

Cyber Security Strategies of Non-Corporate Commonwealth Entities

Across Entities

© Commonwealth of Australia 2021

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-634-9 (Print)

ISBN 978-1-76033-635-6 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <https://www.pmc.gov.au/government/its-honour>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Senior Executive Director
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:

communication@anao.gov.au.





Canberra ACT
19 March 2021

Dear Mr President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit across entities titled *Cyber Security Strategies of Non-Corporate Commonwealth Entities*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website — <http://www.anao.gov.au>.

Yours sincerely

A handwritten signature in black ink, reading 'Grant Hehir', is positioned below the 'Yours sincerely' text.

Grant Hehir
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
<http://www.anao.gov.au>

Audit team

Esther Barnes
Edwin Apoderado
David Willis
Jason Ralston
Carissa Chen
Kelvin Le
Lesa Craswell
Mark Rodrigues

Contents

| | |
|--|-----------|
| Summary and recommendations..... | 7 |
| Background | 7 |
| Conclusion | 9 |
| Supporting findings..... | 10 |
| Recommendations..... | 11 |
| Summary of entity responses | 14 |
| Key messages from this audit for all Australian Government entities | 17 |
| Audit findings..... | 19 |
| 1. Background | 20 |
| Introduction | 20 |
| Responsibilities of Australian Government entities | 20 |
| Cyber security framework..... | 26 |
| Previous audits and JCPAA inquiries | 30 |
| Rationale for undertaking the audit | 31 |
| Audit approach | 31 |
| 2. Implementation of cyber security risk mitigation strategies..... | 35 |
| Have the entities that reported full implementation of any of the Top Four cyber security risk mitigation strategies done so accurately? | 36 |
| If Top Four cyber security requirements have not been fully implemented, have the entities established effective strategies and actions to manage cyber risks? | 46 |
| 3. Support provided by the cyber policy and operational entities..... | 57 |
| Is there adequate technical guidance to support entities to accurately self-assess against the Essential Eight mitigation strategies and their underlying controls in the <i>Australian Government Information Security Manual</i> ? | 58 |
| Have the cyber policy and operational entities developed processes to verify the accuracy of entities' self-assessed reporting? | 68 |
| Have the cyber policy and operational entities established processes to improve the transparency and accountability of entities' implementation of mandatory cyber security requirements? | 76 |
| Appendices | 85 |
| Appendix 1 Entity responses | 86 |
| Appendix 2 Recommendation for the cyber policy entities in Auditor-General Report No.53 2017–18 <i>Cyber Resilience</i> and their respective responses | 100 |
| Appendix 3 2019–20 PSPF assessment questions for 'Policy 10: <i>Safeguarding information from cyber threats</i> ' | 103 |
| Appendix 4 Entities' views on the supporting guidance for PSPF Policy 10 self-assessment | 104 |



Audit snapshot

Auditor-General Report No.32 2020–21

Cyber Security Strategies of Non-Corporate Commonwealth Entities



Why did we do this audit?

- ▶ Malicious cyber activity has been identified as one of the most significant threats affecting government entities, businesses and individuals.
- ▶ Previous ANAO audits have identified low levels of compliance with mandatory cyber security requirements under the Protective Security Policy Framework (PSPF). The Joint Committee of Public Accounts and Audit has expressed its concern about entity implementation of these requirements.



Key facts

- ▶ Policy 10 of the revised PSPF outlines the mandatory requirements for entities to safeguard information from cyber threats.
- ▶ Entities assess their maturity under the PSPF against four maturity levels representing their assessed level of implementation of the requirements: Ad hoc, Developing, Managing and Embedded.
- ▶ The Attorney-General's Department (AGD), the Australian Signals Directorate (ASD) and the Department of Home Affairs have responsibilities in relation to cyber security policy and operational capability.



What did we find?

- ▶ The implementation of cyber security risk mitigation strategies by the selected entities was not fully effective, and did not fully meet the mandatory requirements of PSPF Policy 10.
- ▶ Two of three entities did not accurately self-assess implementation of one of the Top Four mitigation strategies for which they reported full implementation. None of these three entities were cyber resilient.
- ▶ The majority of the entities examined that had self-assessed a maturity level of 'Ad hoc' or 'Developing' have established strategies to progress toward a 'Managing' maturity level for PSPF Policy 10.
- ▶ AGD, ASD and Home Affairs could do more to improve support for the implementation of cyber security requirements.



What did we recommend?

- ▶ The Auditor-General made 13 recommendations aimed at improving entities' cyber security maturity levels, and the support and assurance provided by the three cyber policy and operational entities.

436

cyber security incidents reported by Australian Government entities to ASD in 2019–20.

24%

of non-corporate Commonwealth entities were compliant with the mandatory Top Four mitigation strategies in ANAO performance audits since 2014.

72%

of non-corporate Commonwealth entities reported not fully implementing PSPF Policy 10 in 2018–19.

Summary and recommendations

Background

1. The security of government information communications technology (ICT) systems, networks and data supports Australia's social, economic and national security interests as well as the privacy of its citizens. Malicious cyber activity has been identified as one of the most significant threats affecting Australians.¹ The frequency, scale and sophistication of malicious cyber activity is reported to be increasing², with cyber threats considered to be an increasing risk across Australian Government entities.³ The management of cyber security risk within the Australian Government public sector is the responsibility of individual entities.

2. Three Australian Government entities have responsibilities in relation to whole-of-government cyber security policy and operational support. In relation to cyber security:

- the Attorney-General's Department (AGD) is responsible for administering the Protective Security Policy Framework (PSPF), which provides the framework for Australian Government entities to achieve four protective security outcomes — governance, information security, personnel security and physical security;
- the Australian Signals Directorate (ASD) developed the Top Four mitigation strategies mandated by the PSPF and is a technical operational agency that provides material, advice and other assistance to Australian governments, business, communities and individuals on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means⁴; and
- the Department of Home Affairs (Home Affairs) is responsible for the development and coordination of the Australian Government's cyber security policy, and coordinating the implementation of Australia's Cyber Security Strategy 2020.

3. In February 2017, ASD re-issued its *Strategies to Mitigate Cyber Security Incidents*, which outlines 37 prioritised mitigation strategies to help protect entities from cyber threats. ASD has recommended that entities implement eight of these mitigation strategies, known as the Essential Eight, as a cyber security baseline. ASD also developed the Essential Eight Maturity Model to provide guidance to entities on how to implement the Essential Eight mitigation strategies and how to self-assess the maturity of their Essential Eight implementation. There are three maturity levels in the current Essential Eight Maturity Model — 'Maturity Level One', 'Maturity Level Two'

1 Australian Government, *Australia's Cyber Security Strategy 2020*, Department of Home Affairs, Canberra, 2020, p. 10.

2 Australian Cyber Security Centre, *ACSC Annual Cyber Threat Report July 2019 to June 2020*, Canberra, 2020, p. 4.

3 On 19 June 2020, the Prime Minister of Australia announced that Australian Government and non-government organisations were subject to targeting by malicious cyber activity against Australian networks. Prime Minister, Minister for Home Affairs and Minister for Defence, 'Statement on malicious cyber activity against Australian networks', media statement, 19 June 2020, available from <https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks> [accessed 15 March 2021].

4 Paragraph 7(1)(ca) of the *Intelligence Services Act 2001*.

and 'Maturity Level Three'. ASD recommends that entities should aim to reach 'Maturity Level Three' for each mitigation strategy as a baseline.

4. A revised PSPF commenced on 1 October 2018, outlining 16 core requirements that non-corporate Commonwealth entities must apply to achieve the four protective security outcomes. Non-corporate Commonwealth entities are to apply the revised PSPF using a security risk management approach. Policy 10 of the revised PSPF outlines the mandatory requirements for entities to safeguard information from common and emerging cyber threats. Policy 10 mandates the implementation of the Top Four mitigation strategies and that entities consider the implementation of the other mitigation strategies from ASD's *Strategies to Mitigate Cyber Security Incidents* that are relevant to their operational and risk environment.⁵ While not mandatory under Policy 10, AGD strongly recommends that entities implement the remaining four strategies that comprise the Essential Eight mitigation strategies.

5. Nine non-corporate Commonwealth entities were included in this audit:

- Attorney-General's Department;
- Australian Signals Directorate;
- Department of Home Affairs;
- Department of the Prime Minister and Cabinet (PM&C);
- Future Fund Management Agency (Future Fund);
- Australian Trade and Investment Commission (Austrade);
- Department of Education, Skills and Employment (DESE);
- Department of Health (Health); and
- IP Australia.

Rationale for undertaking the audit

6. Since 2013, the Australian Government has mandated the implementation of the Top Four mitigation strategies by non-corporate Commonwealth entities under the PSPF. The Australian Government has identified malicious cyber activity as one of the most significant threats affecting government entities, businesses and individuals. Previous ANAO audits have identified low levels of compliance with mandatory cyber security requirements under the PSPF. The Joint Committee of Public Accounts and Audit (JCPAA) has expressed its concern about entity implementation of mandatory cyber security requirements.

7. This audit seeks to address a recommendation made by the JCPAA in *Report 467: Cybersecurity Compliance*, for the Auditor-General to consider conducting an audit of the effectiveness of the PSPF self-assessment and reporting requirements for cyber security compliance. The audit also follows up on the recommendation made in Auditor-General Report No.53 2017–18 *Cyber Resilience*, for the responsible cyber policy and operational entities (AGD, ASD and Home Affairs) to work together to improve entities' compliance with mandatory cyber security requirements under the PSPF.

⁵ Policy 10 also sets out the supporting requirement to help entities safeguard information from cyber threats if they engage with members of the public online. The audit did not examine this supporting requirement under Policy 10.

Audit objective and criteria

8. The objective of the audit was to assess the effectiveness of cyber security risk mitigation strategies implemented by selected non-corporate Commonwealth entities to meet mandatory requirements under the PSPF, and the support provided by the responsible cyber policy and operational entities.

9. To form a conclusion against the audit objective, the ANAO adopted the following two high-level criteria:

- Have the selected entities fully implemented the Top Four cyber security risk mitigation strategies or otherwise adopted strategies and actions to progress towards full implementation?
- Have the entities responsible for cyber policy and operational capability 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?

Engagement with the Australian Signals Directorate

10. Independent timely reporting on the implementation of the cyber policy framework supports public accountability by providing an evidence base for the Parliament to hold the executive government and individual entities to account. Previous ANAO reports on cyber security have drawn to the attention of Parliament and relevant entities the need for change in entity implementation of mandatory cyber security requirements, at both the individual entity and framework levels.

11. In preparing audit reports to the Parliament on cyber security in government entities, the interests of accountability and transparency must be balanced with the need to manage cyber security risks. The Australian Signals Directorate has advised the ANAO that adversaries use publicly available information about cyber vulnerabilities to more effectively target their malicious activities.

12. The extent to which this report details the cyber security vulnerabilities of individual entities was a matter of careful consideration during the course of this audit. To assist in appropriately balancing the interests of accountability and potential risk exposure through transparent audit reporting, the ANAO engaged with the ASD to better understand the evolving nature and extent of risk exposure that may arise through the disclosure of technical information in the audit report. This report therefore focuses on matters material to the audit findings against the objective and criteria and contains less detailed technical information than previous audits. Detailed technical information flowing from the audit was provided to the relevant accountable authorities during the audit process to assist them to gain their own assurance that their remediation plans are focussed on improving cyber resilience as required and support reliable reporting through the existing cyber security framework.

Conclusion

13. The implementation of cyber security risk mitigation strategies by selected non-corporate Commonwealth entities under this audit was not fully effective. The selected entities have not met all mandatory requirements of PSPF Policy 10 in safeguarding information from cyber threats. While

the three cyber policy and operational entities have provided more support to entities to meet the mandatory PSPF Policy 10 requirements following Auditor-General Report No.53 2017–18 *Cyber Resilience*, additional ongoing work will be required to assist entities in achieving a more mature and resilient cyber security posture.

14. None of the seven selected entities examined have fully implemented all the mandatory Top Four mitigation strategies.⁶ For the three entities that had self-assessed full implementation for one or more of the Top Four mitigation strategies in their 2018–19 PSPF assessment, two had not done so accurately. None of these three entities were cyber resilient. Five of six selected entities that had self-assessed to have not fully implemented any of the Top Four mitigation strategies have established strategies and implemented activities to manage their cyber risks and to progress toward a ‘Managing’ maturity level for PSPF Policy 10.

15. The cyber policy and operational entities have worked together to provide more guidance following Auditor-General Report No.53 2017–18 *Cyber Resilience* to support non-corporate Commonwealth entities’ self-assessment of their implementation of cyber security requirements under the PSPF. There is scope to further improve the accuracy of entities’ PSPF Policy 10 assessments and strengthen arrangements to hold entities to account for the implementation of cyber security mandatory requirements. Robust accountability arrangements are particularly important in absence of public accountability through reporting to the Parliament.

Supporting findings

Implementation of cyber security risk mitigation strategies

16. PM&C and AGD have each not accurately self-assessed their implementation of one of the Top Four mitigation strategies. PM&C has not fully implemented the mitigation strategy for restricting administrative privileges. AGD has not fully implemented the mitigation strategy for patching operating systems. Future Fund has accurately self-assessed the two Top Four mitigation strategies for which it reported full implementation. None of the three entities were assessed as cyber resilient. Under the cyber security framework, PM&C and AGD are categorised as vulnerable to cyber security incidents as they have not fully implemented all the Top Four mitigation strategies and are continuing to strengthen the controls for managing cyber security incidents. Future Fund has not fully implemented all of the Top Four mitigation strategies, but is internally resilient as it has effective controls in place to support its ability to detect and recover from a cyber security incident.

17. Of the six entities that had reported not fully implementing all the Top Four mitigation strategies, five have established strategies and activities to progress their PSPF Policy 10 maturity level to ‘Managing’. The five entities have also included the implementation of the remaining four strategies that comprise the Essential Eight in their cyber security improvement programs. Three of the six entities had not set a corresponding timeframe to improve their PSPF Policy 10 maturity level to ‘Managing’. There is scope for four of the entities to improve monitoring of the implementation progress of their cyber security program to ensure that the entity is meeting the timeframe to improve its cyber security maturity.

6 ASD and Home Affairs are not included in this assessment. These entities were examined only in their roles as cyber policy and operational entities.

Support provided by the cyber policy and operational entities

18. The revised PSPF maturity assessment model has incorporated more guidance to support entities' self-assessment of their implementation of Policy 10 cyber security requirements. The AGD-developed PSPF Policy 10 guidance cross-references to multiple technical guidance developed by ASD, including guidance on the implementation of the Essential Eight mitigation strategies and the underlying security controls within the *Australian Government Information Security Manual*. There is scope to further improve the alignment of the maturity models for the PSPF and Essential Eight, and the clarity of the guidance to ensure more accurate PSPF Policy 10 self-assessments.

19. The cyber policy and operational entities have not developed processes to verify the accuracy of entities' PSPF Policy 10 self-assessed reporting. ASD has commenced the development of software tools that provide technical reporting to support entities in performing more accurate self-assessments of their Essential Eight implementation. While AGD and ASD have been sharing the results of the PSPF self-assessment reports and the ASD's ACSC Cyber Security Survey, the sharing of data has not yet resulted in obtaining assurance on the accuracy of the self-assessments and facilitating policy and technical assistance for entities.

20. With the release of the whole-of-government PSPF assessment reports by AGD and the annual Australian Government's cyber security posture report by ASD, there has been increased public reporting on non-corporate Commonwealth entities' implementation and maturity level of the Essential Eight mitigation strategies. However, the status of entities' cyber security posture is not transparent due to the policy and operational entities' concerns about increasing security risks following the disclosure of individual entities' cyber security maturity level. The cyber policy and operational entities have not established processes to improve the accountability of entities' cyber security posture. The current framework to support responsible Ministers in holding entities accountable within Government is not sufficient to drive improvements in the implementation of mandatory requirements.

Recommendations

Recommendation no.1 Paragraph 2.13

The Department of the Prime Minister and Cabinet strengthens its validation of privileged user access, specifically documenting the confirmation of the requirement for access from those that are responsible for approving privileged access.

Department of the Prime Minister and Cabinet response: *Agreed.*

Recommendation no.2 Paragraph 2.18

The Attorney-General's Department performs and documents risk assessments for any patches not implemented in accordance with the requirements of the *Australian Government Information Security Manual* and its policies, including defining an action plan for managing the risks associated with not implementing those patches.

Attorney-General's Department response: *Agreed.*

**Recommendation no.3
Paragraph 2.28**

The Department of the Prime Minister and Cabinet:

- (a) improve its risk assessment of security events; and
- (b) improve testing of security configurations and reviews of user access to ensure that the configurations are operating as intended.

Department of the Prime Minister and Cabinet response: *Agreed.*

**Recommendation no.4
Paragraph 2.34**

The Attorney-General's Department improves the processes for documenting risk assessments and monitoring cyber security events, to assure itself that actions taken against cyber security events are performed consistently and appropriately.

Attorney-General's Department response: *Agreed.*

**Recommendation no.5
Paragraph 2.53**

The Australian Trade and Investment Commission:

- (a) sets a timeframe to improve its cyber security maturity to the 'Managing' level for PSPF Policy 10; and
- (b) monitors the progress of the projects within its Cyber Security Work Program against the timeframe set for improving its PSPF Policy 10 maturity level.

Australian Trade and Investment Commission response: *Agreed.*

**Recommendation no.6
Paragraph 2.62**

The Department of Education, Skills and Employment:

- (a) sets a timeframe to improve its cyber security maturity to the 'Managing' level for PSPF Policy 10; and
- (b) monitors the progress of its Cyber Security Essential Eight Work Plan against the timeframe set for improving its PSPF Policy 10 maturity level.

Department of Education, Skills and Employment response: *Agreed.*

**Recommendation no.7
Paragraph 2.84**

The Attorney-General's Department:

- (a) develops a strategy and sets a timeframe to improve its cyber security maturity to the 'Managing' level for PSPF Policy 10;
- (b) provides clear reporting to its governance committees to enable oversight on the progress of its work to improve its Essential Eight maturity; and
- (c) monitors the progress of its work to improve its Essential Eight maturity against the set timeframe and through appropriate governance structures.

Attorney-General's Department response: *Agreed.*

**Recommendation no.8
Paragraph 2.92**

The Future Fund Management Agency monitors the progress of its Essential Eight improvement activities against the timeframe set for improving its PSPF Policy 10 maturity level.

Future Fund Management Agency response: *Agreed.*

**Recommendation no.9
Paragraph 3.37**

The Attorney-General's Department reviews the existing maturity levels under the PSPF maturity assessment model to determine if the maturity levels are fit-for-purpose and effectively aligned with the Essential Eight Maturity Model, having regard to the Australian Signals Directorate's proposed update to the Essential Eight Maturity Model.

Attorney-General's Department response: *Agreed.*

**Recommendation no.10
Paragraph 3.45**

The Attorney-General's Department further improves the guidance on PSPF Policy 10 to clarify:

- (a) the correlation of the maturity levels in the PSPF and Essential Eight maturity models, and their implementation requirements;
- (b) the scope of the maturity level calculation suggested by the reporting portal and how entities can more accurately determine their selected PSPF maturity level; and
- (c) the assessment against the requirement to consider the implementation of the remaining 29 mitigation strategies, and the merit of its inclusion in the PSPF Policy 10 maturity level calculation.

Attorney-General's Department response: *Agreed.*

**Recommendation no.11
Paragraph 3.66**

The Attorney-General's Department implements arrangements to obtain an appropriate level of assurance on the accuracy of entities' PSPF Policy 10 self-assessment results.

Attorney-General's Department response: *Agreed in principle.*

**Recommendation no.12
Paragraph 3.83**

As part of its technical advice and assistance to the Attorney-General's Department, the Australian Signals Directorate draw on its technical tools in addition to its existing capabilities to support the Attorney-General's Department's assurance processes on entities' PSPF Policy 10 self-assessment results.

Australian Signals Directorate response: *Agreed.*

Recommendation no.13
Paragraph 3.115

The Australian Government strengthens arrangements to hold entities to account for the implementation of mandatory cyber security requirements.

Attorney-General's Department response: *Noted.*

Australian Signals Directorate response: *Noted.*

Department of Home Affairs response: *Noted.*

Summary of entity responses

21. The proposed audit report was provided to the Attorney-General's Department, which administers the PSPF and the Australian Signals Directorate, which developed the Top Four mitigation strategies mandated by the PSPF. Extracts of the proposed report were also provided to the other seven selected entities involved in the audit. Summary responses provided by each of the nine selected entities are provided below.

Attorney-General's Department

The Attorney-General's Department (AGD) acknowledges ANAO's findings and welcomes the opportunity to comment on the Audit Report on Cyber Security Strategies of Non-Corporate Commonwealth Entities.

The Attorney-General's Department places a high priority on cyber security through its responsibility for administering the Protective Security Policy Framework (PSPF), and its own implementation of the framework.

The department remains committed to setting robust protective security standards for non-corporate Commonwealth entities. AGD has commenced review of the maturity model to ensure it is fit-for-purpose and aligned with Australian Signals Directorate (ASD) proposed update to the Essential 8 maturity model. AGD will continue to support entities to accurately self-assess and report on their implementation of cyber security requirements under the PSPF.

