsoft Office macros; user application hardening; multi-factor authentication; and daily backup of systems and data, Auditor-General Report No. 1 (2019-20), *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*, p. 7.

[3] Auditor-General Report No. 1 (2019-20), p. 28. (Such entities can be required to apply the PSPF if directed to comply under a government policy order under sections 22 or 93 of the PGPA Act 2013—no such orders have been issued to date, pp. 14-15.)

[4] Auditor-General Report No. 1 (2019-20), p. 14.

[5] Auditor-General Report No. 1 (2019-20), pp. 7-8.

[6] Auditor-General Report No. 1 (2019-20), p. 8.

improvement program and key controls across all its critical assets to enable cyber risks to be within its tolerance level'.[7]

2.6 All three entities 'have a fit for purpose cyber security risk management framework'.[8] ASC and the Reserve Bank had 'met the requirements of their respective frameworks by implementing the specified information and communications technology (ICT) controls that support desktop computers, ICT servers and systems'.[9] Australia Post had 'not met the requirements of its framework, having not implemented all specified key controls'.[10]

2.7 Although the Top Four mitigation strategies from the ISM are not mandatory for GBEs or corporate Commonwealth entities, the Reserve Bank and ASC had implemented controls in line with the Top Four and other mitigation strategies in the Essential Eight.[11] However, Australia Post had 'not fully implemented controls' in line with the Top Four and the Essential Eight.[12] All three entities had 'implemented mitigation strategies beyond the requirements of the Essential Eight, such as the Reserve Bank using machine learning and analytics to detect cyber threats'.[13]

2.8 The audit further found that the Reserve Bank and ASC are 'cyber resilient, with high levels of resilience compared to 15 other entities audited over the past five years', while Australia Post is 'not cyber resilient but is internally resilient'.[14] The Reserve Bank has a 'strong cyber resilience culture', ASC is 'developing this culture', and Australia Post is 'working towards embedding a cyber resilience culture within its organisation'.[15]

2.9 The audit recommended that Australia Post conduct risk assessments for all its critical assets where it has not already done so and take immediate action

[7] Auditor-General Report No. 1 (2019-20), p. 8.

[8] Auditor-General Report No. 1 (2019-20), p. 8.

[9] Auditor-General Report No. 1 (2019-20), p. 8.

[10] Auditor-General Report No. 1 (2019-20), p. 8.

[11] Auditor-General Report No. 1 (2019-20), p. 8.

[12] Auditor-General Report No. 1 (2019-20), p. 8

[13] Auditor-General Report No. 1 (2019-20), p. 9.

[14] Auditor-General Report No. 1 (2019-20), p. 8.

[15] Auditor-General Report No. 1 (2019-20), p. 8.

to address any identified extreme risks to those assets and supporting networks and databases.[16] Australia Post agreed to the recommendation.

Cyber Security Risk Management Framework

2.10 The audit concluded that all three entities 'have a fit for purpose cyber security risk management framework'.[17] Each specific framework either includes the ISM or incorporates elements of it, with Australia Post and the Reserve Bank also adopting aspects of recognised national and international cyber security frameworks applicable to their industry and regulatory environment.[18]

2.11 The ANAO has developed six criteria to assess the effectiveness of entity cyber security arrangements.[19] The Reserve Bank had 'fully established' all six arrangements.[20] ASC and Australia Post had 'established three of the six arrangements and partially or largely established the other three arrangements'.[21]

2.12 Noting that the audit recommendation focused on Australia Post, the three arrangements that Australia Post had partially or largely established were: ICT operational staff understand vulnerabilities and cyber threats to the system; integrated and documented architecture for data, systems and security controls; and systematic approach to managing cyber risks.[22]

2.13 The ANAO also reviewed a sample of controls supporting desktop computers, ICT servers and systems in the Reserve Bank, ASC and Australia Post.[23] The audit found that the Reserve Bank and ASC had 'met the

[16] Auditor-General Report No. 1 (2019-20), p. 10.

[17] Auditor-General Report No. 1 (2019-20), p. 8. For details of each entity's cyber security risk management framework, see pp. 20-22.

[18] Auditor-General Report No. 1 (2019-20), pp. 8-9.

[19] Auditor-General Report No. 1 (2019-20), p. 22. The criteria comprise: enterprise-wide governance arrangements; information security roles assigned and responsibilities communicated; ICT security incorporated into strategy, planning and delivery of services; ICT operational staff understand vulnerabilities and cyber threats to the system; integrated and documented architecture for data, systems and security controls; and systematic approach to managing cyber risks, p. 22.

[20] Auditor-General Report No. 1 (2019-20), p. 20.

[21] Auditor-General Report No. 1 (2019-20), p. 20.

[22] Auditor-General Report No. 1 (2019-20), p. 22

[23] For details of these controls, see Auditor-General Report No. 1 (2019-20), pp. 25-26.

requirements for implementing ICT controls contained in their cyber security risk management framework'.[24] Australia Post had 'not met the requirements for ICT controls in its framework, having not implemented all specified key controls'.[25] The audit found that, in Australia Post, 'only half of the sampled controls (five of 10) were designed and implemented as specified in its cyber security risk management framework. Three of the 10 sampled controls were partly implemented and two controls were not implemented'.[26]

2.14 Australia Post provided an update on progress in implementing the audit recommendation that it conduct risk assessments for all its critical assets where it had not already done so and take immediate action to address any identified extreme risks to those assets.[27] Australia Post confirmed that 'we've been working over the last six months to conduct a formal risk assessment against our critical assets that were identified as a gap in the report', including 'updating assessments for those assets already assessed but also taking immediate action to address any identified concerns'.[28] An approach and methodology review had also been completed by Australia Post internal audit.[29] Australia Post emphasised that it was 'working very quickly to establish that baseline of controls against our critical applications, have the appropriate risks raised and have the appropriate actions taken where we're finding critical gaps'.[30] Implementation monitoring will be managed through Australia Post's information security risk management and compliance programs, and 'reported up through senior management and to our board through our audit and risk committee'.[31] Australia Post's

[24] Auditor-General Report No. 1 (2019-20), p. 25.

[25] Auditor-General Report No. 1 (2019-20), p. 25. For Australia Post, the ANAO reviewed two of 13 Tier 1 Cyber Security mitigation controls and eight of 189 Information Security Standards controls that Australia Post had specified in its cyber security risk management framework, p. 25.

[26] Auditor-General Report No. 1 (2019-20), p. 26.

[27] Auditor-General Report No. 1 (2019-20), p. 10.

[28] Mr Glenn Stuttard, Chief Information Security Officer (Acting), Australia Post, *Committee Hansard*, 19 May 2020, p. 18

[29] Mr Glenn Stuttard, Chief Information Security Officer (Acting), Australia Post, *Committee Hansard*, 19 May 2020, p. 20.

[30] Mr Glenn Stuttard, Chief Information Security Officer (Acting), Australia Post, *Committee Hansard*, 19 May 2020, p. 20.

[31] Mr Glenn Stuttard, Chief Information Security Officer (Acting), Australia Post, *Committee Hansard*, 19 May 2020, p. 18.

cyber security program, 'Securing Tomorrow', is also focused on reducing cyber risks to within its risk tolerance by 2020.[32] Australia Post confirmed that the program was due by 30 June 2020 and on schedule.[33]

2.15 Asked about the current assessment of Australia Post's cyberthreat environment, the Acting Chief Information Security Officer at Australia Post stated:

> I have dedicated information security officers continually reviewing and adjusting our tools and our processes to ensure that we have the strength and protection in place to prevent those cyberattacks. Some of those techniques include ensuring that we have the best-of-breed next generation tooling in place to limit risk and impact of cyberthreats, such as ransomware … We're regularly doing simulated [phishing] campaigns with our employees to train them and educate them … there is the mandatory annual cybertraining for employees.[34]

2.16 In terms of cyber data, Australia Post confirmed that, between 1 January and 30 March 2020, 'we had no extreme or high incidents, but we did respond to over 300 individual cyber-incidents that we saw in our systems', mostly SMS and email phishing campaigns.[35] As to whether any of these incidents had been escalated to the ACSC, Australia Post stated that its 'cyber-emergency response function is regularly talking to the likes of ACSC around … threat intel, threat landscape, but also the information security industry do share intel and help each other defend against threats that we're seeing in the landscape'.[36]

Alignment with ISM Risk Mitigation Strategies

2.17 In establishing specific risk management frameworks for cyber security, the Reserve Bank, ASC and Australia Post adopted mitigation strategies from

---

[32] Auditor-General Report No. 1 (2019-20), p. 27. The program implements 'strategic capability uplift and the remediation of identified vulnerabilities', Australia Post, *Submission 4*, p. 2.

[33] Mr Glenn Stuttard, Chief Information Security Officer (Acting), Australia Post, *Committee Hansard*, 19 May 2020, p. 20.

[34] Mr Glenn Stuttard, Chief Information Security Officer (Acting), Australia Post, *Committee Hansard*, 19 May 2020, p. 19.

[35] Mr Glenn Stuttard, Chief Information Security Officer (Acting), Australia Post, *Committee Hansard*, 19 May 2020, p. 19.

[36] Mr Glenn Stuttard, Chief Information Security Officer (Acting), Australia Post, *Committee Hansard*, 19 May 2020, p. 19.

the ISM, despite not being mandated to do so.[37] The audit therefore examined whether these entities had implemented controls in line with the ISM, noting that 'it is better practice for such entities to implement the Top Four and other Essential Eight mitigation strategies in the ISM'.[38] The audit found that the Reserve Bank and ASC had 'implemented controls in line with the requirements of the ISM, including the Top Four and other mitigation strategies in the Essential Eight'.[39]

2.18 Australia Post had 'not fully implemented controls in line with either the Top Four or the four non-mandatory strategies in the Essential Eight'.[40]

2.19 Australia Post had implemented two of the Top Four mitigation strategies: patching applications and restricting administrative privileges.[41] Australia Post's submission provided details of initiatives to address this matter, including implementing 'ISM accreditation for a number of Australia Post services', as well as 'application whitelisting controls supporting its retail and deliveries environments' and 'the deliveries security uplift project, which is enhancing controls on critical deliveries systems (including whitelisting)'.[42]

2.20 Australia Post had implemented one of the four non-mandatory mitigation strategies in the Essential Eight: daily backups.[43] Australia Post's submission provided details of initiatives to address this matter, including having conducted a 'maturity level assessment' against the Essential Eight mitigation strategies.[44]

2.21 In its response to the audit, the Reserve Bank stated that it would 'continue to align with the security controls outlined in the ... ISM and relevant industry security standards'.[45] In its response to the audit, Australia Post

[37] Auditor-General Report No. 1 (2019-20), p. 11.

[38] Auditor-General Report No. 1 (2019-20), p. 7, p. 43.

[39] Auditor-General Report No. 1 (2019-20), p. 8.

[40] Auditor-General Report No. 1 (2019-20), p. 8.

[41] Auditor-General Report No. 1 (2019-20), p. 29. The other two mitigation strategies are application whitelisting and patching operating systems.

[42] Australia Post, *Submission 4*, pp. 1-2.

[43] Auditor-General Report No. 1 (2019-20), p. 32. (For ANAO analysis of Australia Post's treatment of the other three strategies, see pp. 33-35.)

[44] Australia Post, *Submission* 4, p. 2.

[45] Auditor-General Report No. 1 (2019-20), p. 53.

stated that, while it is 'not required to apply or comply with the Manual or its Top Four mitigation strategies', it has 'voluntarily chosen to incorporate aspects of the Manual into its cyber security framework—together with other industry-leading frameworks … as a matter of best practice'.[46] As Australia Post further observed at the public hearing—'it is clearly not something that we are required to do. However, we certainly see it as sound practice … As a consequence, we've been gradually working through our cyber-risks and building towards the Essential Eight'.[47]

Cyber Security Resilience

2.22 The audit found that the Reserve Bank and ASC were 'cyber resilient, with high levels of resilience compared to 15 other entities audited over the past five years'.[48] The Reserve Bank and ASC respectively had the highest and equal third highest level of cyber resilience of 17 entities examined by the ANAO over the past five years.[49]

2.23 The audit found that Australia Post was 'not cyber resilient but is internally resilient, which is similar to many of the previously audited entities'.[50]

2.24 The ANAO assessed the three entities' culture of cyber resilience against 13 behaviours and practices across the areas of governance and risk management; roles and responsibilities; technical support; and monitoring compliance.[51]

2.25 The audit found that the Reserve Bank has a 'strong cyber resilience culture, having established all 13 assessed behaviours and practices in the areas of cyber security governance and risk management, roles and responsibilities, technical support and monitoring compliance'.[52] At the public hearing, the Reserve Bank confirmed its strong commitment to cyber security resilience,

---

[46] Auditor-General Report No. 1 (2019-20), p. 51.