In relation to the department's own implementation of cyber security strategies, the department considers that it has a robust framework in place to manage cyber security risks. Implementation of the Top 4 mitigation strategies is part of a broader range of strategies implemented by the department. The department will continue to undertake activity to progressively uplift AGD's maturity level, with a view to achieving 'Managing' level for PSPF Policy 10. AGD also agrees to improve its processes for documenting ICT security risk assessments and related management processes.

AGD has accepted the majority of the 7 recommendations and is working towards implementation.

Australian Signals Directorate

As highlighted in the report, the Australian Signals Directorate (ASD) continues to support the whole of economy, including Commonwealth entities, to make Australia the safest place to connect online. We continue to enhance our capabilities to automate threat detection and intelligence sharing arrangements across the Commonwealth, coupled with our ongoing technical uplift program and engagements to harden Commonwealth entity networks against malicious cyber activity.

Cyber espionage remains a substantial threat to Australia's economic prosperity and the confidentiality, integrity and availability of key networks and data across government. Adversaries are constantly adapting their tradecraft to exploit vulnerabilities and avoid detection.

Department of Home Affairs

The Department welcomes the ANAO conclusion that cyber policy entities have worked together to support the implementation of cyber security requirements under the Protective Security Policy Framework.

Under the Minister for Home Affairs, the Department is responsible for national cyber security policy and overseeing the implementation of Australia's Cyber Security Strategy 2020 (the Strategy). The Strategy outlines a range of initiatives to uplift Australia's cyber security, including hardening government IT systems. This initiative is led by the Digital Transformation Agency and supported by the Australian Signals Directorate, the Department of Home Affairs and the Attorney-General's Department.

The Hardening Government IT Program involves the development of a new operating model to address the varying levels of cyber security maturity across Commonwealth entities, and through centralised 'cyber hubs' unifying the level of cyber resilience provided to all users of the hub.

While this initiative aims to strengthen Government's cyber security posture across Commonwealth entities, it is still under development. Any increase in accountability or transparency of mandatory cyber security requirements can be measured once this capability is operational.

The Department notes recommendation 13, and will brief the Government on the ANAO's findings and recommendations as they relate to national cyber security policy and implementation of Australia's Cyber Security Strategy 2020.

Department of the Prime Minister and Cabinet

At the Department of the Prime Minister and Cabinet (PM&C) we work very hard to maintain the highest standards in cyber security, underpinned by strong privacy and security protections, particularly as threats and targets rapidly evolve and shift. We work collaboratively with our staff to enhance the cyber security culture, constantly making sure our staff are cyber aware and vigilant, embedding behaviours as standard work practices.

With regard to the findings generally, we note that the Australian Cyber Security Centre (ACSC) provides broad guidance through the Information Security Manual (ISM) on control mechanisms that entities should put in place. We recognise agencies are encouraged to take a risk-based approach regarding the implementation of ACSC's security controls based on the agency's risk framework. On this basis, PM&C considers that it is compliant with all Top 4 Cyber Mitigations as effective risk controls are in place.

The ANAO assessed in its audit that PM&C is non-compliant with one of the Top 4 Cyber Mitigations. PM&C does not agree with the ANAO's assessment.

Specifically, the ANAO proposed additional processes regarding the detailed implementation of certain security controls, and on that basis considered PM&C non-compliant with one of the Top 4 Cyber Mitigations. PM&C has validation processes in place which adhere to the recommendations of the Information Security Manual and believes that this meets the requirement of the ISM and ACSC guidance.

We note that we will continue to make every effort to improve our processes and it is with this context I provide our response to the draft report. I accept recommendation 1 and 3 as they apply to the Department.

ANAO comment on Department of the Prime Minister and Cabinet summary response

22. As noted in paragraph 1.33, to meet the requirement of the PSPF, the ACSC's Essential Eight Maturity Model requires a minimum set of security controls be implemented to achieve 'Maturity Level Three'. PM&C was unable to provide evidence of the effective implementation of one of the security controls.

Future Fund Management Agency

The Future Fund Management Agency ("Agency") is committed to providing a secure cyber environment to safeguard the assets of the Commonwealth. Underpinning this is the full implementation of the Top Four of the Essential Eight mitigation strategies. The Agency expects to achieve full implementation of the Top Four mitigation strategies by the end of calendar year 2021.

Australian Trade and Investment Commission (Austrade)

Austrade agrees with the ANAO's findings.

Austrade will continue to run the Cyber Security Program of work that commenced in 2018 and will continue to review and evolve that work to address the broader cyber security risks to the organisation as well as those specific to the PSPF Policy 10.

Austrade acknowledges and appreciates the work being undertaken by the Australian Government entities with responsibilities in relation to whole-of-government cyber security policy and operational support and welcome their ongoing enhancements to the compliance framework.

Department of Education, Skills and Employment

The Department of Education, Skills and Employment ('the department') welcomes the ANAO's report on Cyber Security Strategies of Non-corporate Commonwealth Entities.

The department notes the key messages to all Australian Government entities in the audit report and agrees with the one recommendation provided to it.

The department is committed to managing cyber security risks and building a resilient cyber security posture. The department notes that, building on its Protective Security Policy Framework (PSPF) 2019-20 self-assessment report and associated external assessment, a workplan with timeframes for improving security maturity and achieving a 'Managing' maturity rating for PSPF Policy 10 has been developed and endorsed by the department's Executive Board. The department has implemented arrangements to monitor progress of the workplan.

Department of Health

The Department of Health (department) acknowledges the methodology and approach taken by the Australian National Audit Office (ANAO).

The department's Essential Eight Program is underway to uplift the maturity levels of its Essential Eight mitigation strategies by December 2021.

The department has a governance framework in place that ensures appropriate visibility of the Essential Eight program by the Senior Executive and the Audit and Risk Committee.

The department continues to work closely with the Australian Cyber Security Centre (ACSC) to improve its ability to detect and respond to a cyber-security incident.

IP Australia

IP Australia welcomes the report and its findings and the key messages for all Australian Government entities. We are committed to reaching our target maturity in line with the requirements of the Protective Security Policy Framework.

Key messages from this audit for all Australian Government entities

23. Below is a summary of key messages, including instances of good practice, which have been identified in this audit and may be relevant for the operations of other Australian Government entities.

Governance and risk management

- Independent timely reporting on the implementation of the cyber policy framework supports public accountability by providing an evidence base for the Parliament to hold the executive government and individual entities to account. The extent of public reporting should be appropriately balanced with the need to manage cyber security risks where adversaries could use published information about cyber vulnerabilities to more effectively target malicious activities. Strong accountability arrangements within government are required in the absence of public accountability through the Parliament.
- In order to mitigate cyber security incidents caused by cyber threats and meet the mandatory requirements of the framework, non-corporate Commonwealth entities must prioritise the implementation and maturity level of their Essential Eight mitigation strategies to strengthen their cyber security posture and manage the evolving threat environment.
- The effective implementation of cyber security mitigation strategies is underpinned by the identification of assets and risk assessments to identify the level of protection required from cyber threats.
- To meet the mandatory PSPF requirements of mitigating common and emerging cyber threats, it is important for entities to have effective risk management practices for cyber security. This includes conducting assessments of the effectiveness of security controls, security awareness training, and adopting a risk-based approach to prioritise improvements to cyber security.
- When establishing strategies and activities to progress toward implementation of mandatory requirements, entities should support governance oversight arrangements with clear plans including target milestones and accurate reporting against those milestones, to assist in determining the extent to which implementation activities are on track to achieve those milestones.

Policy design

- Policy owners are better positioned to judge the effectiveness of policy frameworks by establishing mechanisms to provide an appropriate level of assurance that mandatory requirements are being implemented as intended and are operating effectively.
- Entities with co-responsibilities for whole of government policy development and oversight should work together to develop clear and consistent guidance to support the achievement of the policy objectives.

Audit findings

1. Background

Introduction

1.1 Australian Government entities deliver a wide range of digital services to Australian businesses and the community. Australian Government entities also hold increasingly large volumes of data, some of which is highly sensitive, within information communications technology (ICT) systems and across their networks. Maintaining the security of government ICT systems, networks and data will support Australia's social, economic and national security interests, as well as the privacy of its citizens.

1.2 The Australian Government has identified malicious cyber activity as one of the most significant threats affecting government entities, businesses and individuals.⁷ The frequency, scale, and sophistication of malicious cyber activity is reported to be increasing.⁸ Among all Australian organisations, based on the visibility of the Australian Cyber Security Centre (ACSC), government entities are regularly targeted by malicious cyber actors. In the period July 2019 to June 2020, there were 436 cyber security incidents⁹ reported to the ACSC by Australian Government entities.¹⁰ Cyber threats¹¹ are an increasing risk across Australian Government entities.¹²

Responsibilities of Australian Government entities

1.3 Under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), accountable authorities of Australian Government entities must establish and maintain an appropriate system of risk oversight and management for the entity, and an appropriate system of internal control for the entity.¹³ The management of cyber security risk is the responsibility of individual entities. Entities are responsible for maintaining the security of their own ICT systems, networks and information holding.

1.4 There are three Australian Government entities with responsibilities for the policy framework and technical operational capability on cyber security:

- the Attorney-General's Department (AGD);
- the Australian Signals Directorate (ASD); and

7 Australian Government, *Australia's Cyber Security Strategy 2020*, Department of Home Affairs, Canberra, 2020, p. 10.

8 Australian Cyber Security Centre, *ACSC Annual Cyber Threat Report July 2019 to June 2020*, Canberra, 2020, p. 4.

9 According to the ACSC, a cyber security incident is 'an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations'.

10 Australian Cyber Security Centre, *ACSC Annual Cyber Threat Report July 2019 to June 2020*, Canberra, 2020, p. 7.

11 According to the ACSC, a cyber threat is 'any circumstance or event with the potential to harm systems or information'.

12 On 19 June 2020, the Prime Minister announced that Australian Government and non-government was subject to targeting by malicious cyber activity against Australian networks. Prime Minister, Minister for Home Affairs and Minister for Defence, 'Statement on malicious cyber activity against Australian networks', media statement, 19 June 2020, available from <https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks> [accessed 15 March 2021].

13 Under the PGPA Act, an accountable authority is the person or group of persons responsible for, and with control over, the operations of the Commonwealth entity.

- the Department of Home Affairs (Home Affairs).

Attorney-General's Department

1.5 In relation to cyber security, AGD is responsible for administering the Protective Security Policy Framework (PSPF), which provides the framework for Australian Government entities to achieve the following four protective security outcomes. Safeguarding an entity's information from cyber threats is a PSPF requirement under the information security outcome.

- **Governance** — each entity manages security risks and supports a positive security culture in an appropriately mature manner ensuring: clear lines of accountability; sound planning, investigation and response, assurance and review processes; and proportionate reporting.
- **Information security** — each entity maintains the confidentiality, integrity and availability of all official information.
- **Personnel security** — each entity ensures its employees and contractors are suitable to access Australian Government resources, and meet an appropriate standard of integrity and honesty.
- **Physical security** — each entity provides a safe and secure physical environment for their people, information and assets.

1.6 A revised PSPF commenced on 1 October 2018 following the *Independent Review of Whole-of-Government Internal Regulation* (Belcher Review). The revised PSPF outlines 16 core requirements that entities must apply to achieve the four protective security outcomes.¹⁴ The revised PSPF also includes changes to improve clarity and foster a strengthened security culture across government entities to effectively engage with risk.¹⁵ The revised PSPF also has an 'increased focus on cyber security matters' to support the achievement of the information security outcome.¹⁶

1.7 Policies 9, 10 and 11 of the revised PSPF reflect the broader cyber security requirements for entities to achieve the information security outcome. Policy 10 of the PSPF outlines the mandatory requirements for entities to safeguard information from common and emerging cyber threats.¹⁷ Policy 9 and Policy 11 define security requirements for mitigating general security risks to ICT systems and information.¹⁸ While the security requirements under Policies 9, 10 and 11 contribute to the mitigation of cyber security incidents, the implementation of the mitigation strategies under

14 There were 36 mandatory requirements in the previous PSPF that applied up until 30 September 2018. The revised PSPF consolidated the previous mandatory requirements into 16 core requirements from 1 October 2018.

15 Attorney-General's Department, *News* [Internet], 1 October 2018, available from <https://www.protectivesecurity.gov.au/about/Pages/News.aspx> [accessed 15 March 2021].

16 Attorney-General's Department, *Summary of key changes* [Internet], Protective Security, available from <https://www.protectivesecurity.gov.au/sites/default/files/PSPF-fact-sheet-summary-of-key-changes.pdf> [accessed 15 March 2021].

17 Policy 10 mandates the implementation of the Top Four mitigation strategies and the consideration of the remaining mitigation strategies from *Strategies to Mitigate Cyber Security Incidents*.

18 Policy 9 mandates that in managing access to information systems holding sensitive or security classified information, entities implement unique user identification, authentication and authorisation practices on each occasion where system access is granted. Policy 11 mandates each entity to ensure the secure operation of their ICT systems to safeguard information and the continuous delivery of government business through the application of the *Australian Government Information Security Manual's* cyber security principles in all stages of each system's lifecycle.

Policy 10 has the potential to mitigate the majority of cyber security incidents. As an Australian Government policy, the PSPF applies to non-corporate Commonwealth entities subject to the PGPA Act.¹⁹ Entities are to apply the revised PSPF using a security risk management approach.

Australian Signals Directorate

1.8 In relation to cyber security, ASD developed the Top Four mitigation strategies mandated by PSPF Policy 10 and is responsible for providing better practice guidance and assistance to Australian governments, business, communities and individuals.²⁰ ASD's role includes providing material, advice and other assistance on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means.²¹ The ACSC is a group within ASD that leads the Australian Government's efforts to improve national cyber security.²²

1.9 Since February 2017, ASD has outlined a list of 37 prioritised mitigation strategies in its published guidance on *Strategies to Mitigate Cyber Security Incidents*, designed to help protect entities from cyber threats.²³ ASD has recommended that entities implement eight of these mitigation strategies, known as the Essential Eight, as a cyber security baseline.²⁴ According to ASD, implementation of the Essential Eight baseline as outlined in Table 1.1, will make it more difficult for adversaries to compromise entities' systems.

Table 1.1: Essential Eight mitigation strategies recommended by ASD

| Mitigation strategy | About the strategy | Why implement the strategy? |
|--|---|--|
| Strategies to prevent malware delivery and execution | | |
| Application control ^a | Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers. | All non-approved applications (including malicious code) are prevented from executing. |
| Patch applications | Patch applications such as Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications. | Security vulnerabilities in applications can be used to execute malicious code on systems. |

19 The PSPF represents better practice for corporate Commonwealth entities and Commonwealth companies.

20 Australian Signals Directorate, *Annual Report 2019–20*, ASD, 2020, p. 21.

21 Paragraph 7(1)(ca) of the *Intelligence Services Act 2001*.

22 Australian Signals Directorate, *Cyber security* [Internet], ASD, available from <https://www.asd.gov.au/cyber> [accessed 15 March 2021].

23 In February 2010, ASD released a list of 35 strategies to assist entities to mitigate the risk of cyber intrusions.

24 In 2010, ASD advised that the Top Four mitigation strategies (application whitelisting, patching applications, restricting administrative privileges and patching operating systems) would prevent at least 85 per cent of targeted cyber intrusions if fully implemented. In 2017, ASD updated its recommended cyber security risk mitigation strategies from the Top Four to the Essential Eight. The update included mitigation strategies to address the increasing threat of ransomware and the evolution of tradecraft used, as the Top Four mitigation strategies in isolation was no longer sufficient as a baseline.

| Mitigation strategy | About the strategy | Why implement the strategy? |
|--|---|---|
| Configure Microsoft Office macro settings | Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate. | Microsoft Office macros can be used to deliver and execute malicious code on systems. |
| User application hardening | Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers. | Applications such as Flash, ads and Java are popular ways to deliver and execute malicious code on systems. |
| Strategies to limit the extent of cyber security incidents | | |
| Restrict administrative privileges | Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing. | Administration accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems. |
| Patch operating systems | Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions. | Security vulnerabilities in operating systems can be used to further the compromise of systems. |
| Multi-factor authentication | Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository. | Stronger user authentication will make it harder for adversaries to access sensitive information and systems |
| Strategies to recover data and system availability | | |
| Daily backups | Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes. | To ensure information can be accessed following a cyber security incident (such as a ransomware incident). |

Note a: The April 2020 updates to the *Australian Government Information Security Manual* included the renaming of 'application whitelisting' to 'application control' to reflect industry accepted terminology.

Source: Adapted from ASD's guidance on *Essential Eight Explained*.

1.10 According to ASD, entities can protect their systems and information from cyber threats through applying the principles of govern, protect, detect and respond. The four principles involve identifying cyber security risks (govern), implementing security controls to reduce risks (protect), detecting cyber security incidents (detect), and responding to and recovering from cyber security incidents (respond). The *Australian Government Information Security Manual* defines cyber resilience as follows:

Cyber resilience is the ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents.²⁵

1.11 The 2019–20 Federal Budget included a measure on *Whole-of-Government – Cyber Uplift for Federal Government Systems and for the 2019 Federal Election* (Cyber Uplift Program) to strengthen the cyber security of Australian Government networks and mitigate potential cyber threats through enhanced monitoring and response capabilities.²⁶

1.12 The Cyber Uplift Program included the conduct of Essential Eight+ Sprints by ASD, which aimed to baseline and improve the maturity of Australian Government entities' Essential Eight mitigation strategies. ASD conducted the Essential Eight+ Sprint program between April 2019 and December 2019 in 25 Australian Government entities. ASD applied a standardised data-driven assessment methodology to all 25 Commonwealth entities to consistently assess and rate the entities' maturity in implementing the Essential Eight mitigation strategies using the Essential Eight Maturity Model (see paragraphs 1.34 and 1.35).

Department of Home Affairs

1.13 With respect to cyber security, the role of Home Affairs is to lead the development of the Australia-wide cyber security policy. It is responsible for cyber security policy coordination and setting the strategic direction of the Australian Government's cyber security effort. It is also responsible for coordinating the implementation of Australia's Cyber Security Strategy 2020.²⁷

1.14 Australia's Cyber Security Strategy 2020 was launched on 6 August 2020. According to the strategy, the Australian Government plans to invest \$1.67 billion over 10 years in cyber security, including:

- protecting the critical infrastructure that Australians depend on;
- stronger defences for Australian Government networks and data;
- increased situational awareness and improved sharing of threat information;
- advice for small and medium enterprises to increase their cyber resilience;
- stronger partnerships with industry through the Joint Cyber Security Centre program; and
- improved community understanding of cyber security threats.²⁸

Whole-of-government cyber security oversight committees

1.15 There are four whole-of-government governance committees with responsibilities in overseeing PSPF and cyber security initiatives for the improvement of Australian Government entities' cyber security posture:

- Government Security Committee;

25 Australian Signals Directorate, *Australian Government Information Security Manual* [Internet], ASD, Australia, 2020, p. 12, available from <https://acsc.gov.au/infosec/ism/index.htm> [accessed 15 March 2021].

26 The expenditure for this measure was listed in Budget Paper No. 2 as not for publication due to national security reasons.

27 Both ASD and AGD contributed to the development of Australia's Cyber Security Strategy 2020.

28 Australian Government, *Australia's Cyber Security Strategy 2020*, Department of Home Affairs, Canberra, 2020, p. 6.

- Cyber Security Band 3 Inter-Departmental Committee;
- Cyber Security Strategy Delivery Board; and
- Secretaries Board.

Government Security Committee

1.16 The role of the Government Security Committee is to provide oversight of the PSPF. The Government Security Committee is chaired by the Deputy Secretary of AGD, with ASD and Home Affairs as members. The Government Security Committee's terms of reference set its responsibilities as:

- providing strategic oversight of whole-of-government protective security policy;
- promoting the consistent, efficient and effective application of security policies in Australian Government entities;
- coordinating strategic level policy and operational responses to emerging protective security threats and issues, and;
- providing advice to the Secretaries Board, Secretaries Committee on National Security, Cyber Security Band 3 Inter-Departmental Committee and the Government on significant security matters where appropriate.

1.17 The Government Security Committee oversees reporting to government by AGD on the maturity and capability of entities' to achieve security outcomes, and issues arising from specific or aggregated risks impacting on government security outcomes.

Cyber Security Band 3 Inter-Departmental Committee

1.18 The role of the Cyber Security Band 3 Inter-Departmental Committee is to improve whole-of-government information sharing and coordination of cyber security issues across the Australian Government, as well as to improve Australia Government's cyber security capability. The committee's responsibilities also include providing strategic oversight and guidance on the development, implementation and evaluation of Australia's Cyber Security Strategy 2020, and monitoring entities' implementation of whole-of-government cyber security measures. The committee discusses the management of cyber security risks through education, workplace skills and technical considerations. Home Affairs co-chairs this committee with the Department of the Prime Minister and Cabinet. AGD and ASD are members of the committee. The committee may raise significant issues to the Secretaries Committee on National Security or the Secretaries Board where appropriate.

Cyber Security Strategy Delivery Board

1.19 The Cyber Security Strategy Delivery Board was set up following the release of Australia's Cyber Security Strategy 2020 to drive the implementation of the strategy. Membership of the Cyber Security Strategy Delivery Board comprises Senior Executive Service Band 1 level representatives. Home Affairs chairs the Cyber Security Strategy Delivery Board, with AGD and ASD as members.

Secretaries Board

1.20 The role of the Secretaries Board includes identifying strategic priorities for and considering issues that affect the Australian Public Service. The Secretaries Board also has responsibility for

developing and implementing strategies to improve the Australian Public Service. The Secretary of the Department of the Prime Minister and Cabinet chairs the Secretaries Board.²⁹

Cyber security framework

1.21 The key elements of the Australian Government cyber security framework are outlined in:

- PSPF Policy 10: *Safeguarding information from cyber threats*;
- PSPF Policy 5: *Reporting on security* (sets out the PSPF maturity self-assessment model);
- Essential Eight Maturity Model;
- *Australian Government Information Security Manual*;
- *Strategies to Mitigate Cyber Security Incidents*;
- PSPF Policy 9: *Access to information*; and
- PSPF Policy 11: *Robust ICT systems*.

PSPF Policy 10: *Safeguarding information from cyber threats*

1.22 In April 2013, the Australian Government mandated the implementation of the Top Four of the ASD prioritised mitigation strategies by non-corporate Commonwealth entities under the PSPF. The Top Four mitigation strategies — application whitelisting, patching applications, restricting administrative privileges, patching operating systems — were part of INFOSEC-4, which was one of the mandatory requirements in the previous PSPF under the information security outcome. The previous PSPF INFOSEC-4 set out the requirements for implementing cyber and ICT system security.

1.23 As discussed in paragraph 1.6, there is increased prominence of cyber security matters in the October 2018 revised PSPF. Policy 10 in the revised PSPF replaces the cyber security requirements in the previous INFOSEC-4 policy.³⁰ Policy 10 in the revised PSPF sets out the mandatory requirement for safeguarding information against cyber threats, as shown in Box 1.³¹

Box 1: Mandatory requirements of PSPF Policy 10

Each entity must mitigate common and emerging cyber threats by:

- (a) implementing the following mitigation strategies from the *Strategies to Mitigate Cyber Security Incidents*:
 - i. application control
 - ii. patching applications
 - iii. restricting administrative privileges
 - iv. patching operating systems
- (b) considering which of the remaining mitigation strategies from the *Strategies to Mitigate Cyber Security Incidents* you need to implement to protect your entity.

Source: Adapted from PSPF Policy 10: *Safeguarding information from cyber threats*.

29 The Secretaries Board was established and governed by section 64 of the *Public Service Act 1999*.

30 As discussed previously, Policy 9 and Policy 11 in the revised PSPF set out the mandatory requirements for safeguarding ICT systems from cyber threats. Policy 9 replaces INFOSEC-5 and Policy 11 replaces INFOSEC-6.

31 Policy 10 also sets out the supporting requirement to help entities safeguard information from cyber threats if they engage with members of the public online. Policy 10 outlines suggested actions for entities to reduce cyber security risk to the public when they transact online with Australian Government entities.

1.24 Policy 10 refers to ASD's *Strategies to Mitigate Cyber Security Incidents* and explicitly mandates the Top Four mitigation strategies. The Top Four strategies are part of the ASD's Essential Eight mitigation strategies as outlined in Table 1.1. In addition to the Top Four mitigation strategies, Policy 10 also mandates that entities consider the implementation of the other mitigation strategies from ASD's *Strategies to Mitigate Cyber Security Incidents* that are relevant to their operational and risk environment.³² While not mandatory under Policy 10, AGD strongly recommends that entities implement the remaining four strategies that comprise the ASD's Essential Eight baseline mitigation strategies.

PSPF maturity self-assessment model

1.25 Since 2013, non-corporate Commonwealth entities have been required to undertake an annual self-assessment against the mandatory requirements of the PSPF. Entities report their overall compliance with mandatory requirements to AGD. According to the consolidated PSPF compliance reports published by AGD, INFOSEC-4 had the highest rate of self-assessed non-compliance from 2014–15 to 2017–18 compared to the other mandatory requirements in the previous PSPF. In 2018–19, only 28 per cent of non-corporate Commonwealth entities reported full implementation of the mandatory requirements of PSPF Policy 10.

1.26 From 2018–19, entities are required to report on their security capability using a maturity assessment model instead of a compliance assessment model. PSPF Policy 5: *Reporting on security* sets out the new maturity self-assessment model for annual PSPF reporting. Under the maturity self-assessment model, entities assess and report on their level of implementation and management of the requirements under the PSPF and the maturity of their security capability. The annual PSPF assessment report is to show the extent to which an entity has:

- achieved the security outcomes for governance, information, personnel and physical security;
- implemented and managed the mandatory and supporting requirements that it must meet to achieve the four protective security outcomes;
- identified the key security risks to its people, information and assets; and
- implemented strategies and timeframes to manage identified and unmitigated risks.

1.27 AGD has developed an online PSPF reporting portal to support the implementation of the new maturity self-assessment model. The PSPF reporting portal allows entities to complete and submit their annual PSPF assessment online, access benchmarking and assessment reports from previous reporting periods.³³ The accountable authority of an entity is responsible for approving the entity's self-assessment.

1.28 Entities are required to provide their PSPF assessment report to the relevant portfolio Minister and AGD each financial year. The due date of entities' PSPF assessment report is 31 August each year. Due to the impacts of the COVID-19 pandemic, the submission date for the 2019–20 PSPF

32 This mandatory requirement for entities to consider all of the mitigation strategies in ASD's *Strategies to Mitigate Cyber Security Incidents* was included in PSPF Policy 10 in November 2019 to ensure that entities do not treat the Essential Eight as the only recommended mitigation strategies for their systems.

33 The PSPF reporting portal has been authorised to process and store information classified as PROTECTED and below. Entities that report information higher than PROTECTED are required to use an offline reporting template for their self-assessment.

assessment report was initially extended to 30 September 2020. Following requests from entities, AGD further extended the submission due date to 15 October 2020.

Assessment of implementation and maturity levels under the PSPF

1.29 The maturity self-assessment model requires entities to assess their security capability and implementation of the requirements in the PSPF policies within the context of their specific risk environment and risk tolerances. To assess the maturity of the implementation of each PSPF policy, entities are to consider their effectiveness in implementing the mandatory and supporting requirements for each policy. Entities assess the effectiveness of their implementation of the PSPF requirements against four different levels — ‘Partial’, ‘Substantial’, ‘Full’ and ‘Excelled’. Descriptions for each implementation level are outlined in Table 1.2.





Table 1.2: Implementation levels of PSPF requirements

| Implementation level | Description |
|----------------------|--|
| Partial | Requirement is not implemented, is partially progressed or is not well-understood across the entity. |
| Substantial | Requirement is largely implemented but may not be fully effective or integrated into business practices. |
| Full | Requirement is fully implemented and effective and is integrated, as applicable, into business practices. |
| Excelled | Requirement and relevant better-practice guidance are proactively implemented in accordance with the entity’s risk environment, are effective in mitigating security risk and are systematically integrated into business practices. |

Source: Adapted from PSPF Policy 5: *Reporting on security*.

1.30 Based on entities’ assessment of their implementation of the requirements for each PSPF policy, the PSPF reporting portal calculates and suggests a maturity level for each policy.³⁴ There are four maturity levels under the PSPF maturity self-assessment model — ‘Ad hoc’, ‘Developing’, ‘Managing’ and ‘Embedded’. The description for each PSPF maturity level is outlined in Table 1.3.

Table 1.3: Maturity levels of the PSPF maturity self-assessment model

| Maturity level | Description |
|--|--|
| Ad hoc  | Partial or basic implementation and management of PSPF mandatory and supporting requirements. |
| Developing  | Substantial, but not fully effective implementation and management of PSPF mandatory and supporting requirements. |
| Managing  | Complete and effective implementation and management of PSPF mandatory and supporting requirements. |
| Embedded  | Comprehensive and effective implementation and proactive management of PSPF mandatory and supporting requirements and excelling at implementation of better-practice guidance. |

Source: Adapted from PSPF Policy 5: *Reporting on security*.

³⁴ Where applicable, entities’ assessment of its implementation of the supporting requirement of safeguarding information from cyber threats when transacting online with the public will also form part of the PSPF Policy 10 maturity level calculation.

1.31 Entities can confirm the suggested maturity level, or select a higher or lower maturity level for each PSPF policy, to reflect the assessment of their individual risk environment and risk tolerances. Entities must include a rationale to support their selected maturity level for a PSPF policy. If the selected maturity level is different to the suggested maturity level, entities should provide a justification in the rationale.³⁵

1.32 The PSPF specifies that the 'Managing' maturity level provides the minimum required level of protection of an entity's people, information and assets. If an entity's self-assessed maturity level for a PSPF policy is 'Ad hoc' or 'Developing', the entity is required to provide information in its assessment regarding the proposed strategies or implementation activities to improve the entity's maturity level to 'Managing'. The entity is also required to provide the associated timeframe for each strategy to achieve 'Managing' maturity.

1.33 PSPF Policy 10 includes guidance to entities on achieving PSPF maturity level of 'Managing'. Policy 10 states that:

To achieve a PSPF maturity rating of **Managing** for each of the four mandatory mitigation strategies from the Strategies to Mitigate Cyber Security Incidents, implement the maturity level three requirements as set out in the Essential Eight Maturity Model.³⁶ [Emphasis in original, the maturity levels are introduced at paragraph 1.29.]

Essential Eight Maturity Model

1.34 The Essential Eight Maturity Model was developed by ASD to provide guidance to entities on how to implement the Essential Eight mitigation strategies (see Table 1.1) in a phased approach and how to self-assess the maturity of their Essential Eight implementation. The Essential Eight Maturity Model was first published in June 2017, with five maturity levels. Changes had been made to the model since its publication. There are three maturity levels in the Essential Eight Maturity Model, as defined in Table 1.4.

Table 1.4: Maturity levels of the Essential Eight Maturity Model (as at October 2020)

| Maturity level | Description |
|----------------------|--|
| Maturity Level One | Partly aligned with the intent of the mitigation strategy. |
| Maturity Level Two | Mostly aligned with the intent of the mitigation strategy. |
| Maturity Level Three | Fully aligned with the intent of the mitigation strategy. |

Source: Adapted from the ACSC's Essential Eight Maturity Model.

1.35 The Essential Eight Maturity Model outlines the criteria for entities to achieve a specific maturity level with respect to entities' implementation of the Essential Eight mitigation strategies. ASD recommends that entities should aim to reach Maturity Level Three for each mitigation strategy as a baseline.

35 Based on the average of all the self-assessed maturity levels selected for each core requirement across the 16 PSPF policies, the portal calculates a stand-alone maturity rating for each of the four security outcomes. The portal subsequently calculates an overall maturity rating for the entity based the ratings for the security outcomes.

36 Attorney-General's Department, *Safeguarding information from cyber threats* [Internet], Protective Security, available from <https://www.protectivesecurity.gov.au/information/safeguarding-information-from-cyber-threats/Pages/default.aspx> [accessed 15 March 2021].

Previous audits and JCPAA inquiries

1.36 Since 2013–14, the Auditor-General has tabled a series of performance audits on Australian Government entities' cyber security and cyber resilience. Four of the audits examined cyber security and cyber resilience of non-corporate Commonwealth entities. One audit examined Government Business Enterprises and corporate Commonwealth entities.

- 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*.

1.37 The five performance audits found that Australian Government entities' compliance with mandatory requirements of the PSPF was generally low³⁷, and that the regulatory framework had not driven sufficient improvement in entities' cyber security. Only six of 17 entities examined (35 per cent) were compliant with the mandatory requirements for implementing all the Top Four cyber security risk mitigation strategies. Of these 17 entities, the ANAO also found that only six — the same six entities that were compliant with the Top Four requirements — were cyber resilient.³⁸

1.38 Auditor-General Report No.53 2017–18 *Cyber Resilience* included a recommendation that the three entities responsible for cyber policy and operational capability (AGD, ASD and Home Affairs) work together to improve compliance with the revised PSPF framework by strengthening: the technical guidance that support entities' PSPF self-assessment, the processes for verifying the accuracy of entities' self-assessment, and the transparency and accountability of entities' compliance with the framework.³⁹

1.39 Auditor-General Report No.38 2019–20 *Interim Report on Key Financial Controls of Major Entities* included a review of the self-assessed level of compliance with the mandatory requirements of PSPF Policy 10 for 18 non-corporate Commonwealth entities. The review was undertaken to confirm the accuracy of the entities' reporting and identify cyber security risks that may impact the preparation of the entities' 2019–20 financial statements. Of the 18 entities reviewed by the ANAO, only one achieved the required PSPF Policy 10 maturity level of 'Managing'.

1.40 The Joint Committee of Public Accounts and Audit (JCPAA) published *Report 467: Cybersecurity Compliance* in October 2017. The report followed a JCPAA inquiry based on Auditor-General Report No.42 2016–17 *Cybersecurity Follow-up Audit*. The JCPAA made two recommendations for the ANAO in Report 467:

-
- 37 Auditor-General Report No.1 2019–20 *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities* found that two of the three entities assessed had implemented controls in line with the requirements of the Information Security Manual, including the Top Four and other mitigation strategies in the Essential Eight.
- 38 The four audits that were conducted across 14 non-corporate Commonwealth entities identified that only four entities (29 per cent) had complied with the mandatory Top Four requirements and were cyber resilient.
- 39 Appendix 2 sets out that recommendation made in Auditor-General Report No.53 2017–18 and the responses of the three cyber policy and operational entities to the recommendation.

- Recommendation 4 — The Committee recommends that the Auditor-General consider conducting an audit of the effectiveness of the self-assessment and reporting regime under the Protected Security Policy Framework;
- Recommendation 6 — The Committee recommends that in future audits on cyber security compliance, the ANAO outline the behaviours and practices it would expect in a cyber resilient entity, and assess against these.⁴⁰

1.41 In February 2020, the JCPAA commenced an inquiry to consider the cyber resilience of government entities and examined two Auditor-General's reports as part of the inquiry.⁴¹ One of these reports is Auditor-General Report No.1 2019–20 *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*.⁴² The JCPAA concluded its inquiry and published *Report 485: Cyber Resilience* in December 2020, after fieldwork for this audit was completed.

Rationale for undertaking the audit

1.42 Since 2013, the Australian Government has mandated the implementation of the Top Four mitigation strategies by non-corporate Commonwealth entities under the PSPF. The Australian Government has identified malicious cyber activity as one of the most significant threats affecting government entities, businesses and individuals. Previous ANAO audits have identified low levels of compliance with mandatory cyber security requirements under the PSPF. The JCPAA has expressed its concern about entity implementation of mandatory cyber security requirements.

1.43 This audit seeks to address a recommendation made by the JCPAA in *Report 467: Cybersecurity Compliance*, for the Auditor-General to consider conducting an audit of the effectiveness of the PSPF self-assessment and reporting requirements for cyber security compliance. The audit also follows up on the recommendation made in Auditor-General Report No.53 2017–18 *Cyber Resilience*, for the responsible cyber policy and operational entities (AGD, ASD and Home Affairs) to work together to improve entities' compliance with mandatory cyber security requirements under the PSPF.

Audit approach

1.44 The following nine non-corporate Commonwealth entities were selected for this audit:

- Attorney-General's Department;
- Australian Signals Directorate;
- Department of Home Affairs;
- Department of the Prime Minister and Cabinet;
- Future Fund Management Agency;

40 The ANAO addressed JCPAA's Recommendation 6 in Auditor-General Report No.53 2017–18 *Cyber Resilience*, ANAO Audit Insights published in July 2018 *Insights from Reports Tabled April to June 2018*, and Auditor-General Report No.1 2019–20 *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*.

41 During the 45th Parliament, the JCPAA commenced an inquiry into cyber resilience based on Auditor-General's Report No.53 2017–18 *Cyber Resilience* in February 2019. This inquiry lapsed when the JCPAA ceased to exist at the dissolution of the House of Representatives on 11 April 2019.

42 The other report examined was Auditor-General Report No.13 2019–20 *Implementation of My Health Record System*.

- Australian Trade and Investment Commission (Austrade);
- Department of Education, Skills and Employment;
- Department of Health; and
- IP Australia.

1.45 AGD, the ASD and Home Affairs were included in this audit due to their roles and responsibilities in relation to cyber security policy and operational capability in the Australian Government.

1.46 The remaining entities were included in this audit to provide coverage across each maturity category of 'Managing', 'Developing' and 'Ad hoc'.⁴³ The entities selected for the ANAO's review of cyber security risk mitigation strategies under this audit and their 2018–19 PSPF Policy 10 self-assessed maturity rating are outlined in Table 1.5.

Table 1.5: Selected entities and their 2018–19 PSPF Policy 10 self-assessed maturity rating

| Entity | Policy 10 maturity rating |
|---|---------------------------|
| Attorney-General's Department | Managing ^a ● |
| Department of the Prime Minister and Cabinet | Managing ● |
| Future Fund Management Agency | Developing ◐ |
| IP Australia | Developing ◐ |
| Australian Trade and Investment Commission (Austrade) | Ad hoc ◑ |
| Department of Education ^b | Ad hoc ◑ |
| Department of Health | Ad hoc ◑ |

Note a: The Attorney-General's Department informed its accountable authority in June 2020 that an error was identified by the ANAO during fieldwork relating to the Department's overall rating for Policy 10: *Safeguarding information from cyber threats* in its 2018–19 PSPF self-assessment. Its overall maturity rating for PSPF Policy 10 was reported as 'Managing'. This should have been reported as 'Developing'.

Note b: The ANAO had selected the Department of Education, Skills and Employment based on the 2018–19 PSPF self-assessment of the former Department of Education. An Administrative Arrangements Order made on 5 December 2019 consolidated the former Department of Education and the former Department of Employment, Skills, Small and Family Business to create the current Department of Education, Skills and Employment (DESE) with effect from 1 February 2020.

Source: Reported 2018–19 PSPF Policy 10 maturity rating for selected entities.

Audit objective, criteria and scope

1.47 The objective of the audit was to assess the effectiveness of cyber security risk mitigation strategies implemented by selected non-corporate Commonwealth entities to meet mandatory

⁴³ The ANAO did not select any entities from the 'Embedded' category due to it not being a representative cyber security maturity level of non-corporate Commonwealth entities. Based on the 2018–19 dataset provided by AGD to the ANAO, only two entities had a self-assessed maturity rating of 'Embedded'.

requirements under the PSPF, and the support provided by the responsible cyber policy and operational entities.

1.48 To form a conclusion against the audit objective, the ANAO adopted the following two high-level criteria:

- Have the selected entities fully implemented the Top Four cyber security risk mitigation strategies or otherwise adopted strategies and actions to progress towards full implementation?
- Have the entities responsible for cyber policy and operational capability 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?

1.49 The audit scope included the maturity self-assessments, the strategies, plans and activities adopted by selected entities that have not fully implemented mandatory requirements, and the implementation of recommendation made to the three cyber policy and operational entities (AGD, ASD and Home Affairs) in Auditor-General Report No.53 2017–18 *Cyber Resilience*.

1.50 The audit did not examine whether the selected entities met the supporting requirement of PSPF Policy 10, which requires entities to avoid exposing the public to unnecessary cyber security risks when they transact with government entities online. The audit also did not examine entities' implementation of the mandatory requirements under PSPF Policy 9 and Policy 11, which relate to appropriate access to official information and secure operation of ICT systems respectively.

1.51 Previous ANAO reports on cyber security included assessments of entities against a list of behaviours and practices developed by the ANAO that may assist entities in building a strong culture of cyber resilience.⁴⁴ The October 2018 revised PSPF requires accountable authorities to ensure that entity personnel and contractors are aware of their collective responsibility to foster a positive security culture.⁴⁵ PSPF Policy 2 outlines ten characteristics of a positive security culture, including recommendations that entities establish appropriate metrics to measure the security culture maturity. The ANAO noted that the selected entities were in the process of establishing these metrics at the time of audit fieldwork. The audit did not assess security culture given the recent updates and maturity of metrics.

1.52 In December 2020, the JCPAA published *Report 485: Cyber Resilience* and recommended that a dedicated section be created within the annual PSPF self-assessment questionnaire addressing the 13 behaviours and practices of a strong cyber resilience culture assessed in Auditor-General Report No.1 2019–20 *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*.⁴⁶ The JCPAA also recommended that the ANAO consider conducting an annual limited assurance review into the cyber resilience of Commonwealth entities, which would

44 Three ANAO reports have assessed entities' cyber resilience culture: Auditor-General Report No.37 2015–16 *Cyber Resilience*, Auditor-General Report No.53 2017–18 *Cyber Resilience* and Auditor-General Report No.1 2019–20 *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*.

45 PSPF Policy 2: *Management structures and responsibilities*.

46 JCPAA *Report 485: Cyber Resilience*, Recommendation 3, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/CyberResilience2019-20/Report [accessed 15 March 2021].

assess entities against the 13 behaviours and practices.⁴⁷ The ANAO will consider the JCPAA's recommendation in the development of its future audit work plan.

Audit methodology

1.53 In undertaking the audit, the ANAO:

- reviewed the selected entities' 2018–19 and 2019–20 PSPSF self-assessments for Policy 10: *Safeguarding information from cyber threats*;
- reviewed PSPF Policy 5: *Reporting on security*;
- assessed the security controls in selected systems of entities that have self-assessed as having fully implemented any of the Top Four mitigation strategies to verify the accuracy of their 2018–19 PSPF self-assessment. The ANAO also assessed whether these entities were cyber resilient based on the ACSC's prescribed strategies relating to detecting and responding to cyber security incidents;
- examined documentation collected from the selected entities relating to their cyber security strategies and activities, including: security risk assessments undertaken, project plans for cyber security improvement programs established, and records of minutes for any governance forums established for cyber security;
- interviewed relevant staff from the selected entities regarding their approaches in mitigating cyber security risks; and
- reviewed the guidance and processes developed by, and interviewed relevant staff from, the cyber policy entities to examine the approaches adopted to support accurate PSPF self-assessment and reporting.