[47] Mr John Cox, Executive General Manager, Transformation and Enablement, Australia Post, *Committee Hansard*, 19 May 2020, p. 20.

[48] Auditor-General Report No. 1 (2019-20), p. 8.

[49] Auditor-General Report No. 1 (2019-20), p. 9.

[50] Auditor-General Report No. 1 (2019-20), p. 8.

[51] Auditor-General Report No. 1 (2019-20), pp. 37-38. For a list of these behaviours and practices, see ANAO, *Submission 6.1*, p. 3.

[52] Auditor-General Report No. 1 (2019-20), p. 9—for details of the assessment, see pp. 38-42.

emphasising that its approach to managing cyber security had 'multiple prongs':

> It's not a cookie-cutter approach—it can't be in the current world where a lot of our adversaries are changing their tactics and techniques on a daily basis and we have to have the ability to respond … we take our security standards very seriously, based on the information security management manual from the government, and we embed them into every aspect of our system delivery and system maintenance. The second prong … is the activity we undertake around intelligence gathering, sharing of information and collaborating with those within the bank and with other people in the financial services sector … to make sure we're on top of the broader landscape. We take a three lines of defence model when it comes to risk management, which extends from our business system owners and our IT system owners as the first line, through our chief information officer and our chief information security officer as the second line and then to the internal audit department as the third line … We also do a lot of reporting across the bank about cybersecurity events and the control, so that it's got that visibility.[53]

2.26 The audit found that ASC is 'developing a cyber resilience culture, having embedded seven of the assessed behaviours and practices and working to more fully establish the other six cyber security behaviours and practices within its business processes'.[54] The ASC confirmed that it is 'working to mature and improve … cyber security related behaviours and practices, as highlighted in the report'.[55]

2.27 The audit found that Australia Post is 'working towards embedding a cyber resilience culture'—while having embedded eight of the 13 assessed behaviours and practices, it has 'not systematically managed cyber risks'.[56]

2.28 At the public hearing, the Auditor-General emphasised that cyber resilience 'goes beyond just having a cybersecurity capacity'—'resilience goes more to the cultural aspect and the broader frameworks in place'.[57] As the Auditor-General further explained, 'the reason we focus on culture is that successful implementation happens when it's important to the leadership of the

---

[53] Mrs Susan Woods, Assistant Governor, Corporate Services, Reserve Bank, *Committee Hansard*, 19 May 2020, pp. 11-12.

[54] Auditor-General Report No. 1 (2019-20), p. 9—for details of the assessment, see pp. 38-42.

[55] ASC, *Submission 2*, p. 2.

[56] Auditor-General Report No. 1 (2019-20), p. 9—for details of the assessment, see pp. 38-42.

[57] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 12.

organisation and they invest in it'.[58] Over time, the ANAO had constructed a framework of 13 behaviours and practices as an indicator of culture and how that resilient culture operates, to test 'whether the leadership of an organisation goes beyond putting out an instruction saying that something should happen and into whether they're embedding it in the day-to-day management and practices of the entity'.[59]

2.29 The Reserve Bank similarly observed that 'a strong cyber culture is fundamental to embedding effective cyber-resilience':

> we've got ourselves to a position where an understanding of cyber-risks and how we respond to them is part of our DNA. We talk about it regularly, from the governor and the deputy governor all the way down through the organisation. It's part of the way we do business … People understand it and recognise it for that, and therefore they start to embed the practices that we are talking about in their daily activities … it's fundamental to having an effective cyber-resilience posture. You can have all the standards in the world, but if people don't live and breathe them, understand them and employ them in what they're doing every day then they're really not worth anything.[60]

2.30 The Reserve Bank explained that it used a 'multiplicity of tools', from formal training to email campaigns and events, to embed its cyber resilient culture.[61] Its activities therefore 'go beyond' training—'training is certainly critical for key roles at the bank, and we do offer baseline training for all staff', but the Reserve Bank also focuses 'on education, which is more about giving a general awareness of cyber-risks'.[62] More recently, the Reserve Bank has further shifted the focus to 'now also focus on literacy, which is really just making sure the language of cyber-risk … is known and understood at meaningful levels, including the leadership of the bank as well'.[63]

---

[58] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 21.

[59] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 17.

[60] Mrs Susan Woods, Assistant Governor, Corporate Services, Reserve Bank, *Committee Hansard*, 19 May 2020, p. 17.

[61] Mrs Susan Woods, Assistant Governor, Corporate Services, Reserve Bank, *Committee Hansard*, 19 May 2020, p. 17.

[62] Mr Gayan Benedict, Chief Information Officer, Reserve Bank, *Committee Hansard*, 19 May 2020, p. 17.

[63] Mr Gayan Benedict, Chief Information Officer, Reserve Bank, *Committee Hansard*, 19 May 2020, p. 17.

2.31 Australia Post provided information about how it was building a stronger cyber resilience culture, emphasising that this matter 'gets discussed all the way from the board through to the executive and management committee … to raise that awareness as we see external threats constantly adjusting'.[64]

Concluding Comment

2.32 The Committee notes the audit finding that the Reserve Bank, ASC and Australia Post have a fit-for-purpose cyber security risk management framework.[65]

2.33 The Reserve Bank and ASC had met the requirements of their respective frameworks by implementing the specified ICT controls.[66]

2.34 Australia Post had not met the requirements of its framework, having not implemented all specified key controls.[67] The audit therefore recommended that Australia Post conduct risk assessments for all its critical assets where it has not already done so and take immediate action to address any identified extreme risks to those assets. The Committee acknowledges that, during the inquiry, Australia Post provided an update on its implementation of this recommendation, including its cyber security program, 'Securing Tomorrow', focused on reducing cyber risks to within its risk tolerance by 2020.

2.35 All three entities incorporated mitigation strategies and controls from the ISM in their cyber security risk management frameworks, despite not being mandated to do so. The Reserve Bank and ASC had implemented controls in line with the Top Four and other mitigation strategies in the Essential Eight.[68] Australia Post had implemented two of the Top Four mitigation strategies and controls for one of the four other mitigation strategies in the Essential Eight.[69] Australia Post provided an update to the Committee on its progress in implementing all of these strategies, including that it was implementing ISM accreditation for a number of Australia Post services and

[64] Mr John Cox, Executive General Manager, Transformation and Enablement, Australia Post, *Committee Hansard*, 19 May 2020, p. 18.

[65] Auditor-General Report No. 1 (2019-20), p. 8.

[66] Auditor-General Report No. 1 (2019-20), p. 8.

[67] Auditor-General Report No. 1 (2019-20), p. 8.

[68] Auditor-General Report No. 1 (2019-20), p. 14.

[69] Auditor-General Report No. 1 (2019-20), p. 14.

had conducted a maturity level assessment against the Essential Eight mitigation strategies.

2.36 The Committee notes that all three entities had implemented mitigation strategies beyond the requirements of the Essential Eight, and that the Reserve Bank and Australia Post had also adopted aspects of recognised and international cyber security frameworks applicable to their industry and regulatory environments.[70]

2.37 The audit found that the Reserve Bank and ASC are cyber resilient, having effectively managed cyber security risks.[71] In particular, the Committee recognises that the Reserve Bank and ASC respectively had the highest and equal third highest level of cyber resilience of 17 entities examined by the ANAO over the past five years.[72] The audit concluded that the Reserve Bank has a strong cyber resilience culture and ASC is developing this culture.[73] The Committee appreciated the examples of best practice in this area, as provided at the public hearing by the Reserve Bank.

2.38 The audit found that Australia Post is not cyber resilient but is internally resilient.[74] The Committee notes Australia Post's work towards embedding a cyber resilience culture within its organisation.

2.39 Despite it not being mandatory for GBEs and corporate Commonwealth entities to implement the Top Four mitigation strategies in the ISM, it is 'better practice' for such entities to do so.[75] Accordingly, the Committee sees merit in Australia Post providing an update on how it is implementing controls in line with the Top Four and other mitigation strategies in the Essential Eight to reflect better practice, and how a cyber resilience culture is being further embedded in the organisation.

[70] Auditor-General Report No. 1 (2019-20), p. 9, p. 11.

[71] Auditor-General Report No. 1 (2019-20), p. 8.

[72] Auditor-General Report No. 1 (2019-20), p. 9.

[73] Auditor-General Report No. 1 (2019-20), p. 8.

[74] Auditor-General Report No. 1 (2019-20), p. 8.

[75] Auditor-General Report No. 1 (2019-20), p. 7, p. 43.

Recommendation 5

2.40 The Committee recommends that Australia Post provide an update on:

- **progress in implementing controls in line with the Top Four and other mitigation strategies in the Essential Eight (in confidence, if required); and**

- **how a cyber resilience culture is being further embedded in the organisation.**

3. Auditor-General Report No. 13 (2019-20)

Implementation of the My Health Record System

Entities Audited: Australian Digital Health Agency

Department of Health

Introduction

3.1 Chapter 3 focuses on the cyber resilience findings of Auditor-General Report No. 13 (2019-20), *Implementation of the My Health Record System*.[1]

3.2 My Health Record is an online electronic summary of a person's health information. It is part of a national digital health agenda to encourage better sharing of health information across healthcare settings. Nine out of every ten Australians now has a My Health Record, following the conclusion of the opt-out period on 31 January 2019.[2] My Health Records may include:

- information from healthcare providers—health summaries, hospital discharge summaries, pathology and diagnostic imaging reports, medications, and referral letters;

[1] The ANAO noted that 'two of the five audit report recommendations related specifically to cyber security' (recommendations 3 and 4), ANAO, *Submission 6*, p. 3.

[2] Auditor-General Report No. 13 (2019-20), *Implementation of the My Health Record System*, p. 14.

- information from repository operators—Medicare data, Pharmaceutical Benefits Scheme/Repatriation Pharmaceutical Benefits Scheme data, Australian Organ Donor Register decisions, and Australian Immunisation Register data;
- information added by healthcare recipients—such as contact numbers, emergency contact details, and advance care plans; and
- back-up copies of documents.[3]

3.3 My Health Records can be accessed by healthcare recipients, healthcare providers, and nominated/authorised representatives.

3.4 The Department of Health (Health), a non-corporate Commonwealth entity, administers the *My Health Records Act 2012*, on behalf of the Minister for Health. The Australian Digital Health Agency (ADHA), a corporate Commonwealth entity, is the System Operator for My Health Record.

3.5 ADHA shares cyber security risks with other participants, including:

- the National Infrastructure Operator (NIO) and subcontractors—provide the core infrastructure for the My Health Record system, and have legislative and contractual security obligations;
- Services Australia—secures the data repositories and myGov portal …;
- software vendors—are responsible for the security of software used to access the My Health Record system, including clinical software used by healthcare providers and mobile applications used by healthcare recipients;
- healthcare provider organisations and their contracted service providers—have access to multiple records by design, and are responsible for their information management and cyber security practices; and
- individual healthcare recipients—are responsible for the security of the passwords, devices and connections they use to access their My Health Record, either through myGov or third party mobile applications.[4]

Audit Rationale

3.6 The My Health Record system potentially impacts all Australians, as it collates electronic summaries of individuals' health information. The system 'requires a balance between increasing access to information, and managing the inherent privacy and cyber security risks of making that information more readily available'.[5] The audit stated that, 'for these reasons, My Health

[3] Auditor-General Report No. 13 (2019-20), p. 16.

[4] Auditor-General Report No. 13 (2019-20), p. 42.

[5] Auditor-General Report No. 13 (2019-20), p. 21.

Record has generated parliamentary and public interest, particularly in relation to the management of privacy and cyber security risks'.[6]

Audit Objective and Criteria

3.7 The audit objective was to assess the effectiveness of the implementation of the My Health Record system under the opt-out model, with the audit adopting the following criteria: 'implementation of the My Health Record system promotes achievement of its purposes; My Health Record system risks are appropriately assessed, managed and monitored; and monitoring and evaluation arrangements for the My Health Record system are effective'.[7]

Overall Audit Conclusion

3.8 The audit concluded that 'implementation of the My Health Record system was largely effective'.[8] Implementation planning for and delivery of My Health Record under the opt-out model was 'effective in promoting achievement of its purposes', and implementation planning and execution was 'appropriate' and supported by 'appropriate governance arrangements'.[9] Communication activities were also 'appropriate to inform healthcare recipients and providers'; risk management for the My Health Record expansion program was 'partially appropriate'; and monitoring and evaluation arrangements for My Health Record were 'largely appropriate'.[10]

3.9 In terms of cyber resilience, the audit found that ADHA had 'largely appropriate systems to manage cyber security risks to the core infrastructure of the My Health Record system, except its management of shared cyber security risks and its oversight processes should be improved'.[11] On these specific matters, the audit found that ADHA's approach to managing shared cyber security risks was 'not appropriate' and recommended that ADHA develop an assurance framework for third-party software connecting to the

[6] Auditor-General Report No. 13 (2019-20), p. 21.