1.54 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of \$639,385.

1.55 Team members for this audit were Esther Barnes, Edwin Apoderado, David Willis, Jason Ralston, Carissa Chen, Kelvin Le, Lesa Craswell and Mark Rodrigues.

47 JCPAA Report 485: *Cyber Resilience*, Recommendation 4, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/CyberResilience2019-20/Report [accessed 15 March 2021].

2. Implementation of cyber security risk mitigation strategies

Areas examined

This chapter examines whether the selected entities have fully implemented the mandatory Top Four mitigation strategies or otherwise adopted strategies and actions to progress towards full implementation. The chapter also examines whether those entities that reported full implementation of any of the Top Four mitigation strategies are cyber resilient.

Conclusion

None of the seven selected entities examined have fully implemented all the mandatory Top Four mitigation strategies. For the three entities that had self-assessed full implementation for one or more of the Top Four mitigation strategies in their 2018–19 PSPF assessment, two had not done so accurately. None of these three entities were cyber resilient. Five of six selected entities that had self-assessed to have not fully implemented any of the Top Four mitigation strategies have established strategies and implemented activities to manage their cyber risks and to progress toward a ‘Managing’ maturity level for PSPF Policy 10.

Areas for improvement

The ANAO made the following recommendations aimed at:

- the Department of the Prime Minister and Cabinet strengthening controls in relation to validating and assessing the security configurations for user access, and improving its event logging process;
- the Attorney-General's Department improving its processes for documenting risk assessments for implementation of patches and monitoring of cyber security events; and
- selected entities that had self-assessed a PSPF Policy 10 maturity level of ‘Ad hoc’ and ‘Developing’ to set a timeframe to improve its maturity level, have clear reporting to governance committees, and monitoring of the progress of the entity’s cyber security program against the set timeframe.

2.1 Policy 10 under the revised Protective Security Policy Framework (PSPF) specifies how non-corporate Commonwealth entities can safeguard their information assets from cyber threats. PSPF Policy 10 sets out that entities must implement four of the Essential Eight mitigation strategies (the Top Four) to mitigate common and emerging cyber threats. The Top Four mitigation strategies mandated by PSPF Policy 10 are application control, patching applications, restricting administrative privileges and patching operating systems.

2.2 In undertaking their annual self-assessments under the PSPF maturity assessment model, entities assess the effectiveness of their implementation of the Top Four mitigation strategies against four grading levels — ‘Partial’, ‘Substantial’, ‘Full’ and ‘Excelled’.⁴⁸ The description for each implementation level is outlined in Table 1.2. If an entity’s self-assessed maturity level for PSPF

48 As subsequently outlined in Table 3.1 and discussed in paragraph 3.19, ‘Partial’ implementation corresponds to ‘Ad hoc’ maturity, ‘Substantial’ implementation corresponds to ‘Developing’ maturity, ‘Full’ implementation corresponds to ‘Managing’ maturity, and ‘Excelled’ implementation corresponds to ‘Embedded’ maturity.

Policy 10 is 'Ad hoc' or 'Developing', which means that it has not fully implemented all the Top Four mitigation strategies, the entity is required to detail the proposed strategies and associated timeframes to improve its PSPF maturity level to 'Managing' (which requires full implementation of all the Top Four).

2.3 To assess the effectiveness of the selected entities' implementation of cyber security risk mitigation strategies to meet mandatory PSPF requirements, the ANAO:

- tested the security controls of three entities — the Department of the Prime Minister and Cabinet (PM&C), the Attorney-General's Department (AGD), and the Future Fund Management Agency (Future Fund) — that had reported full implementation of one or more of the Top Four mitigation strategies in their 2018–19 PSPF self-assessment to verify the accuracy of the assessment;
- assessed whether PM&C, AGD and Future Fund are cyber resilient; and
- reviewed the strategies and plans as well as the corresponding timeframes to reach full implementation of the Top Four mitigation strategies in selected entities that had self-assessed in their 2018–19 PSPF assessment report as not having full implementation of all the Top Four. The six entities are:
 - Australian Trade and Investment Commission (Austrade);
 - Department of Education, Skills and Employment (DESE)⁴⁹;
 - Department of Health (Health);
 - IP Australia;
 - AGD; and
 - Future Fund.

Have the entities that reported full implementation of any of the Top Four cyber security risk mitigation strategies done so accurately?

PM&C and AGD have each not accurately self-assessed their implementation of one of the Top Four mitigation strategies. PM&C has not fully implemented the mitigation strategy for restricting administrative privileges. AGD has not fully implemented the mitigation strategy for patching operating systems. Future Fund has accurately self-assessed the two Top Four mitigation strategies for which it reported full implementation. None of the three entities were assessed as cyber resilient. Under the cyber security framework, PM&C and AGD are categorised as vulnerable to cyber security incidents as they have not fully implemented all the Top Four mitigation strategies and are continuing to strengthen the controls for managing cyber security incidents. Future Fund has not fully implemented all of the Top Four mitigation strategies, but is internally resilient as it has effective controls in place to support its ability to detect and recover from a cyber security incident.

49 As discussed in Table 1.5, a Machinery of Government change in December 2019 consolidated the former Department of Education (Education) and former Department of Employment, Skills, Small and Family Business (Employment) into the Department of Education, Skills and Employment with effect from February 2020. The ANAO had selected DESE based on the 2018–19 PSPF self-assessment of Education.

2.4 PM&C, AGD and Future Fund each reported in their 2018–19 PSPF self-assessment that they had fully implemented one or more of the mandatory Top Four mitigation strategies. The three entities' self-assessment of their implementation of the Top Four mitigation strategies for 2018–19 is presented in Table 2.1.

Table 2.1: Entities' self-assessed implementation levels for the Top Four mitigation strategies in their 2018–19 PSPF assessment report

| Mitigation strategy | Self-assessed implementation level | | |
|---------------------------------------|------------------------------------|-------------|-------------|
| | PM&C | AGD | Future Fund |
| Application control | Full | Substantial | Substantial |
| Patching applications | Full | Substantial | Substantial |
| Patching operating systems | Full | Full | Full |
| Restricting administrative privileges | Full | Full | Full |

Source: Entities' 2018–19 PSPF self-assessments for Policy 10: *Safeguarding information from cyber threats*.

2.5 The ANAO verified the accuracy of the three entities' PSPF Policy 10 self-assessments through an assessment of their implementation level of the Top Four mitigation strategies, for which they had reported full implementation. To achieve full implementation for each of the Top Four mitigation strategies under PSPF Policy 10, entities are required to implement the 'Maturity Level Three' requirements set by the ACSC (see paragraphs 1.33 and 3.21). As outlined in Table 1.4, the ACSC defines 'Maturity Level Three' as 'fully aligned with the intent of the mitigation strategy'. To reach 'Maturity Level Three' for each of the Top Four, entities are required to:

- implement application control⁵⁰ on all workstations and servers to restrict execution of unapproved or malicious programs and Microsoft's latest recommended block rules to prevent application control bypasses;
- patch security vulnerabilities assessed as extreme risks in applications and operating systems⁵¹ 48 hours from vendor release; use an automated mechanism to confirm and record that patches have been installed; and update or replace unsupported applications and operating systems; and
- restrict administrative access⁵² to that required for personnel to undertake their duties; validate privileged access when first requested and revalidate on an annual or more frequent basis; and prevent privileged users from accessing email and Internet.

2.6 The ANAO also assessed whether the three entities are cyber resilient. As noted in paragraph 1.10, the *Australian Government Information Security Manual* (ISM) defines cyber resilience to include the ability to detect and recover from cyber security incidents. The ACSC's guidance on *Strategies to Mitigate Cyber Security Incidents* includes prioritised mitigation strategies

50 Application control is a security approach in which only approved applications are allowed to execute on systems. When successfully implemented it can prevent the execution and spread of malicious code.

51 Patches are issued by vendors when they become aware of security vulnerabilities. Applying patches or updates in a timely manner is critical to prevent adversaries running malicious code on known vulnerabilities.

52 Privileged users are a subset of users that can change or bypass a system's security controls. Restricting administrative privileges and monitoring privileged users can prevent or limit an adversary from accessing systems following a cyber intrusion.

for detecting and responding to cyber security incidents, and for recovering data and system availability. The ANAO assessed the three entities' cyber resilience based on the entities' implementation and operating effectiveness of relevant ISM requirements relating to:

- the Top Four mitigation strategies, assessed against the implementation levels of the PSPF maturity assessment model; and
- mitigation strategies for continuous incident detection and response⁵³, and daily backups⁵⁴, assessed against the Essential Eight Maturity Model.⁵⁵

Accuracy of entities' PSPF Policy 10 self-assessments

Department of the Prime Minister and Cabinet

2.7 PM&C self-assessed as having fully implemented all the mandatory Top Four mitigation strategies in its 2018–19 PSPF self-assessment.

Application control

2.8 The ANAO assessed that PM&C has fully implemented the requirements for application control. PM&C has a documented and endorsed application control strategy. Any changes to the application control policy must be approved by the PM&C cyber security team. PM&C has implemented application control in both workstations and servers. PM&C blocks applications with known vulnerabilities across its workstations and servers in line with the latest Microsoft guidance.

Patching applications

2.9 The ANAO assessed that PM&C has fully implemented the requirements for patching applications. PM&C has a formalised patch management process for applications with patching timeframes aligned with ISM requirements. Patches are deployed automatically to all PM&C workstations by the information communications technology (ICT) operations team. The ANAO reviewed a sample of applications on workstations and found that all were patched and meeting the requirements of the ISM and PM&C policy. PM&C uses an automated tool to manage and confirm that patches have been installed. The ANAO's review also found that all applications in use in PM&C's environment were vendor-supported versions.

Patching operating systems

2.10 The ANAO assessed that PM&C has fully implemented the requirements for patching operating systems. PM&C has a formalised patch management process for operating systems with patching timeframes aligned with ISM requirements. Patches are deployed automatically to all PM&C workstations and manually to PM&C servers by the ICT operations team. The ANAO reviewed

53 Continuous incident detection and response is achieved through automated immediate analysis of logs of allowed and denied computer events. Effective event logging supports investigations into, and responses to, a cyber security incident.

54 Backups of data, software and configuration settings can be made and stored separately from the rest of the IT environment. Daily backups can ensure that information is not lost and can be restored quickly after a cyber security incident.

55 The ANAO selected these two mitigation strategies as they were rated as most effective by ASD in detecting, managing and recovering from cyber security incidents. The *Essential Eight to ISM Mapping* guidance does not define the Information Security Manual controls to be implemented for the mitigation strategy for continuous incident detection and response under the Essential Eight Maturity Model. The ANAO has adopted the ASD's model in our testing and assumed that all Information Security Manual controls relating to the strategy as being 'Essential'.

a sample of workstations and servers and found that all were patched and meeting the requirements of the Information Security Manual and PM&C policy. PM&C uses an automated tool to manage and confirm that patches have been installed. The ANAO's review also found that all operating systems in use in PM&C's environment were vendor-supported versions.

Restrict administrative privileges

2.11 The ANAO assessed that PM&C has partially implemented the requirements for restricting administrative privileges. The ANAO's assessment found that the following security controls are in place for restricting administrative privileges:

- security policies, standards and guidelines for granting and revoking privileged access to its systems; and
- privileged access users are restricted from accessing the Internet or email and have dedicated workstations segregated from other PM&C networks.

2.12 While PM&C has a process for validating privileged access on an annual basis, it does not sufficiently ensure that privileged access is restricted to personnel that require it to undertake their duties. Weaknesses in PM&C's validation processes increases the risk that a cyber intrusion could result in an adversary acquiring privileged access to its systems and subsequently change and bypass other security measures to compromise the system.

Recommendation no.1

2.13 The Department of the Prime Minister and Cabinet strengthens its validation of privileged user access, specifically documenting the confirmation of the requirement for access from those that are responsible for approving privileged access.

Department of the Prime Minister and Cabinet response: *Agreed.*

2.14 *PM&C has made changes to the revalidation process of administrative accounts, with additional processes being added to the PM&C primary network system security plan. PM&C considers that the process assessed by the ANAO was consistent with ACSC and ISM control recommendations. We note that no administrator access was found by the ANAO during the course of the audit that exceeded that individual's requirement to perform their duties.*

Attorney-General's Department

2.15 In its 2018–19 PSPF self-assessment, AGD reported that it had fully implemented two of the Top Four mitigation strategies — patching operating systems and restricting administrative privileges.

Patching operating systems

2.16 The ANAO assessed that AGD has 'substantially' implemented the requirements for patching operating systems. Further improvements should be made to reach full implementation. AGD has a formalised patch management process for operating systems with patching timeframes set to align with ISM requirements. Operating systems in use in AGD's environment during the ANAO's review were all still supported by vendors. Patches for workstations are managed through a multi-stage process by an operator before deployment to all workstations. Servers are patched manually by the AGD ICT operations team. AGD uses an automated tool to deploy patches in

addition to security vulnerability scanning tools to manage and confirm that patches have been installed. The ANAO reviewed a sample of workstations and found that workstations were patched and meeting AGD policy. AGD informed the ANAO that it decided to not use a vulnerability scanning tool across its whole environment. As a result, there is a risk that missed patches will not be detected.

2.17 The ANAO's review of servers found that some operating system patches had not been applied within ISM timeframes. The AGD cyber security team stated that this was due to the outage period for patches to be installed not being agreed upon by all business units. AGD did not perform risk assessments against the missed patches. AGD has since established agreed outage periods where these patches can be applied.

Recommendation no.2

2.18 The Attorney-General's Department perform and document risk assessments for any patches not implemented in accordance with the requirements of the *Australian Government Information Security Manual* and its policies, including defining an action plan for managing the risks associated with not implementing those patches.

Attorney-General's Department response: *Agreed.*

2.19 *The Attorney-General's Department (AGD) acknowledges the need to consistently document risk assessments relating to patches not applied in accordance with the Information Security Manual (ISM) and its policies. Where AGD operational or technical requirements delay application of patches, Information Division has an internal governance mechanism to assess the risk and monitor outstanding application of patches and associated risk. The risk assessment considers the risk to AGD systems taking into account the exposure to the internet of the specific systems affected and other preventative measures in place. In response to this recommendation, AGD is implementing a process to maintain a formal record of risk assessments undertaken.*

Restrict administrative privileges

2.20 The ANAO assessed that AGD has fully implemented the requirements for restricting administrative privileges. AGD has security policies, standards and guidelines for granting and revoking privileged access to its systems. The AGD information technology security adviser (ITSA) must approve access requests prior to users being granted administrative privileges. The ITSA validates that privileged access is restricted only to users with a business need. AGD validated privileged access on an annual basis. Privileged accounts cannot access the Internet unless they are members of an authorised group and for specific duties only. Users with privileged access use separate machines or logon environments to perform administrative duties.

Future Fund Management Agency

2.21 In its 2018–19 PSPF self-assessment, Future Fund reported that it had fully implemented two of the Top Four mitigation strategies — patching operating systems and restricting administrative privileges.

Patching operating systems

2.22 The ANAO assessed that Future Fund has fully implemented the requirements for patching operating systems. Future Fund has a Vulnerability Management Standard for applications and

operating systems with patching timeframes set to align with the ISM requirement. Future Fund uses automated tools to gather and deploy patches. The tools are configured to automatically deploy patches. Patches are first implemented in test groups before being deployed to the wider environment, where there is no negative impact on business. Future Fund also uses a combination of tools to confirm that patches are applied to workstations and servers within the ISM requirement. The ANAO reviewed a sample of operating systems and found that they were all patched within the Vulnerability Management Standard timeframes. All operating systems in use in the Future Fund environments reviewed by the ANAO were the vendor-supported versions.

Restrict administrative privileges

2.23 The ANAO assessed that Future Fund has fully implemented the requirements for restricting administrative privileges. Future Fund has security policies, standards and guidelines for granting and revoking privileged access to its systems. Privileged access is validated by the Future Fund cyber security team when first requested. The cyber security team reviews all privileged user accounts against each users' official duties on a quarterly basis to ensure that privileged access is limited only to personnel with a business need. Users with privileged access do not have separate machines, but have to authenticate using a jump server to perform administrative activities.

2.24 Future Fund's policies and security controls do not allow privileged accounts to access email or the Internet. However, the ANAO's assessment found that privileged user accounts could access the Internet. Future Fund was aware of this misconfiguration and stated that it was due to a recent update that had occurred during the ANAO's fieldwork. Future Fund remediated the non-compliance with its policy during the ANAO's fieldwork.

Entities' cyber resilience

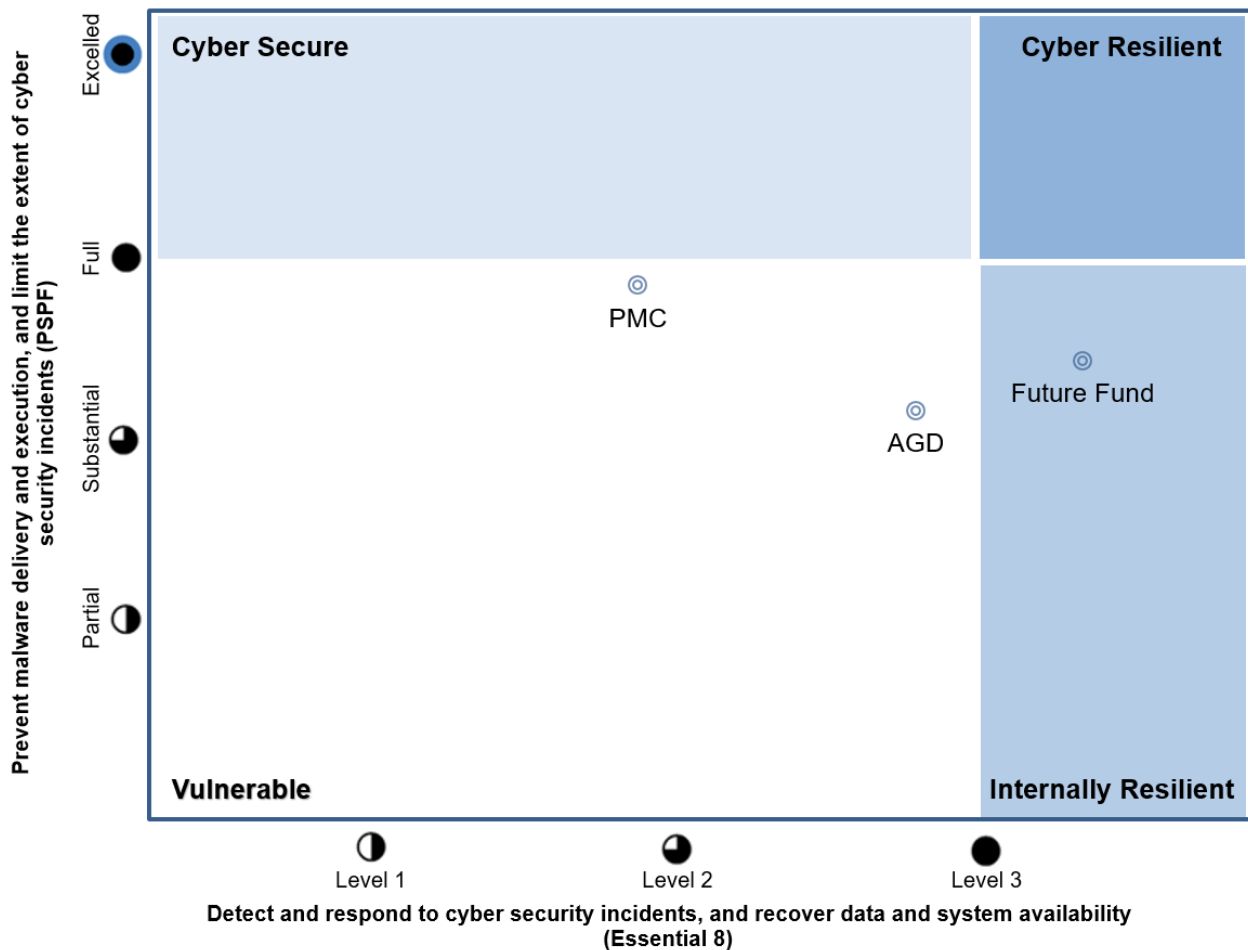
2.25 The ANAO assessed whether the three entities were cyber resilient by assessing each entity's degree of implementation of the Top Four strategies to mitigate cyber security incidents, and maturity level of its mitigation strategies for continuous incident detection and response and daily backups (see paragraph 2.6). The implementation levels of PSPF requirements and the maturity levels under the Essential Eight Maturity Model are described in Table 1.2 and Table 1.4 respectively. The matrix indicates where entities are positioned in terms of four security zones, as defined in Table 2.2. The entities' cyber resilience posture, as assessed by the ANAO, is presented in Figure 2.1.

Table 2.2: Definitions of security zones

| Zone | Definition |
|----------------------|--|
| Vulnerable | High level of exposure and occurrence of disruptions to business operations due to cyber security incidents. |
| Cyber secure | A level of protection to support the confidentiality, integrity and availability of systems and information. |
| Internally resilient | A level of measures to support the detection, management and recovery from cyber security incidents. |
| Cyber resilient | High level of measures to adapt to and protect against disruptions caused by cyber security incidents. |

Source: Developed by the ANAO based on ASD cyber security framework.

2.26 The PSPF outlines that the full implementation ('Managing' maturity) of all the Top Four mitigation strategies will provide the minimum level of protection to mitigate current cyber threats targeting Australian Government entities. PSPF Policy 10 also specifies that the implementation of 'Maturity Level Three' requirements as set out in the Essential Eight maturity Model will help to achieve a PSPF maturity rating of 'Managing'. Paragraph 3.30 describes the cyber security framework and differing maturity level requirements within the PSPF and Essential Eight Maturity Model. The cyber resilience assessment does not include consideration of the other remaining strategies from ASD's *Strategies to Mitigate Cyber Security Incidents*.

Figure 2.1: Entities' cyber resilience

Source: ANAO assessment of entities' cyber resilience posture.

Department of the Prime Minister and Cabinet

Continuous incident detection and response

2.27 PM&C has an event logging policy and has implemented a security information and event management (SIEM) system as its central event logging solution. PM&C's SIEM has been configured to analyse logs from PM&C workstations and servers for security events. PM&C does not have a robust process to ensure that it is monitoring all security events relevant to its environment. This weakness reduces PM&C's ability to manage cyber security threats.

Recommendation no.3

2.28 The Department of the Prime Minister and Cabinet:

- (a) improve its risk assessment of security events; and
- (b) improve testing of security configurations and reviews of user access to ensure that the configurations are operating as intended.

Department of the Prime Minister and Cabinet response: *Agreed.*

2.29 *Anomalies in our security event reporting (from our technical logging system) found by ANAO during the course of this audit have been investigated and addressed. Security event reporting is now working as intended. A risk assessment on the current security event system and processes has been completed, with any residual risk accepted by the department.*

2.30 *As part of our scheduled hardware upgrade process there is an active project in place to enhance our security event systems within PM&C which will also improve and streamline the risk assessment process.*

Daily backups

2.31 PM&C has documented standard operating procedures for backups. PM&C uses data protection software to backup its important data daily. Backups are stored offline and retained for six months. PM&C has a process for restoring and monitoring backups. Data restorations occurred frequently in response to user requests.

Cyber resilience posture

2.32 The ANAO's assessment found that PM&C's overall level of implementation for the Top Four mitigation strategies was 'Substantial' as it had implemented the majority of the Top Four strategies. The ANAO also found that PM&C had 'Maturity Level One' controls implemented for continuous incident detection and response and 'Maturity Level Three' controls implemented for daily backups. Under the cyber security framework, PM&C is therefore categorised to be in the 'Vulnerable' zone, which indicates that it is susceptible to cyber security incidents.

Attorney-General's Department

Continuous incident detection and response

2.33 AGD has an event logging policy and has implemented a SIEM as its central event logging solution. The AGD IT security team prioritises key security events and monitors the alerts generated by the SIEM in real-time. AGD has enabled event logging for the majority of its systems and has established mitigating controls to manage residual risks. AGD informed the ANAO that there was no documentation and formal approval of reviews. As a result, cyber security risks for which the SIEM has been implemented as a control against may impact AGD's ability to consistently manage security events.

Recommendation no.4

2.34 The Attorney-General's Department improves the processes for documenting risk assessments and monitoring cyber security events, to assure itself that actions taken against cyber security events are performed consistently and appropriately.

Attorney-General's Department response: *Agreed.*

2.35 *In 2020, AGD established a working group to review current cyber monitoring and alerting arrangements to identify and implement improvements. The activities of this working group are ongoing and responsive to the dynamic risk environment.*

2.36 *AGD is implementing a process to keep a formal record as verification of risk assessments undertaken and responses to cyber security monitoring alerts.*

Daily backups

2.37 AGD has documented standard operating procedures for backups. AGD uses data protection software to backup its important data daily. Backups are stored offline for seven years. AGD has a standard process for restoring backups. The ANAO reviewed AGD's change management register and observed that backups frequently occur in response to user requests and as part of system development and testing.

Cyber resilience posture

2.38 The ANAO's assessment found that AGD's overall level of implementation for the Top Four mitigation strategies was 'Substantial' as it had largely implemented the requirements for the Top Four mitigation strategies. The ANAO also found that AGD had 'Maturity Level Two' controls for continuous incident detection and response and 'Maturity Level Three' controls for daily backups. Under the framework, AGD is therefore categorised to be in the 'Vulnerable' zone, which indicates that it is susceptible to cyber security incidents.

Future Fund Management Agency

Continuous incident detection and response

2.39 Future Fund has an Event Logging Standard aligned to ACSC guidance. Future Fund uses an event logging tool to log security events for workstations. For servers, Future Fund uses a combination of tools to collect logs. Future Fund's logging tools have been effectively configured to automatically send alerts to the Future Fund security team. In addition to reviewing individual event alerts daily, Future Fund reviews alerts across key risk areas weekly. Future Fund appropriately documents the review and resolution of alerts.

Daily backups

2.40 Future Fund has documented standard operating procedures for backups. A range of tools are used to backup data at least daily. Future Fund stores backups offline for no maximum retention period. Health checks are performed on offline backups every two weeks. Future Fund policy requires an annual restoration test for backups. In July 2020, a full restoration of backups was performed, which identified no issues with the integrity of the data.

Cyber resilience posture







2.41 The ANAO's assessment found that Future Fund's overall level of implementation for the Top Four mitigation strategies was 'Substantial' as it had largely implemented the requirements for the Top Four mitigation strategies. The ANAO also found that Future Fund had 'Maturity Level Three' controls for continuous incident detection and response and daily backups. Under the framework, Future Fund is therefore categorised to be in the 'Internally Resilient' zone, which indicates that it has some measures in place to detect, manage and recover from cyber security incidents.

If Top Four cyber security requirements have not been fully implemented, have the entities established effective strategies and actions to manage cyber risks?

Of the six entities that had reported not fully implementing all the Top Four mitigation strategies, five have established strategies and activities to progress their PSPF Policy 10 maturity level to 'Managing'. The five entities have also included the implementation of the remaining four strategies that comprise the Essential Eight in their cyber security improvement programs. Three of the six entities had not set a corresponding timeframe to improve their PSPF Policy 10 maturity level to 'Managing'. There is scope for four of the entities to improve monitoring of the implementation progress of their cyber security program to ensure that the entity is meeting the timeframe to improve its cyber security maturity.

2.42 Austrade, the former Department of Education, Health and IP Australia each reported in their 2018–19 PSPF self-assessment for Policy 10 that they had not fully implemented any of the Top Four mitigation strategies. AGD and Future Fund reported that they had not fully implemented two of the Top Four mitigation strategies. The six entities' 2018–19 self-assessed Top Four implementation levels and selected maturity levels for PSPF Policy 10 is shown in Table 2.3.

Table 2.3: Entities' self-assessed Policy 10 maturity levels in their 2018–19 PSPF assessment report

| Entity | 2018–19 PSPF Policy 10 maturity level |
|------------------------|---|
| Austrade | Ad hoc  |
| Education ^a | Ad hoc  |
| Health | Ad hoc  |
| IP Australia | Developing  |
| AGD | Managing ^b  |
| Future Fund | Developing  |

Note a: See footnote 49. Prior to the Machinery of Government changes, the then Department of Employment, Skills, Small and Family Business (Employment) provided ICT infrastructure and desktop services to the then Department of Education (Education). In terms of the Top Four mitigation strategies, Employment was the owner of the relevant systems, policies and plans relating to three of the Top Four mitigation strategies for both former departments.

Note b: See Table 1.5, AGD incorrectly reported its overall PSPF Policy 10 maturity as 'Managing'. This should have been reported as 'Developing'.

Source: Entities' 2018–19 PSPF self-assessments for Policy 10: *Safeguarding information from cyber threats*.

2.43 If an entity self-assesses that it has not implemented all the Top Four mitigation strategies and thus has a maturity level of 'Ad hoc' or 'Developing' for PSPF Policy 10, it is required to detail the proposed strategies and timeframes to improve the entity's maturity level to 'Managing' (equivalent to full implementation of all the Top Four).

2.44 As the six selected entities in Table 2.3 had not fully implemented all the Top Four mitigation strategies and had a PSPF maturity level of 'Ad hoc' or 'Developing' for the 2018–19 reporting period⁵⁶, the ANAO reviewed whether they have established strategies and plans as well as corresponding timeframes to reach full implementation of the Top Four. To examine the effectiveness of the entities' strategies and plans to achieve full implementation of the Top Four, the ANAO assessed:

- whether the entities' strategies were informed by risk assessments or third party reviews, to support the management of cyber risks and address gaps in Top Four implementation; and
- whether the entities have appropriate governance structures in place to monitor the progress of their Top Four improvement strategies and to address emerging issues.

⁵⁶ The ANAO has included AGD in our testing although it selected 'Managing' as its Policy 10 maturity level. This is on the basis that AGD made an error in its Policy 10 maturity level assessment by rating itself at the 'Managing' level despite having not fully implemented all the Top Four mitigation strategies.

Austrade

2.45 Based on the responses Austrade provided to the questions for Policy 10, the PSPF reporting portal calculated a maturity level of 'Ad hoc' for Austrade's 2018–19 PSPF Policy 10 assessment. Austrade informed the ANAO that it undertook a separate assessment of its maturity level, based on its environment and the residual risks for those controls of the Essential Eight mitigation strategies that are yet to be fully implemented, and assessed its maturity level to be 'Developing'.

2.46 In 2018, Austrade commenced a Cyber Security Work Program to improve the maturity level of its Essential Eight mitigation strategies and its cyber security capability. The program of work comprises 10 projects. It includes projects that address each of the Top Four mitigation strategies, other Essential Eight as well as some of the remaining 29 mitigation strategies from ACSC's *Strategies to Mitigate Cyber Security Incidents* that Austrade has prioritised based on risks in its environment.

2.47 The Cyber Security Work Program does not include a set timeframe for Austrade to achieve 'Managing' maturity for PSPF Policy 10. Austrade informed the ANAO that the Cyber Security Work Program underway will help improve its cyber security maturity by June 2022. In its 2019–20 PSPF self-assessment Austrade outlined that it has prioritised projects for improving the maturity of the Top Four mitigation strategies, based on risk within its environment. These projects are planned to be progressively implemented and completed by June 2021.

2.48 Austrade has stated that it is not feasible in some cases to achieve 'Maturity Level Three' for some of the Essential Eight mitigation strategies. Under such circumstances, Austrade has indicated that it will identify alternative mitigation measures that will meet the intent of the Essential Eight.

2.49 Following the introduction of the revised PSPF in October 2018, Austrade also undertook a PSPF Reform Project that included the conduct of a gap analysis to measure Austrade's existing maturity levels against the updated PSPF requirements. Key activities were identified, including projects within the Cyber Security Work Program, with the intent of achieving a maturity rating of 'Managing' where reasonably practicable to do so. In early 2019, Austrade engaged a third party to undertake a security threat and risk assessment of its IT systems with a maturity assessment of its Essential Eight implementation. The report recommended work packages to improve Austrade's Essential Eight maturity levels, which informed the development of Austrade's Cyber Security Work Program.

2.50 The ACSC performed an Essential Eight+ Sprint at Austrade in the period July to August 2019. The findings from the ACSC's Essential 8+ Sprint have informed Austrade's prioritisation and progress of work packages under the Cyber Security Work Program.

2.51 Austrade provides regular reporting on its cyber security posture to its Executive as well as its various governance committees. The governance committees that provide assurance on Austrade's management of cyber security risk and implementation of cyber security risk mitigation strategies are the: Security Committee; Digital, Data and Information Committee; and Audit and Risk Committee. Austrade also participated in and provided updates on its Cyber Security Work Program at the Department of Foreign Affairs and Trade (DFAT) Portfolio Agencies ICT Cyber Steering Group.⁵⁷

57 The DFAT Portfolio Agencies ICT Cyber Steering Group plays a role in coordinating, governing and reporting on the resilience and hygiene of the cyber security posture of entities across the DFAT portfolio.

2.52 The ANAO's review of the meeting papers of the various governance committees identified that Austrade has reported to the committees the progress of its implementation of the projects within its Cyber Security Work Program. However, as noted at paragraph 2.47, the monitoring is not against a set timeframe for achieving 'Managing' maturity for PSPF Policy 10.

Recommendation no.5

2.53 The Australian Trade and Investment Commission:

- (a) sets a timeframe to improve its cyber security maturity to the 'Managing' level for PSPF Policy 10; and
- (b) monitors the progress of the projects within its Cyber Security Work Program against the timeframe set for improving its PSPF Policy 10 maturity level.

Australian Trade and Investment Commission response: *Agreed.*

2.54 *Austrade will more clearly link the Cyber Security program outcomes and timeframes to specific PSPF maturity levels. The Security Program will report on the progress towards those maturity levels and timeframes on a six monthly basis to the program sponsor, the Austrade Security Committee and the Austrade Audit and Risk Committee.*

Department of Education, Skills and Employment

2.55 DESE established a Cyber Security Essential Eight Work Plan in June 2020 as part of its Cyber Security Work Program. The Work Plan consists of projects to improve the maturity of DESE's implementation of the Essential Eight mitigation strategies. The Cyber Security Essential Eight Work Plan does not include a set timeframe for DESE to improve the maturity for each of the Essential Eight mitigation strategies or achieve 'Managing' maturity for PSPF Policy 10. DESE reported in its 2019–20 PSPF assessment that it is developing a revised work plan, which was due to be completed by December 2020, to continue its efforts in increasing the maturity of its Essential Eight implementation.

2.56 DESE has stated that for 2020 it will target 'Maturity Level Two' under the Essential Eight Maturity Model for two of the Top Four mitigation strategies⁵⁸ and the remaining non-mandatory Essential Eight mitigation strategies. According to DESE, there are elements of the Essential Eight mitigation strategies that are difficult to implement in its IT environment or where implementation would significantly impact its business operations and take considerable time. DESE has approved risk plans in place outlining the mitigation treatments where the Maturity Level 3 controls for a mitigation strategy are not met.

2.57 In April 2018 and July 2019, the then Department of Employment, Skills, Small and Family Business (Employment) engaged a third party to conduct a review of its cyber security posture and an assessment of its Essential Eight maturity level. In June 2020 following the consolidation of Employment and Education, DESE engaged the same third party to undertake a review of its PSPF maturity level to provide assurance to the DESE Executive on the accuracy of its self-assessed PSPF maturity levels for the 2019–20 reporting period. The external review included an assessment of

⁵⁸ DESE cited changes to the Information Security Manual and impact of the Machinery of Government changes as the reasons for the need to adjust the target maturity level for these two Top Four mitigation strategies.

all 37 strategies in ACSC's *Strategies to Mitigate Cyber Security Incidents* with a focus on the Essential Eight mitigation strategies, to identify gaps and recommend actions to improve DESE's maturity level. The external reviews and risk assessments on DESE's implementation of the Essential Eight mitigation strategies informed the development of its Cyber Security Essential Eight Work Plan.⁵⁹

2.58 ACSC performed an Essential Eight+ Sprint engagement at the then Employment during June 2019. The ACSC's findings have been used by DESE to inform the projects under its Cyber Security Essential Eight Work Plan.

2.59 The key governance committees that provide oversight of DESE's Cyber Security Essential Eight Work Program are: a steering committee; the Risk, Security and Governance Committee; and the Executive Board.

2.60 The DESE Chief Security Officer has received monthly updates on the progress of the projects under the Cyber Security Essential Eight Work Plan, and has been provided a Cyber Security Dashboard report that includes information on the implementation status of the Top Four mitigation strategies. In June 2020, the DESE Executive Board received its first cyber security update from the Chief Information Security Officer. The briefing covered DESE's efforts to improve its maturity against the Essential Eight and the Cyber Security Dashboard report on the implementation status of the Top Four mitigation strategies.

2.61 The ANAO's review of the reporting to the Chief Security Officer, the steering committee meetings and the Executive Board meetings identified that there was monitoring of the completion status and progress of the Essential Eight projects under the Cyber Security Work Program. There was also monitoring of the implementation status of the Top Four mitigation strategies. However, as noted at paragraph 2.55, the monitoring is not against an agreed timeframe for improving the maturity for each of the Essential Eight mitigation strategy or achieving 'Managing' maturity for PSPF Policy 10.

59 DESE informed the ANAO that the output of the June 2020 external review would inform the development of the revised December 2020 Cyber Security Essential Eight Work Plan.

Recommendation no.6

2.62 The Department of Education, Skills and Employment:

- (a) sets a timeframe to improve its cyber security maturity to the 'Managing' level for PSPF Policy 10; and
- (b) monitors the progress of its Cyber Security Essential Eight Work Plan against the timeframe set for improving its PSPF Policy 10 maturity level.

Department of Education, Skills and Employment: Agreed.

2.63 *The department agrees with the recommendation. The department notes that, building on its Protective Security Policy Framework (PSPF) 2019-20 self-assessment report and associated external assessment, a workplan with timeframes for improving security maturity and achieving a 'Managing' maturity rating for PSPF Policy 10 has been developed and endorsed by the department's Executive Board. The department has implemented arrangements to monitor progress of the workplan.*

Department of Health

2.64 Since 2018–19, Health has been undertaking a program of work to improve its implementation of the Essential Eight mitigation strategies. In early 2020, Health developed a revised Essential Eight Program to ensure that the Essential Eight mitigation strategies are implemented across its ICT environment at the targeted maturity level and within specified timeframe. The Essential Eight Program comprises three project streams. Each project stream consists of individual work packages for each of the Essential Eight mitigation strategies.

2.65 Health has developed a schedule with proposed timeframes to meet the implementation requirements of the Essential Eight mitigation strategies. In its 2019–20 PSPF self-assessment Health outlined that it has a program to progressively improve its maturity against the Top Four mitigation strategies. The program is scheduled to achieve Maturity Level Three by December 2021.

2.66 In early 2020, Health undertook an assessment of its Essential Eight mitigation strategies based on the risks and threats against its operating environment and its baseline Essential Eight maturity levels to determine the strategies it needed to prioritise.

2.67 Health engaged a third party to undertake an Essential Eight compliance architecture review. The review analysed the Essential Eight maturity baseline of Health's environment in each of its domains, examined the gap in achieving 'Maturity Level Three' for the Essential Eight and provided recommendations on the best approach to achieve the target maturity level. The review took into consideration Health's assessment on its Essential Eight priorities. The Essential Eight priorities assessment and the architecture review informed the development of Health's Essential Eight Program.

2.68 Health has introduced a process within its Essential Eight Program to exempt an Essential Eight mitigation strategy from reaching 'Maturity Level Three' where the risk is acceptable for Health to attain a lower maturity level. Health has identified constraints, within its operating environment, to achieve 'Maturity Level Three' for some of the Essential Eight mitigation

strategies.⁶⁰ The exemption is to be approved by the Chief Security Officer. Approvals have been provided by the Chief Security Officer to exempt Health from achieving 'Maturity Level Three' for two of the non-mandatory Essential Eight mitigation strategies.

2.69 Health has established a program board to oversee delivery of expected program outcomes. The program board provides oversight on the progress of the Essential Eight Program to ensure that program risk, cost, quality and timelines are being tracked and managed effectively.⁶¹ The program board reports quarterly to the Security and Workforce Integrity Assurance Committee (SWIAC). The SWIAC meets quarterly to discuss security and workforce integrity risks and activities to mitigate those risks by various business areas. The SWIAC provides updates to the Executive Committee quarterly, including the progress of the Essential Eight Program.

2.70 The ANAO's review of the Essential Eight Program Board meeting papers identified that the program board has been monitoring the status and progress of the implementation of the individual Essential Eight work packages under the Essential Eight Program. The meeting papers showed that the program board was tracking the timeframes of the Essential Eight Program. There is no evidence in the meeting papers to indicate that Health is not meeting the timeframe it has set for improving the maturity levels of its Essential Eight mitigation strategies.

2.71 In August 2020, an update on Health's PSPF maturity levels was provided to the SWIAC. The SWIAC was advised of Health's self-assessed PSPF maturity levels for the four protective security outcomes as at 30 June 2020 and its forecast PSPF maturity levels as at 30 June 2021. As a result of the various improvement activities underway, Health is expecting to achieve an improvement in its overall PSPF maturity levels for all four outcomes to the 'Developing' or 'Managing' level by June 2021.

IP Australia

2.72 In October 2019, IP Australia commenced a project to progress towards 'Maturity Level Three' of the Essential Eight Maturity Model for its implementation of the Essential Eight mitigation strategies. In July 2020, IP Australia developed a Security Uplift Program to bring together a number of IT security initiatives, including the Essential Eight project, under one program. The Security Uplift Program was approved by the Business Investment Committee⁶² to be a Tier 1 project in June 2020.⁶³ The Security Uplift Program identifies improving against the Top Four mitigation strategies as a priority.

60 To seek an exemption, an exemption report is required to be completed providing an overview of the exemption details (including current approach and future mitigations), exemption timeframe and the risk assessment undertaken.