[7] Auditor-General Report No. 13 (2019-20), p. 21. The audit did not examine the decisions to create the My Health Record system or adopt the opt-out model, or consider the framework for secondary use of data, and no individual My Health Records were examined, p. 7. Further, the ANAO 'did not test the technical effectiveness of cyber security controls as part of this audit', p. 41.

[8] Auditor-General Report No. 13 (2019-20), p. 7.

[9] Auditor-General Report No. 13 (2019-20), p. 7.

[10] Auditor-General Report No. 13 (2019-20), pp. 7-8.

[11] Auditor-General Report No. 13 (2019-20), p. 9.

My Health Record system, including clinical software and mobile applications, in accordance with the Australian Government Information Security Manual (ISM).[12] It also recommended that ADHA develop, implement and regularly report on a strategy to monitor compliance with mandatory legislated security requirements by registered healthcare provider organisations and contracted service providers.[13] ADHA agreed to these recommendations.

Cyber Security Standards

3.10 It is not mandatory for corporate Commonwealth entities to apply the Protective Security Policy Framework (PSPF) or the Top Four strategies from the ISM for mitigating cyber threats.[14] However, in March 2017, the Council of Australian Governments amended the Intergovernmental Agreement on National Digital Health to acknowledge that ADHA (a corporate Commonwealth entity) would comply with the PSPF and ISM.[15]

3.11 The My Health Record system underwent five information security assessments between 2012 and 2017, conducted by an external Information Security Registered Assessors Program (IRAP) assessor.[16] The audit noted the 2017 IRAP assessment found that, for My Health Record core infrastructure, ADHA had implemented the Top Four and Essential Eight cyber security mitigation strategies.[17] ADHA also stated to the Australian National Audit Office (ANAO) that 'the My Health Record system has not been the subject of any actual malicious cyber activity, events or incidents'.[18]

3.12 The audit concluded that ADHA had 'managed risks' to the core infrastructure of the My Health Record system through 'establishing a Digital Health Cyber Security Centre; undertaking a series of dedicated cyber security assessments; and implementing the "Essential Eight" cyber

[12] Auditor-General Report No. 13 (2019-20), p. 9, p. 10.

[13] Auditor-General Report No. 13 (2019-20), p. 10.

[14] The PSPF requires non-corporate Commonwealth entities to implement four mitigation strategies (known as the Top Four) of eight essential mitigation strategies (known as the Essential Eight), as referenced in the ISM.

[15] Auditor-General Report No. 13 (2019-20), p. 42.

[16] Auditor-General Report No. 13 (2019-20), p. 43.

[17] Auditor-General Report No. 13 (2019-20), p. 44.

[18] Auditor-General Report No. 13 (2019-20), p. 45.

security mitigation strategies and decreasing the number of ISM cyber security controls not implemented'.[19]

3.13 The audit noted that its analysis of cyber security risks was based on 'a review of ADHA's documentation and management frameworks'—the ANAO 'did not test the technical effectiveness of cyber security controls as part of this audit'.[20] As the Auditor-General further advised, 'we reported that, effectively, they had provided assurance that they met the mandatory four and the top eight. We didn't do an independent assessment of those things in that audit like we do in the cyberaudits'.[21]

3.14 ADHA provided additional information at the public hearing about the IRAP assessment.[22] The Auditor-General observed that 'we've reported in other audit reports that sometimes we've found that IRAPs haven't always provided an accurate indicator of cyber resilience … That said, they are a key part of the framework, so it's an important part of what agencies undertaking them do'.[23]

Assurance Framework for Third Party Software

3.15 The audit found that ADHA 'did not assess, certify or accredit the ISM compliance of third party software and systems connected to the My Health Record system', as required by the PSPF—'this included clinical software that gives healthcare providers access to multiple health records, and mobile applications for healthcare recipients'.[24] This decision 'limited ADHA's assurance over the cyber security risks of the My Health Record system'.[25] The audit stated that 'an ISM assessment, certification and accreditation approach would provide a rigorous system for ADHA to understand and manage cyber security risks from third party software', but any assurance

[19] Auditor-General Report No. 13 (2019-20), p. 9.

[20] Auditor-General Report No. 13 (2019-20), p. 41.

[21] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 9.

[22] Mr Ronan O'Connor, National Health Chief Information Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 9.

[23] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 9.

[24] Auditor-General Report No. 13 (2019-20), p. 46. (Instead, software vendors must complete a Conformance Vendor Declaration Form and a 'deed poll' that warrants their conformance testing against requirements set by ADHA, and mobile application vendors must sign a Portal Operator Registration Agreement that details their responsibilities and obligations, p. 46.)

[25] Auditor-General Report No. 13 (2019-20), p. 46.

process 'must be balanced against disincentives to register and use the system'.[26]

3.16 The audit recommended that ADHA develop an assurance framework for third party software connecting to the My Health Record system, including clinical software and mobile applications, in accordance with the ISM.[27] ADHA agreed to the recommendation and, at the time of the audit, advised that 'an assurance framework exists for systems (including clinical software and mobile applications) connecting to the Healthcare Identifiers Service and the My Health Record system, including processes to confirm conformance'—but stated that it would 'review the standards that apply to these systems, and alignment with the ISM. We will work with industry to update the assurance framework as required'.[28]

3.17 The ADHA-Health submission provided further details of ADHA's implementation plan for this audit recommendation.[29] ADHA also provided implementation timeframes over 2020 for the recommendation, encompassing 'external engagement, internal engagement, baseline framework, prioritise roadmap, roadmap delivery'.[30]

Shared Risk and Compliance with Legislated Security Requirements

3.18 The ANAO outlined that the My Health Record program has a number of shared risks involving different Commonwealth agencies, various jurisdictions, the healthcare sector and consumers. More specifically, the ADHA shares My Health Record risks with a variety of system participants including Services Australia, healthcare provider organisations, medical practitioners, software vendors, healthcare recipients and the Information Commissioner.[31] The ANAO highlighted the importance of not only

[26] Auditor-General Report No. 13 (2019-20), p. 46.