61 The Terms of Reference of the Essential Eight Program Board provides that the program board reports relevant security and risk issues as required to the ICT Security and Risk Committee. Prior to the establishment of the Essential Eight Program Board in early 2020, Health ICT Security team was reporting monthly to the ICT Security and Risk Committee. The ANAO's review of the ICT Security and Risk Committee meeting minutes found that the committee was provided with updates on the progress of Health's Essential Eight maturity initiatives.

62 The Business Investment Committee was replaced by the Investment, ICT and Property Committee in October 2020 and is chaired by the Director-General.

63 A Tier 1 project is identified as being high risk and a significant investment by IP Australia. Tier 1 projects are required to have oversight by the Investment, ICT and Property Committee.

2.73 The Security Uplift Program identifies ‘Maturity Level Three’ as the target state for IP Australia. The Security Uplift Program has a work plan, which outlines a number of initiatives and milestones to the end of 2022–23. The business case for the Security Uplift Program states that projects to improve maturity against the Top Four mitigation strategies will be prioritised based on risk. The initiatives under the work plan are ongoing and are scheduled to achieve ‘Maturity Level Three’ by June 2023.

2.74 In July 2018, an internal audit was undertaken to assess the appropriateness of IP Australia’s plans to address gaps and improve its maturity against the Essential Eight. IP Australia agreed to the audit recommendations that it formalise and document the processes used to monitor and report on its Essential Eight maturity. The internal audit findings were used to inform IP Australia’s work to improve its Essential Eight maturity. IP Australia has another internal audit planned for the fourth quarter of 2020–21. This internal audit will be informed by the outcomes of IP Australia’s participation in the Department of Industry, Science, Energy and Resources’ Portfolio Security Uplift Program which commenced in July 2020.

2.75 ACSC performed an Essential Eight+ Sprint engagement at IP Australia in the period November to December 2019 and found a lower level of maturity compared with the 2018 internal audit. The findings from the ACSC’s Essential Eight+ Sprint have informed IP Australia’s prioritisation and progress of work packages under the Security Uplift Program.

2.76 IP Australia has a process in place to exempt IT solutions from meeting the ‘Maturity Level Three’ requirements of the Essential Eight. All solutions exempt against meeting the full requirements of the Essential Eight require a Security Risk Assessment with planned treatments to mitigate the risks identified. The IP Australia Chief Information Officer had approved exemptions for five solutions.

2.77 IP Australia has established a Security Uplift Program Board to manage and make decisions pertaining to the Security Uplift Program. The Security Uplift Program Board is responsible for ensuring that the Security Uplift Program is delivering on its business case and that the budget, scope, risk and schedule is controlled appropriately. Significant decisions made by the Security Uplift Program Board can be referred to the Investment, ICT and Property Committee by the Chair.⁶⁴

2.78 In October 2020, IP Australia established a Security Governance Committee that reports to the Investment, ICT and Property Committee. The Security Governance Committee is responsible for reviewing and contributing to IP Australia’s annual PSPF self-assessment. Prior to the establishment of a designated security committee in October 2020, the IP Australia Audit Committee monitored IP Australia’s compliance with the Essential Eight requirements. The IP Australia Audit Committee has received reports on the progress of IP Australia’s work to improve its Essential Eight maturity.

2.79 The Audit Committee has discussed the progress of the Security Uplift Program and regularly receives a report on the level of IP Australia’s Essential Eight maturity to enable reporting to the Executive. The September 2020 cyber security paper to the Audit Committee was the first to include a project schedule for the Security Uplift Program. The project schedule indicated that IP Australia was on track to meet its Essential Eight maturity level targets.

64 The IP Australia Chief Information Officer chairs the Security Uplift Program Board.

Attorney-General's Department

2.80 In November 2019, AGD developed a draft program of work to improve its Essential Eight maturity. AGD informed the ANAO that it is targeting 'Maturity Level Three' against the Essential Eight mitigation strategies. However, AGD has not set a timeframe for achieving 'Managing' maturity for Policy 10. AGD informed the ANAO that 'uncertainty about funding for initiatives to improve maturity prevents development of a reliable timeframe.' AGD reported in its 2019–20 PSPF self-assessment for Policy 10 that its strategy to improve its maturity level was 'Continual review, assessment, and improvement to meet the evolving cyber threat environment' and that its timeframe was 'on-going'. As at October 2020, AGD has not developed a clear strategy for achieving 'Managing' maturity.

2.81 AGD informed the ANAO that it assessed its maturity against the Essential Eight model. AGD prioritised the mitigation strategies that present the most likely vulnerability to AGD's systems and information. AGD also informed the ANAO that as part of business-as-usual it has an ongoing continual improvement model for the management of risk to ensure that it meets its obligations under regulatory frameworks. AGD has not provided evidence to demonstrate its processes to improve its maturity against Policy 10 to 'Managing'.

2.82 AGD informed the ANAO that it undertook independent system penetration testing in 2018 and 2020. However, these reviews did not assess AGD against the Top Four mitigation strategies. AGD has not had independent assurance of its compliance with the Top Four mitigation strategies.

2.83 The AGD Security and Risk Management Committee is responsible for ensuring AGD's compliance with the PSPF. The Security and Risk Management Committee does not receive reports on the progress of AGD's work to improve its Essential Eight maturity and is unable to monitor the progress of its implementation.

Recommendation no.7

2.84 The Attorney-General's Department:

- (a) develops a strategy and sets a timeframe to improve its cyber security maturity to the 'Managing' level for PSPF Policy 10;
- (b) provides clear reporting to its governance committees to enable oversight on the progress of its work to improve its Essential Eight maturity; and
- (c) monitors the progress of its work to improve its Essential Eight maturity against the set timeframe and through appropriate governance structures.

Attorney-General's Department response: *Agreed.*

2.85 *AGD takes its cyber security seriously. AGD has a broad collection of measures and strategies to mitigate risk as AGD progresses its implementation of the Essential 8. AGD is undertaking activity to progressively uplift AGD's maturity level with the view to achieving 'Managing' level for PSPF Policy 10.*

2.86 *Taking into account this recommendation, AGD will develop a strategy and set internal timeframes for implementation, to be monitored by the Audit and Risk Management and the Security and Risk Management Committees.*

Future Fund

2.87 Future Fund has developed plans to improve its implementation of the Essential Eight mitigation strategies. Future Fund expects to achieve 'full' implementation of all of the Top Four mitigation strategies by the end of 2021–22. As at October 2020, an internal review was planned to inform future improvement activities.

2.88 Future Fund's Information Security Policy requires a System Accreditation to be performed on all new IT solutions before their use in its IT environment. As part of the System Accreditation, a Solution Design Risk Assessment must be conducted on all new solutions. Risks are assessed according to the Risk Management Policy and where deemed appropriate, the ISM is applied as a baseline for required controls. Future Fund informed the ANAO that the System Accreditation process supports the identification and management of risks related to the Top Four mitigation strategies.

2.89 Future Fund has not had independent assurance of its compliance with the Top Four mitigation strategies since its establishment. Future Fund informed the ANAO that it does not have any exemptions against the Top Four mitigation strategies for reaching 'Maturity Level Three'.

2.90 The Future Fund Management Committee is responsible for reviewing the progress of the Essential Eight work against the Technology Risk and Security area business plan. The Management Committee comprises of the Chief Executive Officer, the Chief Security Officer⁶⁵ and other senior management. The Committee is responsible for providing advice and support to the Chief Executive Officer in relation to the general management of Future Fund's operations and meets at least monthly. The Future Fund Operational Risk & Compliance Committee is responsible for reviewing

⁶⁵ Future Fund reported in its 2018–19 and 2019–20 PSPF self-assessments that 'The accountable authority has appointed the Agency's Chief Financial Officer as the CSO [Chief Security Officer]'.

Future Fund's annual PSPF self-assessment. Future Fund informed the ANAO that the Operational Risk & Compliance Committee Charter is being updated and that the Chief Security Officer is responsible for assessing compliance with the PSPF.

2.91 The Technology Risk and Security area provides a Technology Business Management Dashboard to the Management Committee. The most recent dashboard provided the Committee with an update on the completion of a phase of an Essential Eight improvement activity. Future Fund informed the ANAO that the Management Committee does not receive updates through the dashboard on the progress of the Essential Eight improvement activities, but only of their completion. In September 2020, the Future Fund Board of Guardians was presented with Future Fund's plans to improve its implementation of the Essential Eight mitigation strategies.⁶⁶ In November 2020, Future Fund began providing a dashboard report to the Operational Risk & Compliance Committee on the status of its Essential Eight work.

Recommendation no.8

2.92 The Future Fund Management Agency monitors the progress of its Essential Eight improvement activities against the timeframe set for improving its PSPF Policy 10 maturity level.

Future Fund Management Agency response: *Agreed.*

2.93 *The Agency's Operational Risk & Compliance Committee ("ORCC") now receives quarterly status reports to monitor the progress of the Essential Eight improvement activities against the timeframes set. The first such report was received by the ORCC in November 2020. In addition, from 2021, the Board Audit & Risk Committee will receive such status reports at least annually.*

66 The Chair of the Future Fund Board of Guardians is the Future Fund's accountable authority.

3. Support provided by the cyber policy and operational entities

Areas examined

This chapter examines whether the entities responsible for cyber policy and operational capability in the Australian Government — the Attorney-General's Department (AGD), the Australian Signals Directorate (ASD), the Department of Home Affairs (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 (PSPF).

Conclusion

The cyber policy and operational entities have worked together to provide more guidance following Auditor-General Report No.53 2017–18 *Cyber Resilience*, to support non-corporate Commonwealth entities' self-assessment of their implementation of cyber security requirements under the PSPF. There is scope to further improve the accuracy of entities' PSPF Policy 10 assessments and strengthen arrangements to hold entities to account for the implementation of cyber security mandatory requirements. Robust accountability arrangements are particularly important in absence of public accountability through reporting to the Parliament.

Areas for improvement

The ANAO made five recommendations aimed at:

- AGD ensuring the maturity levels under the PSPF maturity assessment model are fit-for-purpose and effectively aligned with the maturity levels under ASD's Essential Eight Maturity Model;
- AGD providing additional clarity on the PSPF Policy 10 supporting guidance;
- AGD implementing measures to obtain assurance on the accuracy of entities' PSPF Policy 10 self-assessments;
- ASD providing assistance to AGD to support AGD's assurance processes on entities' PSPF Policy 10 self-assessment results; and
- the Australian Government strengthening arrangements to hold entities to account for the implementation of mandatory cyber security requirements.

3.1 Auditor-General Report No.53 2017–18 *Cyber Resilience* identified that the implementation of the previous Protective Security Policy Framework by non-corporate Commonwealth entities was not achieving compliance with cyber security requirements. The report recommended that the three Australian Government entities with responsibilities for cyber security policy and operational capability — AGD, ASD and Home Affairs — work together to improve non-corporate Commonwealth entities' compliance with the framework.⁶⁷ It was recommended that the following areas be strengthened:

⁶⁷ Appendix 2 of this report sets out the recommendation made to the three cyber policy and operational entities in Auditor-General Report No.53 2017–18 *Cyber Resilience* and the corresponding responses provided by the three entities.

- technical guidance to support entities' PSPF self-assessment of their compliance with the mandatory Top Four mitigation strategies;
- processes for verifying the accuracy of entities' PSPF self-assessment of their compliance with the mandatory cyber security requirements; and
- transparency and accountability of entities' compliance with the mandatory cyber security requirements.

3.2 AGD agreed to work with the other two cyber policy entities to strengthen guidance and improve transparency and accountability, and agreed in principle to the development of a verification program for the PSPF self-assessments. ASD agreed to the recommendation, noting that it is neither a regulatory body nor a compliance reporting agency. Home Affairs agreed to the recommendation stating that it would continue to work with AGD and ASD to strengthen the cyber security standard of Australian Government networks in its cyber security policy and coordination role.

3.3 This chapter follows up on the recommendation made in the 2017–18 Auditor-General Report by examining whether AGD, ASD and Home Affairs have worked together to strengthen the three recommended areas to help improve non-corporate Commonwealth entities' implementation of the mandatory cyber security requirements under the revised PSPF.

Is there adequate technical guidance to support entities to accurately self-assess against the Essential Eight mitigation strategies and their underlying controls in the *Australian Government Information Security Manual*?

The revised PSPF maturity assessment model has incorporated more guidance to support entities' self-assessment of their implementation of Policy 10 cyber security requirements. The AGD-developed PSPF Policy 10 guidance cross-references to multiple technical guidance developed by ASD, including guidance on the implementation of the Essential Eight mitigation strategies and the underlying security controls within the *Australian Government Information Security Manual*. There is scope to further improve the alignment of the maturity models for the PSPF and Essential Eight, and the clarity of the guidance to ensure more accurate PSPF Policy 10 self-assessments.

3.4 Auditor-General Report No.53 2017–18 *Cyber Resilience* identified that there was a lack of guidance under the previous compliance-based PSPF assessment model for entities to self-assess and report against their compliance with the Top Four cyber security risk mitigation strategies:

- The non-corporate Commonwealth entities examined in that audit did not have access to comprehensive guidance or supporting tools in conducting their PSPF self-assessments. There was no common control assessment methodology or a grading scheme to help entities to accurately assess the effectiveness of the security controls implemented for the Top Four mitigation strategies. The rating of either compliant or non-compliant under the previous PSPF was limited, and may not accurately reflect the adequacy of an entity's implementation of the Top Four mitigation strategies or the operating effectiveness of the associated security controls.

- In assessing the implementation of the Essential Eight mitigation strategies, there was inconsistent alignment between the criteria used for attaining baseline maturity level under the previous Essential Eight Maturity Model and the criteria for achieving the minimum requirements under the previous *Australian Government Information Security Manual* (ISM). The previous Essential Eight Maturity Model did not provide a way for entities to accurately self-assess their Top Four compliance.

3.5 The report recommended that the three cyber policy and operational entities work together to provide adequate technical guidance to support entities to accurately self-assess against the Top Four mitigation strategies and the underlying security controls within the *Australian Government Information Security Manual* (Recommendation 2(a)). All three entities agreed to the recommendation.

3.6 AGD reported to its audit and risk management committee in December 2020 that it had completed its implementation of Recommendation 2(a) of the 2017–18 audit through the 1 October 2018 PSPF reforms that more clearly articulate the Policy 10 requirements and how they link to the underlying controls contained in the *Australian Government Information Security Manual*.⁶⁸ ASD reported to its audit and risk committee that it has implemented Recommendation 2(a) of the 2017–18 Auditor-General Report audit with respect to the provision of supporting technical guidance to entities.

3.7 To follow up on the recommendation made in the 2017–18 report, the ANAO examined the guidance provided by AGD, ASD and Home Affairs under the revised PSPF maturity assessment model to determine whether the guidance adequately supports entities' self-assessment of their implementation of the PSPF Policy 10 requirements and determination of their PSPF Policy 10 maturity level. The ANAO's examination encompassed a review of guidance provided in PSPF information sessions and reporting forums, and guidance on the PSPF implementation levels, PSPF maturity models and Essential Eight Maturity Model.

Supporting guidance provided by AGD and ASD

3.8 As noted at paragraphs 1.26 to 1.27, a major change in the 2018 reforms to the PSPF was a shift from a compliance-based to a maturity-based reporting approach. The 2018 PSPF reforms also updated the policy on cyber security to more clearly set out the requirements for safeguarding information from cyber threats. Policy 10 in the revised PSPF articulates the cyber security requirements under the framework and provides guidance on how entities can safeguard information from cyber threats.

PSPF information sessions, reporting forums and supporting activities

3.9 Following the finalisation of the 2018 PSPF reforms, AGD held five information sessions in various Australian capital cities with non-corporate Commonwealth entities to assist entities to understand the new PSPF maturity self-assessment model.⁶⁹ The information sessions provided entities with the opportunity to seek specific guidance on self-assessing their security maturity and completing their annual PSPF assessment report using the new PSPF reporting portal.

68 AGD informed its audit and risk management committee that it did not report on the implementation of the recommendation at the time of completion because the 2017–18 Auditor-General Report was of the Department of the Treasury, National Archives of Australia and Geoscience Australia and not of AGD.

69 Information sessions were conducted in Canberra, Brisbane, Melbourne, Sydney and Adelaide in September and October 2018.

3.10 Other activities conducted by AGD to promote awareness of the new PSPF maturity self-assessment model include: convening the Chief Security Officer forums; developing a new PSPF website and PSPF factsheets; and responding to entities' queries on implementation and self-assessment via the PSPF hotline and website form. ASD also presented at the information sessions and forums on issues relating to cyber security and the implementation of the Essential Eight mitigation strategies.

3.11 AGD intends to conduct PSPF assessment reporting forums biannually. The earlier forum is to prepare entities for the PSPF reporting period while the latter forum provides entities with a snapshot of areas requiring heightened attention. The 2019–20 PSPF assessment reporting forum was held on 18 June 2020. ASD also presented at the forum to provide a briefing on cyber security and areas for future focus.

Implementation levels of PSPF Policy 10 requirements

AGD guidance

3.12 In undertaking their annual assessment on PSPF Policy 10, entities are required to assess the effectiveness of their implementation of the cyber security risk mitigation strategies. Entities assess the effectiveness of their implementation of the mitigation strategies against four grading levels — 'Partial', 'Substantial', 'Full' and 'Excelled' — as outlined in Table 1.2. The descriptions of the four implementation levels are provided in PSPF Policy 5: *Reporting on security*⁷⁰ and within the Policy 10 assessment module in the PSPF reporting portal.

3.13 The four grading levels under the maturity assessment model represent an improvement from the binary compliant or non-compliant rating under the previous compliance assessment model. Under the compliance assessment model, entities reported their overall compliance with the previous INFOSEC-4 requirements instead of their compliance with the individual Top Four mitigation strategies. The revised implementation levels enable entities to better reflect the effectiveness of their implementation of the various cyber security risk mitigation strategies.

3.14 As part of the 2018 PSPF reforms, an online PSPF reporting portal was developed to provide an improved mechanism for entities to report on the maturity of their security capability. The portal guides entities through a series of questions and prompts for additional information where relevant. For the 2019–20 reporting period, Policy 10 of the PSPF assessment requires entities to respond to a set of 11 questions. Appendix 3 lists the set of questions for Policy 10.

- The first four questions relate to the extent of the entity's implementation of the mandatory Top Four mitigation strategies.
- Another four questions relate to the extent of the entity's implementation of the four non-mandatory strategies of the Essential Eight mitigation strategies.
- One of the questions addresses the supporting requirement of PSPF Policy 10 regarding whether the entity has measures in place to protect the public from cyber security risk when they transact online with the government. Entities have the choice to select the 'Not Applicable' option if this question does not apply to them.

70 PSPF Policy 5: *Reporting on security* provides guidance on reporting under the new PSPF maturity self-assessment model.

- The final two questions relate to the implementation of the remaining 29 of the 37 ASD prioritised mitigation strategies. Entities are required to assess the extent of their consideration of the implementation of these remaining mitigation strategies and detail the strategies the entity has implemented.

3.15 Within the reporting portal, all 11 questions for Policy 10 have ‘tooltips’ (guidance) to help entities in their self-assessment. The tooltip guidance for each question refers entities to relevant sections of PSPF Policy 10 and the ASD’s publication on *Strategies to Mitigate Cyber Security Incidents*.

ASD guidance

3.16 PSPF Policy 10 includes guidance to support entities in implementing cyber security risk mitigation strategies prescribed by ASD. The guidance within Policy 10 cross-references to the following ASD cyber security publications:

- *Strategies to Mitigate Cyber Security Incidents* — provides guidance on the 37 prioritised strategies developed to mitigate cyber security incidents including suggested implementation order for the mitigation strategies;
- *Essential Eight Maturity Model* — provides guidance on how to implement the Essential Eight mitigation strategies in a phased approach and how to self-assess the maturity level of the implementation;
- *Australian Government Information Security Manual* — outlines a cyber security framework that entities can apply, using their risk management framework, to protect their systems and information from cyber threats;
- *Essential Eight to ISM Mapping* — outlines the minimum security controls within the ISM that entities must implement to meet the intent of the Essential Eight mitigation strategies;
- *Implementing Application Control* — provides guidance on what application control is and how to implement application control;
- *Assessing Security Vulnerabilities and Applying Patches* — provides guidance on assessing security vulnerabilities to determine the risk to entities if patches are not applied in a timely manner;
- *Restricting Administrative Privileges* — provides guidance on how to effectively restrict administrative privileges; and
- *Strategies to Mitigate Cyber Security Incidents – Mitigation Details* — a guidance document that complements the *Strategies to Mitigate Cyber Security Incidents* publication. This guidance provides an overview of the threats of various cyber security incidents and outlines implementation guidance for the mitigation strategies.

3.17 In addition to the above guidance, the ASD’s Australian Cyber Security Centre (ACSC) website contains additional cyber security advice and publications. The ACSC also provides advice to entities via the Cyber Security Hotline and the ACSC Partnership Program.⁷¹

71 The ACSC Partnership Program is open to Australian Government entities, state and territory government entities, industry organisations and the research community. ACSC partners are able to access timely alerts and advisories, share insights and work together to solve common cyber security challenges.





3.18 The tooltip guidance in AGD’s PSPF reporting portal specifically states that entities are to ensure that they are meeting ‘Maturity Level Three’ requirements of the Essential Eight Maturity Model in order to self-assess as having fully implemented the requirements for each of the Top Four mitigation strategies.

PSPF maturity assessment model and the Essential Eight Maturity Model

Maturity levels of PSPF Policy 10

3.19 PSPF Policy 10 also includes guidance on how to achieve PSPF maturity with implementation of the ASD’s mitigation strategies. Under the PSPF maturity self-assessment model, entities assess their security capability against four levels of maturity. Each PSPF policy has maturity level indicators that are tailored to the specific policy. The descriptions and indicators for each maturity level of PSPF Policy 10 are outlined in Table 3.1.

Table 3.1: PSPF maturity levels – Policy 10: *Safeguarding information from cyber threats*

| Maturity level | Maturity level description | Maturity level indicator ^a |
|---|---|--|
| Ad hoc  | Partial: Some PSPF mandatory and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas. | Partial implementation of Top Four strategies to mitigate targeted cyber intrusions. Reactive approach to implementing the remaining Strategies to Mitigate Cyber Security Incidents to protect the entity. |
| Developing  | Substantial: The majority of PSPF mandatory and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes. | The entity has implemented the majority of the Top Four strategies to mitigate targeted cyber intrusions. The entity understands and has substantially implemented the remaining Strategies to Mitigate Cyber Security Incidents it considers necessary to protect the entity. |
| Managing  | Full: All PSPF mandatory and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes. | All Top Four strategies to mitigate targeted cyber intrusions have been fully implemented with ongoing performance monitoring. The entity understands and has implemented the remaining Strategies to Mitigate Cyber Security Incidents it considers necessary to protect the entity. |
| Embedded  | Excelled: All PSPF mandatory and supporting requirements are implemented, are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance. | The entity has fully implemented the Essential Eight, and other activities relevant to the entity’s risk environment, to protect against harm from identified cyber threats. Processes are regularly tested to ensure real-time response to potential cyber intrusions and emerging threats. |

Note a: The maturity level indicators for PSPF Policy 10 were updated for the 2019–20 reporting period to include the November 2019 changes made to the mandatory requirement for entities to consider all of the mitigation strategies in ASD’s *Strategies to Mitigate Cyber Security Incidents*.

Source: Adapted from Table 2: PSPF Maturity Self-Assessment Model – Information Security within Annex A of Policy 5: *Reporting on security*.

3.20 The maturity level descriptions and maturity level indicators show alignment between the four maturity levels and the four implementation levels under the PSPF with ‘Managing’ maturity corresponding with ‘Full’ implementation.

3.21 The PSPF specifies that the ‘Managing’ maturity level provides the minimum required level of protection of an entity’s people, information and assets. PSPF Policy 10 states that to achieve the ‘Managing’ maturity level for the implementation of each of the Top Four mitigation strategies, entities are to implement the ‘Maturity Level Three’ requirements of the Essential Eight Maturity Model. This further indicates that the PSPF maturity level of ‘Managing’ is equivalent to ‘Maturity Level Three’ in the Essential Eight Maturity Model.

3.22 The PSPF reporting portal calculates and suggests a maturity level for Policy 10 based on entities’ responses on the level of their implementation of the mandatory Top Four mitigation strategies and consideration of the remaining mitigation strategies in ASD’s *Strategies to Mitigate Cyber Security Incidents*.⁷² Guidance in the portal specifies that entities’ responses to the questions on their implementation of the four non-mandatory Essential Eight strategies are not included in the maturity level calculation for Policy 10. Of the six selected entities in Chapter 2 that had self-assessed a PSPF maturity level of ‘Ad hoc’ or ‘Developing’, all but one had detailed proposed strategies that were beyond the Top Four for improving its Policy 10 maturity level. This was despite the exclusion of the non-mandatory Essential Eight mitigation strategies from Policy 10 maturity calculation.

3.23 The section for Policy 10 on the ‘Strategies and timeframes to improve your maturity level’ does not specify whether entities should provide details on proposed strategies for the Top Four only. The section could be interpreted as requiring entities to provide details on all the Essential Eight mitigation strategies they have in place for improving their PSPF Policy 10 maturity. This is incongruent with the calculation of the PSPF Policy 10 maturity level in the portal whereby the entities’ implementation of the four non-mandatory Essential Eight strategies does not contribute to the entity’s Policy 10 maturity.

Maturity levels of the ASD’s Essential Eight Maturity Model

3.24 As discussed in paragraph 3.21, the PSPF refers to ‘Maturity Level Three’ of the ASD’s Essential Eight Maturity Model in advising entities on how to achieve the baseline ‘Managing’ maturity level for PSPF Policy 10. As at October 2020, there are three maturity levels in the Essential Eight Maturity Model — ‘Maturity Level One’, ‘Maturity Level Two’ and ‘Maturity Level Three’ — as outlined in Table 1.4.

3.25 The Essential Eight Maturity Model outlines the minimum criteria that entities have to meet in their implementation of the Essential Eight mitigation strategies for reaching the three maturity levels. ASD recommends that entities should aim to reach Maturity Level Three for each mitigation strategy as a baseline.

3.26 The Essential Eight Maturity Model was first published in June 2017 with five maturity levels, defined as follows:

- Maturity Level Zero — Not aligned with the intent of the mitigation strategy;

⁷² If applicable, entities’ response to the question on the extent of the entity’s implementation of the requirement to safeguard information from cyber threats when transacting online with the public is included in the maturity calculation for Module 10.

- Maturity Level One — Partly aligned with the intent of the mitigation strategy;
- Maturity Level Two — Mostly aligned with the intent of the mitigation strategy;
- Maturity Level Three — Fully aligned with the intent of the mitigation strategy; and
- Maturity Level Four — For higher risk environments.

3.27 ASD removed ‘Maturity Level Zero’ and ‘Maturity Level Four’ from the model in February 2019. ASD informed the ANAO that the removal of the two maturity levels was to simplify and improve the focus of the maturity assessment model.⁷³ ASD removed ‘Maturity Level Four’ on the basis that it did not follow the escalating pattern of maturity assessment reflected in the other maturity levels. ‘Maturity Level Four’ was also removed so that the maturity model has a greater emphasis on achieving alignment with the intent of the Essential Eight mitigation strategies.

3.28 As discussed in paragraph 3.4, Auditor-General Report No.53 2017–18 *Cyber Resilience* identified misalignment between the previous Essential Eight Maturity Model and the ISM. In November 2018, ASD addressed the inconsistent alignment through a rewrite of the ISM with the inclusion of new security controls and an update of the language in the Essential Eight Maturity Model. ASD also developed a guidance document on *Essential Eight to ISM Mapping*, which was initially released in January 2019 with subsequent updates made to reflect relevant changes in the ISM.⁷⁴

3.29 The *Essential Eight to ISM Mapping* guidance document outlines the minimum security controls within the ISM that entities must implement to achieve Maturity Level Three for meeting the intent of the Essential Eight mitigation strategies. It clarifies the criteria for meeting the baseline requirements of the Essential Eight Maturity Model when implementing the Essential Eight mitigation strategies. It also aligns the criteria with the minimum requirements in the ISM.

Alignment between the PSPF maturity assessment model and Essential Eight Maturity Model

3.30 The PSPF Policy 10 guidance (May 2020 version) clearly sets out that entities are to implement the requirements for ‘Maturity Level Three’ of the Essential Eight Maturity Model for them to self-assess as having fully implemented a mitigation strategy and achieved a corresponding PSPF maturity level of ‘Managing’. However, the guidance does not clearly outline the alignment for the remaining maturity levels of the PSPF maturity assessment model and the Essential Eight Maturity Model. The availability of guidance that more clearly articulates the correlation of the two models will better support entities in assessing the implementation requirements of the mitigation strategies across the different maturity levels.

3.31 The ANAO identified that AGD and ASD have different interpretations of the maturity level mapping between the PSPF maturity assessment model and the Essential Eight Maturity Model. In responding to a question asked in the 2019–20 PSPF assessment reporting forum held in June 2020 in relation to the mapping between the two models, AGD indicated that Maturity Levels One, Two and Three generally correspond to ‘Ad hoc’, ‘Developing’ and ‘Managing’ maturity levels or ‘Partial’, ‘Substantial’ and ‘Full’ implementation levels respectively. In the ANAO’s discussion with ASD during the audit, ASD informed that its understanding of the PSPF maturity levels is:

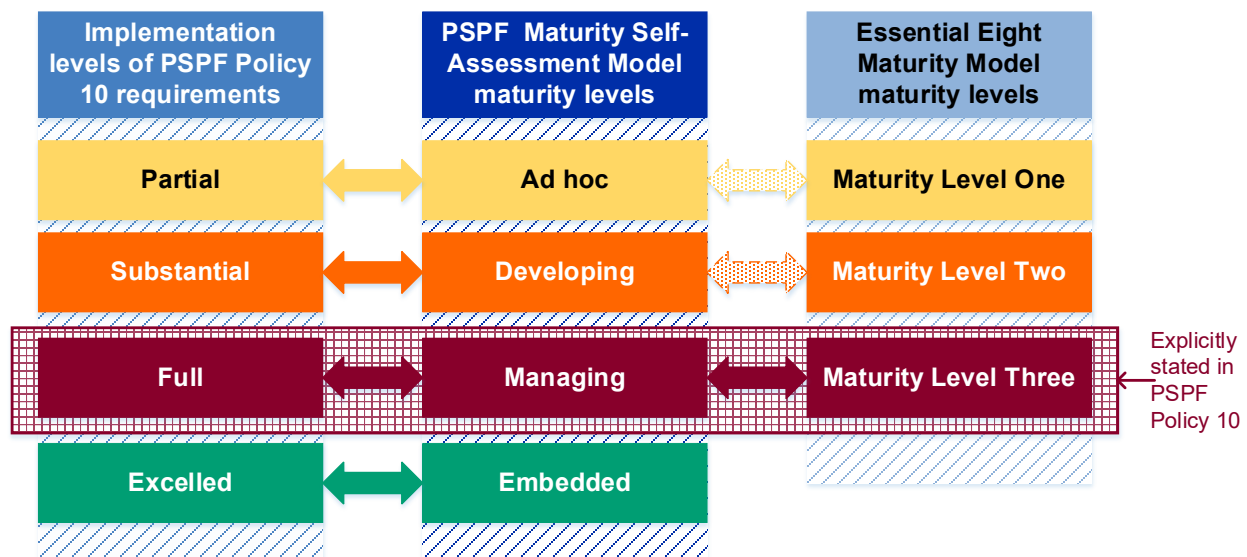
73 The ASD’s September 2020 Essential Eight Maturity Model consultation draft proposes to restore Maturity Level Zero – defined as ‘Incapable of mitigating basic cyber threats.’

74 ASD updates the ISM monthly and publishes the document on its website. Previous versions of the ISM are also available on the ASD’s ACSC website.

The maturity levels of ‘ad hoc’ and ‘developing’ are an indication of the degree of implementation of Maturity Level 3 requirements — not whether an entity is either Maturity Level 1 or Maturity Level 2...

3.32 The ANAO’s review of the maturity level descriptions and indicators identified that there is an inherent alignment between the two models despite it not being clearly set out in the guidance. The ANAO also identified that there is an apparent misalignment between the PSPF maturity assessment model and the Essential Eight Maturity Model, which is the different grading levels within the two models. While there are four maturity levels under the PSPF maturity assessment model, the current ASD’s Essential Eight Maturity Model only has three maturity levels. There is no equivalent Essential Eight maturity level for the highest PSPF maturity level of ‘Embedded’. ANAO analysis of the alignment between the PSPF maturity assessment model and the Essential Eight Maturity Model is depicted in Figure 3.1.

Figure 3.1: AGD mapping of the PSPF maturity assessment model to the Essential Eight Maturity Model



Source: ANAO analysis of the guidance for PSPF Policy 10 and the Essential Eight Maturity Model.

3.33 PSPF Policy 10 guidance does not elaborate on what an ‘Excelled’ level of implementation entails for entities to achieve an ‘Embedded’ PSPF maturity level. There is no guidance on the Essential Eight Maturity Model criteria entities have to meet to reach ‘Embedded’ maturity. This misalignment between the two maturity models and the lack of technical guidance reduces clarity for entities on how an ‘Embedded’ maturity level could be achieved.⁷⁵

3.34 As discussed in paragraphs 1.35 and 3.25, ASD recommends that entities should aim to reach ‘Maturity Level Three’ for each of the eight mitigation strategies as a baseline. The existence of a maturity level as a baseline implies that there is a higher maturity level that should be attained. However, ‘Maturity Level Three’ is also the highest maturity level under the current Essential Eight Maturity Model.

3.35 Regular meetings between ASD and AGD on cyber security reporting included discussions on the misalignment of the maturity models. As at December 2020, ASD and AGD had not resolved

⁷⁵ See Appendix 4 for the selected entities’ views on the supporting guidance for PSPF Policy 10 self-assessment.

the misalignment between the PSPF maturity assessment model and the Essential Eight Maturity Model.

3.36 Following the completion of the Essential Eight+ Sprint Program, ASD commenced a review of the current Essential Eight Maturity Model to ensure that it remains 'contemporary, contestable and actionable'. In October 2020, ASD shared a consultation draft of the revised Essential Eight Maturity Model with Information Technology Security Advisers, Chief Information Officers and Chief Information Security Officers from federal, state and territory governments, as well as key industry partners from various sectors, to seek feedback on its proposed update to the Essential Eight Maturity Model. As at early December 2020, the proposed update to the Essential Eight Maturity Model was yet to be finalised.

Recommendation no.9

3.37 The Attorney-General's Department reviews the existing maturity levels under the PSPF maturity assessment model to determine if the maturity levels are fit-for-purpose and effectively aligned with the Essential Eight Maturity Model, having regard to the Australian Signals Directorate's proposed update to the Essential Eight Maturity Model.

Attorney-General's Department response: *Agreed.*

3.38 *AGD is currently reviewing the maturity model to ensure it is fit-for-purpose, and will consider the lessons learned from the previous 2 years of reporting under the updated PSPF. We will continue to work closely with ASD on the interaction between the PSPF and the Essential Eight Maturity Model; and will ensure appropriate alignment of the two models as part of this process. AGD will continue to periodically review the maturity model to ensure it remains fit-for-purpose.*

Other issues relating to the guidance

3.39 As discussed in paragraph 3.22, an entity's PSPF maturity level for Policy 10 is calculated by the reporting portal based on the responses provided to some of the questions for Policy 10. The guidance in the portal specifies that the responses to four of the 11 questions for Policy 10, which relate to the implementation level of the four non-mandatory Essential Eight mitigation strategies, are not included in the maturity calculation for Policy 10.

3.40 While the reporting portal states what is excluded from the Policy 10 maturity calculation, the methodology for the maturity calculation has not been adequately explained in other PSPF guidance.⁷⁶ There is merit in clarifying the guidance on the scope of the maturity calculation for PSPF Policy 10 to enable entities to more accurately consider the system-suggested maturity level and determine the entity's Policy 10 maturity level.

3.41 Following the November 2019 amendment made to the PSPF Policy 10 mandatory requirements (see Box 1 and paragraph 1.24), Policy 10 of the 2019–20 PSPF assessment has included questions on entities' consideration of the relevant strategies from the remaining ASD's prioritised mitigation strategies that the entity needed to implement (see Appendix 3, Questions

76 Guidance in Module 10 of the PSPF reporting portal specifies that entities' implementation of the four non-mandatory Essential Eight strategies are not included in the maturity level calculation for Policy 10. There is no guidance that specifies which responses to the Module 10 questions contribute to the maturity level calculation. Please refer to Appendix 4 for entities' views on the supporting guidance for PSPF Policy 10 self-assessment.

10.10 and 10.11). The tooltip guidance for Question 10.10 states that entities are required to advise which of the remaining 29 mitigation strategies they have implemented.

3.42 AGD informed the ANAO that the intention of this question is for entities to assess the mandatory requirement in relation to the level — ‘Partial’, ‘Substantial’, ‘Full’ or ‘Excelled’ — to which the entity has considered each of the remaining strategies. The purpose of this mandatory requirement is for entities to make an assessment based on the entity’s risk environment and business operations to determine if it needs to implement any of the remaining ASD’s mitigation strategies. Entities are then required to detail which of the remaining 29 strategies they have implemented in a free-text box in Question 10.11.

3.43 Question 10.10 requires entities to assess the level of their consideration of the implementation of the mitigation strategies. This is in contrast to the other Policy 10 questions that require entities to assess the level of their implementation of the mitigation strategies. Assessment of an entity’s level of consideration involves subjective judgment. There is a lack of guidance on how entities are to assess and grade Question 10.10, which could lead to misinterpretations of the question. Further, it is unclear how the level to which entities have considered the implementation of cyber security risk mitigation strategies would contribute to their actual cyber security maturity level.⁷⁷

3.44 During the course of this audit, the ANAO sought the views of the selected entities under this audit regarding the supporting guidance available for their PSPF Policy 10 self-assessment. Appendix 4 outlines some of the views expressed by the selected entities.

⁷⁷ Refer to Appendix 4 for entities’ views on the supporting guidance provided for PSPF Policy 10 self-assessments.

Recommendation no.10

3.45 The Attorney-General's Department further improves the guidance on PSPF Policy 10 to clarify:

- (a) the correlation of the maturity levels in the PSPF and Essential Eight maturity models, and their implementation requirements;
- (b) the scope of the maturity level calculation suggested by the reporting portal and how entities can more accurately determine their selected PSPF maturity level; and
- (c) the assessment against the requirement to consider the implementation of the remaining 29 mitigation strategies, and the merit of its inclusion in the PSPF Policy 10 maturity level calculation.

Attorney-General's Department response: *Agreed.*

3.46 *AGD places a high priority on ensuring entities understand the requirements in the PSPF and the methodology for calculating their maturity levels. As a result, AGD regularly updates the PSPF and provides additional guidance and assistance to entities via reporting fora and through a dedicated hotline and inbox. AGD will undertake further work to improve the guidance in Policy 10 through these existing processes, including through consultation with ASD on the correlation of maturity levels.*

3.47 Home Affairs informed the ANAO that it does not play a role in developing guidance to assist entities in cyber security self-assessments and reporting under the PSPF. In its cyber security policy coordination role, Home Affairs was involved in the development of the revised PSPF Policy 10. Home Affairs provided strategic advice to AGD and ASD to ensure that the PSPF and ISM are consistent with national cyber security policy and are mutually supportive of improved cyber security standards across the Australian Government.

Have the cyber policy and operational entities developed processes to verify the accuracy of entities' self-assessed reporting?

The cyber policy and operational entities have not developed processes to verify the accuracy of entities' PSPF Policy 10 self-assessed reporting. ASD has commenced the development of software tools that provide technical reporting to support entities in performing more accurate self-assessments of their Essential Eight implementation. While AGD and ASD have been sharing the results of the PSPF self-assessment reports and the ASD's ACSC Cyber Security Survey, the sharing of data has not yet resulted in obtaining assurance on the accuracy of the self-assessments and facilitating policy and technical assistance for entities.

3.48 In light of the continued low level of compliance with the Top Four mitigation strategies, Auditor-General Report No.53 2017–18 *Cyber Resilience* recommended that the three cyber policy and operational entities work together to develop a program under the revised PSPF to verify the accuracy of entities' self-assessment of their compliance with the mandatory mitigation strategies (Recommendation 2(b)). ASD and Home Affairs both agreed to the ANAO's recommendation. In agreeing to the recommendation, ASD noted that it is neither a regulatory body nor a compliance reporting agency for cyber security.

3.49 AGD agreed in principle to the recommendation in the 2017–18 report regarding the verification program. AGD stated that while the revised PSPF would assist with verification by requiring supporting evidence from entities to provide greater assurance on the accuracy of their self-assessment, the development of a verification program is a matter for ASD.

3.50 AGD reported to its audit and risk management committee in December 2020 that it had completed its implementation of Recommendation 2(b) of the 2017–18 Auditor-General Report by introducing reforms to the PSPF and the revised PSPF maturity self-assessment model. ASD reported to its audit and risk committee that it has implemented Recommendation 2(b) from Auditor-General Report No.53 2017–18 *Cyber Resilience* through the conduct of the ACSC Cyber Security Survey and the Cyber Uplift Program.

3.51 To follow up on the recommendation, the ANAO examined in this audit the processes developed by AGD, ASD and Home Affairs to gain assurance on the accuracy of entities' PSPF self-assessments and reporting.

AGD assurance activities

3.52 During the course of this audit, AGD reiterated its response to the 2017–18 Auditor-General Report that it does not have the technical capability to verify the accuracy of entities' Essential Eight assessment and considered the development of any such verification program to be a matter for ASD. AGD informed the ANAO that it also does not undertake any technical verification for entities' assessments of other PSPF policies. AGD informed the ANAO that it will engage with entities to provide advice on policy implementation and facilitate access to subject matter experts. AGD noted that it does not have a regulatory role in relation to the PSPF⁷⁸; its function is to ensure that the PSPF policy is appropriate and entities are supported to implement the policy and self-assess their maturity level to meet reporting obligations under the framework.

Reviews and analysis of PSPF assessment reports

3.53 While AGD does not verify the accuracy of entities' PSPF self-assessments, AGD reviews and analyses the PSPF assessment reports submitted by entities. AGD does not have a framework that it uses to guide the analysis.