[27] Auditor-General Report No. 13 (2019-20), p. 10.

[28] Auditor-General Report No. 13 (2019-20), p. 47.

[29] Health-ADHA, *Submission 1*, p. 3. See also 'ANAO My Health Record Performance Audit Implementation Plan', 20 February 2020, and Appendix A, 'Implementation scope for ANAO recommendations', ADHA website, <www.adha.gov.au/anao-performance-audit-implementation-plan-publication> [accessed August 2020].

[30] Appendix A, 'Implementation scope for ANAO recommendations', pp. 9-10.

[31] Auditor-General Report No. 13 (2019-20), p. 32.

managing risks to Commonwealth agencies but also assessing and managing risks shared with other participants.[32]

3.19 The Commonwealth Risk Management Policy requires that entities implement strategies to manage shared risks and outlines measures that may be taken including: establishing memoranda of understanding with partners to formalise shared risk management; development of shared risk registers; educating officials on their responsibilities to identify and manage shared risks; and documenting control owners and governance arrangements for monitoring shared risks.[33]

3.20 The ANAO stated that the ADHA could further clarify the roles and responsibilities of government entities in managing shared risks 'by explicitly indicating which risks are shared, with which entities, and who in other entities is responsible for controls implementation'.[34] Further, the ANAO recommended that 'ADHA conduct an end-to-end privacy risk assessment of the operation of the My Health Record system under the opt-out model, including shared risks and mitigation controls, and incorporate the results of this assessment into the risk management framework for the My Health Record system'.[35] The Australian Digital Health Agency agreed to this recommendation.

3.21 Under the relevant My Health Records legislation, entities such as healthcare provider organisations and contracted service providers must comply with mandatory legislated security requirements in order to be eligible, and remain eligible, for registration. As the System Operator, ADHA should not register an ineligible entity, and may consider revoking registration of an entity that does not remain eligible.[36] ADHA has 'clear statutory functions and powers to register and deregister entities'.[37]

3.22 The audit found that ADHA 'conducted limited compliance monitoring to ensure registered healthcare providers met legislated security requirements', noting that 'legislative requirements are only effective risk controls when

[32] Auditor-General Report No. 13 (2019-20), p. 12.

[33] Auditor-General Report No. 13 (2019-20), p. 31.

[34] Auditor-General Report No. 13 (2019-20), p. 32.

[35] Auditor-General Report No. 13 (2019-20), p. 35.

[36] Auditor-General Report No. 13 (2019-20), p. 47.

[37] Auditor-General Report No. 13 (2019-20), p. 47.

enforced'.[38] The risk that multiple health records are accessed, modified or made unavailable without authorisation due to compromise of a participating healthcare organisation or their contracted service provider 'remains a shared risk above ADHA's residual risk tolerance'.[39]

3.23 At the public hearing, the Auditor-General explained that the shared risks in My Health Record 'bring additional risks', and 'the increase is because there needs to be coordination between various agencies to manage the risk … So it's simply the number of players involved and getting accountability in the right spot for where mitigation can best occur'.[40] As the Auditor-General further noted:

> Part of the response to our report from the agencies … was the balance between meeting statutory requirements and ensuring broad uptake of a system … at the end of the day, parliament has put through some legislation saying that certain things have to happen before someone can be registered as a provider, and that's sort of where we landed with respect to the recommendations.[41]

3.24 ADHA outlined some of its cyber security initiatives to manage risk and improve the level of awareness and education, including cybersecurity guidance materials 'designed to encourage improved information security practices across the health sector and into GP practices'; presentations and workshops; and digital health security awareness e-learning courses.[42] ADHA also worked with the Australian Cyber Security Centre (ACSC) to issue alerts into the health sector.[43] ADHA further emphasised that this is a 'continuing, ongoing improvement process. The landscape changes on a minute-by-minute, daily basis … this is just ongoing in relation to the support that we provide to those organisations'.[44] ADHA also advised that all traffic to and from the My Health Record system is monitored for 'any

[38] Auditor-General Report No. 13 (2019-20), p. 47.

[39] Auditor-General Report No. 13 (2019-20), p. 48.

[40] Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 10.

[41] Mr Grant Hehir, Auditor General, ANAO, *Committee Hansard*, 19 May 2020, p. 8.

[42] Mr Ronan O'Connor, National Health Chief Information Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 6.

[43] Mr Ronan O'Connor, National Health Chief Information Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 6.

[44] Mr Ronan O'Connor, National Health Chief Information Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 6.

unusual behaviour or activity', using specialist real-time monitoring tools and, 'in instances where we have particular concern, we can suspend access from that organisation to the My Health Record system'.[45]

3.25 In terms of benchmarking cyber security practice within healthcare providers and tracking progress, Health responded that:

> obviously we've still got work ahead of us in terms of more detailed consultation with the peak organisations about lifting the security posture of all of those participants that interact with the Commonwealth government, and specifically with My Health Record. So that is a … design piece of work that we need to do with them about what is their current level of conformance and then how we might continue to attest that and its improvement.[46]

3.26 As Health further explained, 'part of the work that we're trying to do collectively at the Commonwealth level is to have a look at how we continue to lift the minimum level of conformance with security requirements for all participants that connect to Commonwealth infrastructure'.[47]

3.27 Another matter explored at the public hearing was the cyber attack threat level for Australian healthcare providers, noting the audit had stated that:

> in Australia, evidence shows: not all healthcare provider organisations achieve minimum cyber security levels; in 2018, the private health service provider sector reported the most notifiable data breaches of any industry sector; and more than 40 per cent of data breaches from the private health service provider sector notifications to the [Office of the Australian Information Commissioner] in 2018 were due to malicious or criminal attacks, almost half of which were cyber incidents.[48]

3.28 ADHA observed that 'those reports have shown that there are risks to the health system from cyberattack, as there are in the rest of the economy, and those need to be managed through improved security over time, which is what we're working with the sector on at the moment'.[49] Health further emphasised that it constantly monitors this area with its service delivery

---

[45] Mr Ronan O'Connor, National Health Chief Information Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 7.

[46] Mr Daniel McCabe, First Assistant Secretary, Provider Benefits Integrity Division, , *Committee Hansard*, 19 May 2020, p. 6.

[47] Mr Daniel McCabe, First Assistant Secretary, Provider Benefits Integrity Division, Health, *Committee Hansard*, 19 May 2020, p. 7.

[48] Auditor-General Report No. 13 (2019-20), p. 41.

[49] Ms Bettina McMahon, Acting Chief Executive Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 5.

partners, ADHA and Services Australia, 'to look at how we can strengthen those parts of the health sector that government participates in'.[50] Health also pointed to 'the challenges that we've got … to work through with peak organisations around how they continue to lift their cybermaturity' and 'the need to work with states and territories … So, it's a complex and quite distributed landscape that we need to manage'.[51]

3.29 The audit recommended that ADHA 'develop, implement and regularly report on a strategy to monitor compliance with mandatory legislated security requirements by registered healthcare provider organisations and contracted service providers'.[52] The ADHA-Health submission provided details of ADHA's implementation plan for this audit recommendation.[53] ADHA also provided implementation timeframes over 2020 for the recommendation, encompassing 'context, engagement, regulatory design, consultation/refinement, implementation/review'.[54]

Timeframes for Implementation of Recommendations

3.30 The ADHA-Health submission provided details of the ADHA implementation plan for the audit recommendations, with indicative timeframes.[55] ADHA confirmed that it consulted with the ANAO in the development of the implementation plan.[56]

---

[50] Mr Daniel McCabe, First Assistant Secretary, Provider Benefits Integrity Division, Health, *Committee Hansard*, 19 May 2020, p. 5.

[51] Mr Daniel McCabe, First Assistant Secretary, Provider Benefits Integrity Division, Health, *Committee Hansard*, 19 May 2020, p. 5.

[52] Auditor-General Report No. 13 (2019-20), p. 10.

[53] Health-ADHA, *Submission 1*, p. 3. See also 'ANAO My Health Record Performance Audit Implementation Plan', 20 February 2020, and Appendix A, 'Implementation scope for ANAO recommendations'.

[54] Appendix A, 'Implementation scope for ANAO recommendations', p. 12.

[55] Health-ADHA, *Submission 1*, p. 2. See 'ANAO My Health Record Performance Audit Implementation Plan', 20 February 2020, and Appendix A, 'Implementation scope for ANAO recommendations'. ADHA noted that the plan was approved by the ADHA Board and incorporates ANAO quality indicators for implementation of audit recommendations, Health-ADHA, *Submission 1*, p. 3.

[56] Ms Bettina McMahon, Acting Chief Executive Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 2. The ANAO is also an observer on ADHA's audit and risk committee, which 'plays an oversight role to provide assurance that we're implementing the plan', Ms McMahon, p. 2.

3.31 Asked about the assistance to entities of such implementation plans in addressing recommendations, the Auditor-General observed that 'we think setting up those types of frameworks is the best practice way of driving implementation'—the best chance of successfully implementing recommendations is to 'have a plan and for it to be monitored, usually through the audit and risk committee. That will put some accountability in terms of who's going to do things and by when'.[57]

3.32 There was interest at the public hearing in further exploring ADHA's timeframes for implementing the recommendations, noting that the ADHA Implementation Plan 'does not cover the actual changes which the Agency and others must make to implement the recommendations; this detail will be developed in 2020 through the activities described in the plan'.[58] ADHA provided an update on its 'indicative timeline', confirming that the first two milestones had been completed (plan approval and analysis).[59] Engagement was due to be conducted from March to July 2020, but ADHA 'shifted that back slightly to take into account the availability of stakeholders', with this instead commencing in April and now 'likely to run through to the end of July or August'.[60] ADHA advised that 'the final completion date is October next year, which is within the two-year time frame that we've articulated we'll implement each of the recommendations'.[61]

3.33 As to whether there had been any impact on implementation timeframes due to COVID-19, ADHA confirmed:

> Yes, absolutely. That is the reason why stakeholders are less available … we're cognisant of the capacities, particularly around emergency access—there are people working in hospitals and running health services who we need to consult with ... We want to work around their availability rather than forging ahead.[62]

---

[57] Mr Grant Hehir, Auditor General, ANAO, *Committee Hansard*, 19 May 2020, p. 2.

[58] 'ANAO My Health Record Performance Audit Implementation Plan', 20 February 2020, p. 5.

[59] Ms Bettina McMahon, Acting Chief Executive Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 1.

[60] Ms Bettina McMahon, Acting Chief Executive Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 1. ADHA indicated that this engagement would 'consider other aspects of the health system that also control privacy and security risks', such as professional indemnity insurance, Health- ADHA, *Submission 1*, p. 2. (See, for example, MIGA, *Submission 5*, p. 3.)

[61] Ms Bettina McMahon, Acting Chief Executive Officer, ADHA, *Committee Hansard*, 19 May 2020, pp. 2-3.

[62] Ms Bettina McMahon, Acting Chief Executive Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 3.

3.34 It was also noted that ADHA's Implementation Plan made reference to funding sensitivities, with the plan stating that:

> execution of the solutions … is scheduled to commence in August 2020, however, funding is not secured for the Agency beyond June 2020 … If resourcing is not available in the 2020/21 budget, execution on the plan would largely shift to FY 2021/22, which could put all recommendations within two years at risk (particularly recommendation 4 which calls for implementation of the compliance framework).[63]

3.35 However, ADHA confirmed at the public hearing that it does now have 'sufficient funding to implement these recommendations':

> at the time we developed the implementation plan, we didn't have the funding … for the next financial year. We do now have funding, which was provided through the supply bills in March, through to the end of January … activities both in this financial year and the next financial year to implement the recommendations are funded.[64]

Concluding Comment

3.36 The audit concluded that implementation of the My Health Record system was largely effective.[65] The Committee understands that implementation planning for and delivery of My Health Record under the opt-out model was effective in promoting achievement of its purposes, and implementation planning and execution was appropriate and supported by appropriate governance arrangements.[66] Communication activities were also appropriate to inform healthcare recipients and providers; risk management for the My Health Record expansion program was partially appropriate; and monitoring and evaluation arrangements for My Health Record were largely appropriate.[67]

3.37 Specifically on cyber resilience, the Committee notes the audit finding that ADHA had managed risks to the core infrastructure of the My Health Record system through establishing a Digital Health Cyber Security Centre; undertaking a series of dedicated cyber security assessments; and

---

[63] 'ANAO My Health Record Performance Audit Implementation Plan', 20 February 2020, p. 16.

[64] Ms Bettina McMahon, Acting Chief Executive Officer, ADHA, *Committee Hansard*, 19 May 2020, p. 2.

[65] Auditor-General Report No. 13 (2019-20), p. 7.

[66] Auditor-General Report No. 13 (2019-20), p. 7.

[67] Auditor-General Report No. 13 (2019-20), pp. 7-8.

implementing the 'Essential Eight' cyber security mitigation strategies and decreasing the number of ISM cyber security controls not implemented.[68]

3.38 The My Health Record system needs to take into account both effectively maintaining an appropriate level of privacy and cyber security, and providing ease of access to the system for healthcare professionals and others to encourage high levels of engagement.[69] Under My Health Record, ADHA shares cyber security risks with many other participants, including the NIO and subcontractors; Services Australia; software vendors; healthcare provider organisations and their contracted service providers; and individual healthcare recipients. The Committee appreciates that this creates additional challenges because there needs to be coordination between various agencies to manage shared risk.

3.39 Against this background, the audit found that ADHA's approach to managing shared cyber security risks needed to be improved, by ADHA developing an assurance framework for third party software connecting to the My Health Record system in accordance with the ISM, and implementing a strategy to monitor compliance with mandatory legislated security requirements by registered healthcare provider organisations and contracted service providers.[70]

3.40 The Committee notes that ADHA has agreed to these recommendations and that it provided an update at the public hearing on implementation progress. ADHA has also published an Implementation Plan, with indicative timeframes.

3.41 The Committee appreciates that the COVID-19 pandemic has had an impact on ADHA's implementation timeframes for the audit recommendations, particularly given that a significant part of this work involves engaging with key stakeholders across the Health community.[71] However, the Committee notes that the current Implementation Plan 'does not cover the actual changes which the Agency and others must make to implement the recommendations; this detail will be developed in 2020 through the

[68] Auditor-General Report No. 13 (2019-20), p. 9.

[69] Auditor-General Report No. 13 (2019-20), p. 21.

[70] Auditor-General Report No. 13 (2019-20), p. 10.

[71] Health-ADHA, *Submission 1*, p. 3. See also 'ANAO My Health Record Performance Audit Implementation Plan', 20 February 2020, and Appendix A, 'Implementation scope for ANAO recommendations'.

activities described in the plan'.[72] Accordingly, the Committee seeks an update on the key milestones and implementation dates for the audit recommendations, particularly recommendations 3 and 4 relating to cyber security.

Recommendation 6

3.42 The Committee recommends that the Australian Digital Health Agency (ADHA) provide an update on its 'ANAO My Health Record Performance Audit Implementation Plan' (20 February 2020), including:

- **key milestones and implementation dates for each of the recommendations in Auditor-General Report No. 13 (2019-20), *Implementation of the My Health Record System*, with a particular focus on recommendations 3 and 4; and**
- **details of the specific changes that ADHA and other stakeholders need to make to implement the recommendations.**

3.43 The Committee understands that, while Auditor-General Report No. 13 (2019-20) examined My Health Record cyber security risks, it was not a specific cyber audit.[73] Auditor-General Report No. 1 (2019-20) noted that the 'small number' of government business enterprises (GBEs) and corporate Commonwealth entities assessed to date means 'it is not possible to draw conclusions as to the relative level of cyber resilience of corporate compared to non-corporate Commonwealth entities'.[74] Noting this point and the cyber related recommendations directed at ADHA in Auditor-General Report No. 13, the Committee believes there would be merit in ADHA (as a corporate Commonwealth entity) being included in a future cyber audit of GBEs and corporate Commonwealth entities.

[72] 'ANAO My Health Record Performance Audit Implementation Plan', 20 February 2020, p. 5.

[73] Auditor-General Report No. 13 (2019-20), p. 41. The Auditor-General advised 'we reported that, effectively, they had provided assurance that they met the mandatory four and the top eight. We didn't do an independent assessment of those things in that audit like we do in the cyberaudits', Mr Grant Hehir, Auditor-General, ANAO, *Committee Hansard*, 19 May 2020, p. 9.

[74] Auditor-General Report No. 1 (2019-20), *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*, p. 43.

Ms Lucy Wicks MP
Chair

3 December 2020

A. Submissions

1 Department of Health and Australian Digital Health Agency

2 ASC Pty Ltd

3 Mr Justin Warren

4 Australia Post

5 MIGA

6 Australian National Audit Office

- 6.1 Supplementary to submission 6
- 6.2 Supplementary to submission 6

7 Attorney-General's Department

- 7.1 Supplementary to submission 7
- 7.2 Supplementary to submission 7

8 Minister for Defence

9 Australian Signals Directorate

10 Department of Home Affairs

B. Public Hearings

Tuesday, 19 May 2020—Canberra

Australian Digital Health Agency

- Ms Bettina McMahon, Acting Chief Executive Officer
- Mr Ronan O'Connor, National Health Chief Information Officer

Department of Health

- Mr Daniel McCabe, First Assistant Secretary, Provider Benefits Integrity and Digital Health Policy
- Mr Simon Cleverley, A/g Assistant Secretary, Digital Health and Services Australia Branch

Australian National Audit Office

- Mr Grant Hehir, Auditor-General
- Mr Andrew Morris, Executive Director, Performance Audit Services Group
- Ms Lisa Rauter, Group Executive Director, Performance Audit Services Group

Australian Postal Corporation

- Mr John Cox, Chief Information Officer
- Mr Glen Stuttard, Chief Information Security Officer (Acting)

Reserve Bank of Australia

- Ms Susan Woods, Assistant Governor (Corporate Services)
- Mr Gayan Benedict, Chief Information Officer

Thursday, 2 July 2020—Canberra

Australian National Audit Office

- Mr Grant Hehir, Auditor-General
- Ms Lisa Rauter, Group Executive Director, Performance Audit Services Group

Department of Home Affairs

- Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy Division

Australian Signals Directorate

- Ms Jessica Hunter, Acting First Assistant Director-General, Protect, Assure and Enable
- Ms Abigail Bradshaw, Australian Cyber Security Centre

Attorney-General's Department

- Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group
- Ms Liz Brayshaw, Assistant Secretary, Security, Law and Policy Branch