3.54 AGD informed the ANAO that it reviews entities' responses in the submitted reports to ensure that they have captured all required information before it accepts the reports as final. AGD then considers the responses provided in each PSPF assessment module to ensure that the rationale provided justifies the maturity level selected by the entities. Where an entity has selected an 'Ad hoc' or a 'Developing' maturity level, AGD will review the information provided in the 'Strategies' and 'Timeframes' text boxes to ensure that there is sufficient information for AGD to understand how the entity will improve its maturity level for the applicable PSPF policy.

3.55 Where further information and evidence is required, AGD informed the ANAO that it has an internal procedure to return the assessment report to the entity with comments for the entity to

78 AGD was identified as one of the regulators under the Independent Review of Whole-of-Government Internal Regulation (Belcher Review) in 2015. The Belcher Review assessed the need and impact of regulations on Australian Government entities, with regulation being defined as 'requirements that are mandatory for all or most entities, or guidance, practice or procedure that is treated as such'. The PSPF was one of the regulatory areas reviewed. The findings on the PSPF from the Belcher Review informed the PSPF reforms in 2018.

address before it resubmits the report. In 2018–19, AGD made 78 requests for entities to re-submit their self-assessments with additional information.⁷⁹ In 2019–20, AGD made 45 requests for additional information.⁸⁰

3.56 AGD analyses the results from all the PSPF assessment reports and the qualitative data within to determine the overall protective security posture of the Australian Government and the broader implications. AGD found that irrespective of entities' risk environments and maturity levels, entities in 2018–19 were most concerned about the risk of a cyber-attack. Of the 2018–19 PSPF assessment reports for Policy 10 AGD identified that for those entities with maturity levels of 'Ad hoc' and 'Developing', the following were the key challenges faced by the entities with respect to their implementation of the required level of maturity:

- limited allocation of funding or staff to achieve the implementation of the Top Four mitigation strategies;
- low capability;
- reliance on outsourced service providers for information communications technology (ICT) and cyber security services, whereby entities had limited influence or control over the implementation of the mitigation strategies;
- lack of prioritisation to implement the Top Four, whereby entities often targeted mitigation strategies that were easier to implement;
- lack of comprehensive understanding of the implementation requirements of the Top Four mitigation strategies;
- lack of understanding of how the implementation level of the mitigation strategies relates to the entity's risk environment;
- reliance on legacy and unsupported systems; and
- the significant investment required to achieve full implementation of the Top Four mitigation strategies.

3.57 As at February 2021, AGD's analysis of entities' PSPF self-assessments for 2019–20 was ongoing.

Sharing of PSPF and ACSC survey results

3.58 AGD shares the cyber security related PSPF self-assessment results with ASD. The 2018–19 PSPF Policy 10 self-assessment results were shared with ASD and contributed to the inaugural report to the Parliament in April 2020 on Australian Government entities' cyber security posture (see paragraph 3.89). This report on Government entities' cyber security posture was also informed by the 2019 ACSC Cyber Security Survey conducted by the ACSC.⁸¹

79 The 2018–19 data on requests to re-submit self-assessments with additional information included two requests to AGD and one request to the Australian National Audit Office.

80 The 2019–20 data on requests to re-submit self-assessments with additional information included one request to the Australian National Audit Office.

81 ASD's ACSC conducts an annual cyber security survey of Australian Government entities to measure entities' cyber security maturity (paragraphs 3.76 to 3.82).

3.59 In August 2020, ASD shared all the raw data from its 2019 ACSC Cyber Security Survey with AGD.⁸² The sharing of the survey data was for the purpose of enabling AGD and ASD to compare the PSPF assessment results with the ACSC survey findings. ASD informed the ANAO that it had used the information in the 2017–18 PSPF assessment results provided by AGD to inform its December 2018 correspondence to those entities that had reported non-compliance to offer cyber security assistance. ASD had also used the PSPF assessment results shared by AGD to inform the selection of entities for its Essential Eight+ Sprint Program (see paragraph 1.12).

3.60 Comparison of the survey results can potentially assist AGD in obtaining assurance on the accuracy of the self-assessments. AGD has not used the data to inform assurance activities on the self-assessed maturity ratings.

Assistance for entities with PSPF Policy 10 maturity rating of 'Ad hoc'

3.61 AGD and ASD have met regularly since August 2019 to discuss the PSPF self-assessment and ACSC cyber security surveys. The key purpose of these meetings is to identify ways to streamline the PSPF and ACSC surveys to reduce duplication.⁸³ Minutes from the meetings indicate that AGD and ASD discuss the results of the PSPF assessment and ACSC Cyber Security Survey, but do not record any actions taken following the meetings.

3.62 In the May 2020 meeting, AGD raised the possibility of ASD being involved in follow-up activities from the PSPF assessment report. The coordinated approach involved AGD offering assistance to entities that have self-assessed as having an 'Ad hoc' maturity for PSPF Policy 10 to provide them with advice and support in implementing the PSPF policy. AGD requested ASD be involved in offering technical cyber security assistance to those entities to improve their cyber security posture. ASD agreed to provide assistance to those entities with an 'Ad hoc' maturity rating.

3.63 A plan has not been developed for the coordinated approach to offer AGD's policy assistance and ASD's technical support on cyber security. While this approach could potentially assist entities in improving their implementation of cyber security requirements, the assistance may not be appropriately targeted at those entities that inaccurately overstate their maturity level.

Moderation of self-assessments

3.64 At the time of this audit, AGD informed the ANAO that it was considering appropriate processes that could provide assurance on the quality of entities' self-assessments. The assurance activities considered include peer reviews and a validation model that would provide entities with a list of the typical underlying evidence that would need to be in place to support the self-assessments made.⁸⁴

3.65 In the Government Security Committee⁸⁵ meeting held on 20 May 2020, the committee noted that there was low maturity assessed for cyber security under Policy 10. It was also noted

82 ASD informed the ANAO that the sharing of raw data from the survey only commenced in 2020. They only shared high-level survey results with AGD in previous years.

83 In agreeing to the JCPAA's recommendation in *Report 467: Cybersecurity Compliance* to make the annual ACSC Cyber Security Survey mandatory, the Australian Government made an undertaking to review the various cyber security surveys to reduce duplication.

84 This would be in addition to the current requirement for entities to reference supporting evidence in their rationale for their security maturity self-assessments.

85 The role of the Government Security Committee is discussed in paragraph 1.16.

that there was variation across entities in relation to the information provided, including the level of detail on individual risk environments in the 2018–19 PSPF reporting. As a result, it was agreed that AGD will further explore options to strengthen the PSPF maturity self-assessment model, including consideration of the New Zealand self-assessment moderation model.⁸⁶ AGD was to return to a future Government Security Committee meeting to discuss proposed improvements to the PSPF self-assessments and appropriate assurance activities for the self-reported data. AGD informed the ANAO in November 2020 that it was still considering a moderation model for the annual PSPF self-assessment data. AGD has not returned to the Government Security Committee to discuss the moderation of self-assessments. AGD also informed the ANAO that work will be progressed following analysis and comparison of data from the 2019–20 PSPF self-assessment report and the 2020 ACSC Cyber Security Survey.

Recommendation no.11

3.66 The Attorney-General's Department implements arrangements to obtain an appropriate level of assurance on the accuracy of entities' PSPF Policy 10 self-assessment results.

Attorney-General's Department response: *Agreed in principle.*

3.67 *Entities are required to undertake a self-assessment against all 16 policies under the PSPF. AGD recognises the importance of accurate self-assessment and reporting; and on this basis, the department is already exploring options, including moderation, to further support entities to improve the accuracy of their self-assessments.*

ANAO comment

3.68 The report notes at paragraph 4 that the PSPF outlines 16 core requirements that entities must apply to achieve the four protective security outcomes. Paragraph 1.25 of the report notes that since 2013, non-corporate Commonwealth entities have been required to undertake an annual self-assessment against the mandatory requirements of the PSPF. Paragraph 19 of the report notes that the cyber policy and operational entities have not developed processes to verify the accuracy of entities' PSPF Policy 10 self-assessed reporting. At paragraph 3.65 the report notes that in May 2020 AGD undertook to further explore options to strengthen the PSPF maturity self-assessment model, including consideration of the New Zealand self-assessment moderation model. AGD has further undertaken to return to a future Government Security Committee meeting to discuss proposed improvements to the PSPF self-assessments and appropriate assurance activities for the self-reported data. Without appropriate assurance, AGD is unable to provide advice to the Australian Government on the extent to which the policy is achieving its information security outcome.

ASD assurance activities

3.69 ASD informed the ANAO that while it has the responsibility and expertise to undertake technical assessments of entities' cyber security capability, it is not responsible for verifying the accuracy of entities' PSPF Policy 10 self-assessments. As part of its delivery of the Cyber Uplift

86 The New Zealand framework involves the review of entities' self-assessments of their protective security requirements by a moderator. The moderator reviews the entities' self-assessments against supporting evidence to provide assurance on the accuracy of the entity's self-assessed ratings.

Program (see paragraph 1.11), ASD has developed the Cyber Toolbox and Host-Based Sensor initiatives to assist entities in improving their cyber security posture. The Cyber Toolbox and Host-Based Sensors are software tools developed to support entities in performing more accurate self-assessments of their Essential Eight implementation. These tools provide technical reporting through automated sensors and other technical means, which ASD believes may assist in verifying the accuracy of entities' self-assessments in the long term.

Cyber Toolbox

3.70 The Cyber Toolbox, is a collection of software tools and processes, to help Government entities understand their Essential Eight maturity to enable them to perform more objective self-assessments to improve their cyber security posture going forward. The Cyber Toolbox is aimed at initially helping Government entities in self-assessing their current cyber security posture and subsequently providing tailored advice to entities to make iterative improvements.

3.71 In April 2020, ASD released the first two tools — the Essential Eight Maturity Verification Tool and the Application Control Verification Tool — to six pilot entities (as at September 2020) for testing. ASD informed the ANAO that the pilot entities were able to continue using the tools after the pilot. The Essential Eight Maturity Verification Tool and the Application Control Verification Tool are outlined in Table 3.2.

Table 3.2: Initial assessment tools from the Cyber Toolbox

| Cyber Toolbox assessment tools and their functions | |
|--|--|
| Essential Eight Maturity Verification Tool (E8MVT) | |
| <ul style="list-style-type: none"> • The E8MVT provides an indication of the Essential Eight maturity level of a representative system and improvement recommendations. • The E8MVT examines registry settings, commonly installed applications and patch levels. It then compares these with key elements of the Essential Eight Maturity Model. The results provide an indication of the existing maturity level of the assessed system and recommends the next steps to improve the maturity level, with direct references to relevant ASD publications and guidance. • As system changes are made, the E8MVT can be run again to confirm the effectiveness of the changes. • The E8MVT does not assess three of the Essential Eight mitigation strategies — restricting administrative privileges, multi-factor authentication, and daily backups, as these were considered not assessable on a single system. | |
| Application Control Verification Tool (ACVT) | |
| <ul style="list-style-type: none"> • The ACVT assesses the effectiveness of entities' application control policy and identify existing gaps. • Application control is a security control designed to prevent unauthorised applications from executing on a system. Application control is implemented via a set of execution policies that are defined by the entities' business needs. • The ACVT diagnoses issues with an implemented policy by attempting to bypass the policy restrictions. Where the ACVT is successful in bypassing the policy, this is reported to the entity for further action. | |

Source: ANAO representation of information provided by ASD.

3.72 After the pilot was been completed, ASD released the E8MVT and ACVT for the use of Government entities. ASD also informed the ANAO that more tools are being developed as part of the Cyber Toolbox; however, they are not yet ready for release.

Host-Based Sensor program

3.73 The Cyber Uplift Program included the piloting of a Host-Based Sensor initiative with two Australian Government entities, deploying end-point sensors across the two entities. The Host-Based Sensor pilot program monitored the entities' networks for signs of cyber intrusion. ASD completed the pilot in December 2019 and has rolled out the Host-Based Sensor program to other Government entities. As at September 2020, six Government entities were participating in the Host-Based Sensor program. At the same time, there were another 44 entities at different stages of engagement with ASD to participate in the Host-Based Sensor program.

3.74 The Host-Based Sensor program involves ASD deploying host-based monitoring software (known as sensors) to the network devices (known as hosts) of participating Government entities to detect intrusion and investigate, respond to and generate intelligence on cyber threats. The sensors are defensive software tools developed by ASD for deployment on servers, workstations and laptops. The sensors provide the participating entities and ASD with data to identify malicious cyber activities, generate threat indicators and contribute to the development of appropriate mitigation strategies. Following the deployment of the host-based sensors, the participating entity is to receive a Threat Surface Report that provides information about the hosts and vulnerabilities within the network to help reduce the cyber threat surface.

3.75 The technical reporting provided through the deployment of automated sensors has the potential to support participating entities in undertaking more accurate self-assessments of their implementation of the Essential Eight mitigation strategies. ASD intends to further develop the Threat Surface Report to measure more technical controls of the Essential Eight mitigation strategies as well as provide guidance to counter trending adversary tradecraft.

ACSC Cyber Security Survey

3.76 Since 2010, ASD conducts an annual cyber security survey of Australian Government entities to assess their cyber security posture. The survey was non-mandatory before 2018–19 and had a low completion rate.⁸⁷ The Joint Committee of Public Accounts and Audit (JCPAA) recommended in *Report 467: Cybersecurity Compliance* that the completion of the annual ASD survey be made mandatory for all *Public Governance, Performance and Accountability Act 2013* entities by June 2018.

3.77 The ASD's ACSC Cyber Security Survey for Commonwealth Entities (ACSC Cyber Security Survey) was made mandatory for non-corporate Commonwealth entities with the commencement of the revised PSPF in October 2018.⁸⁸ The mandatory requirement in PSPF Policy 5: *Reporting on Security* requires entities to report on cyber security matters to ASD each year.

3.78 Unlike the PSPF survey, the ACSC Cyber Security Survey is not a self-assessment of an entity. The ACSC survey is the key method for the ACSC to measure the cyber security maturity of Australian Government entities. Based on the responses provided by entities in the survey, ASD assigns a maturity rating using the Essential Eight Maturity Model. The ACSC survey is designed to

87 The survey was only completed by around 30–40 per cent of entities in 2016 and 2017. See Joint Committee of Public Accounts and Audit, Parliament of Australia, *Report 467: Cybersecurity Compliance*, October 2017, p. 5.

88 Corporate Commonwealth entities and Commonwealth companies are strongly encouraged to respond to the ACSC Cyber Security Survey.

inform a picture of the cyber threat landscape, and helps ASD to identify high-risk entities to better target its advice and assistance to help entities respond to cyber threats.

3.79 ASD informed the ANAO that the assignment of Essential Eight maturity ratings based on assessments it undertook, whether via the cyber security survey or the Essential Eight+ Sprint program, will provide a level of independent assurance that an appropriate maturity rating is given to an entity.

3.80 The ACSC Cyber Security Survey focuses on technical questions regarding the implementation of the Essential Eight mitigation strategies to enable ASD to determine the cyber security maturity of the entity. In contrast, the AGD's PSPF Policy 10 assessment questions are more high level policy questions designed to ascertain the entity's PSPF maturity against the PSPF maturity model. The ACSC Cyber Security Survey also include questions on cyber threats, cyber security incidents, and the entity's cyber security culture.

3.81 The 2020 ACSC Cyber Security Survey was released on 1 October 2020.⁸⁹ ASD informed the ANAO that it plans to send entities individual reports detailing the entity's results in late 2020. ASD intends to include, in the individual report, a written explanation of its assessment of the entity's maturity against the Essential Eight Maturity Model. ASD also intends to share key findings from the aggregated survey results in a summary report with all Government entities in March 2021.⁹⁰

3.82 The results of the 2019 ACSC Cyber Security Survey and the Cyber Uplift Program contributed to the findings in *The Commonwealth Cyber Security Posture in 2019* report to the Parliament. ASD informed the ANAO that other data sources are to be used for the 2020 report to Parliament, including data from programs similar to the Cyber Uplift Program.

Recommendation no.12

3.83 As part of its technical advice and assistance to the Attorney-General's Department, the Australian Signals Directorate draw on its technical tools in addition to its existing capabilities to support the Attorney-General's Department's assurance processes on entities' PSPF Policy 10 self-assessment results.

Australian Signals Directorate response: *Agreed.*

3.84 *ASD agrees with the recommendation and will work with the Attorney-General's Department to support AGD's assurance processes on entities PSPF Policy 10 Self-assessment results.*

3.85 In response to Recommendation 2 from Auditor-General Report No.53 2017–18 *Cyber Resilience*, Home Affairs agreed to work with AGD and ASD to develop a fit-for-purpose mechanism to verify entities' self-assessments on their compliance with cyber security requirements. Home Affairs informed the ANAO that it has worked with AGD and ASD through the provision of strategic cyber security advice in support of their efforts to increase accountability regarding entities' self-assessments under the PSPF.

⁸⁹ Entities initially had to respond to the 2020 ACSC Cyber Security Survey by 30 October 2020. An extension was granted until 13 November 2020 for entities to respond.

⁹⁰ ASD will also be sharing all survey data collected with AGD.

Have the cyber policy and operational entities established processes to improve the transparency and accountability of entities' implementation of mandatory cyber security requirements?

With the release of the whole-of-government PSPF assessment reports by AGD and the annual Australian Government's cyber security posture report by ASD, there has been increased public reporting on non-corporate Commonwealth entities' implementation and maturity level of the Essential Eight mitigation strategies. However, the status of entities' cyber security posture is not transparent due to the policy and operational entities' concerns about increasing security risks following the disclosure of individual entities' cyber security maturity level. The cyber policy and operational entities have not established processes to improve the accountability of entities' cyber security posture. The current framework to support responsible Ministers in holding entities accountable within Government is not sufficient to drive improvements in the implementation of mandatory requirements.

3.86 Prior to the 2017–18 reporting period, PSPF compliance reports submitted to AGD were not made public. Auditor-General Report No.53 2017–18 *Cyber Resilience* found that there was a lack of mechanisms to provide transparency and accountability for entities' compliance with cyber security requirements. The report recommended (Recommendation 2(c)) that the three cyber policy entities work together to improve compliance with the cyber security framework by increasing the transparency and accountability of entities' compliance with cyber security requirements. All three entities agreed to the ANAO's recommendation.

3.87 AGD reported to its audit and risk management committee in December 2020 that it had completed its implementation of Recommendation 2(c) of the 2017–18 Auditor-General Report by publicly releasing the 2017–18 whole-of-government PSPF Compliance Report and working to finalise the 2018–19 whole-of-government PSPF Assessment report. ASD reported to its audit and risk committee that it had implemented Recommendation 2(c) through the provision of the annual report on Australian Government entities cyber security posture to Parliament.

3.88 To follow up on this recommendation, the ANAO examined whether AGD, ASD and Home Affairs have:

- improved external reporting and transparency of non-corporate Commonwealth entities cyber security posture; and
- established mechanisms for the Parliament and relevant Australian Government cyber security governance committees to hold entities accountable for their cyber security posture.

Public reporting and transparency

Whole-of-government PSPF assessment reports

3.89 Following the tabling of the 2017–18 Auditor-General Report, AGD publicly released the 2016–17 and 2017–18 consolidated PSPF compliance reports on the PSPF website. These PSPF compliance reports contain aggregated findings on non-corporate Commonwealth entities' compliance with mandatory PSPF requirements.

3.90 The 2018–19 consolidated PSPF maturity assessment report was published on the PSPF website on 15 January 2021. The 2018–19 consolidated PSPF maturity assessment report is the first report to be released under the revised PSPF maturity self-assessment model. Similar to past consolidated PSPF compliance reports, the 2018–19 report contains aggregated findings and does not disclose the security maturity level of individual entities.

Report on cyber security posture of Australian Government entities

3.91 In April 2020, ASD tabled the inaugural *The Commonwealth Cyber Security Posture in 2019* report in the Parliament and published the report on its website.⁹¹ This report outlines the overall maturity of Australian Government entities' implementation of the Essential Eight mitigation strategies and the status of their cyber security posture. The findings in the report were based on information obtained from the 2019 ACSC Cyber Security Survey and the results from AGD's 2018–19 PSPF Policy 10 assessment reports. The findings were also informed by the results of the Cyber Uplift Program, cyber security incident reporting and investigations undertaken by ASD.⁹²

3.92 The 2019 report on Australian Government entities' cyber security posture contains anonymised and aggregated data. The report does not identify individual entities and the maturity level of their Essential Eight implementation. ASD informed the ANAO that it has no intention to disaggregate the data to identify the cyber security posture of individual entities in future reports.

Security concerns with publicly reporting individual entities' cyber security posture

3.93 ASD and AGD informed the ANAO that security concerns were the reason for not publicly reporting specific entities' cyber security posture. ASD and AGD both indicated that the identification of individual entities' cyber security maturity level in public reporting provides detailed information on a 'heat map of vulnerabilities' in Australian Government networks. This may increase the risk of targeted attacks by malicious actors.

3.94 ASD has information to indicate that malicious actors seek to compromise networks based on known security vulnerabilities. ASD has also seen evidence of malicious actors manoeuvring between connected networks to target attacks on the weakest network.

3.95 In the 2020–21 Budget Estimates in October–November 2020, questions were put to non-corporate Commonwealth entities that include: their compliance with the mandatory requirements of PSPF Policy 10 and their implementation of the Essential Eight mitigation strategies. In November 2020, an email was sent by AGD to all non-corporate Commonwealth entities' Chief Security Officers and generic security mailboxes providing entities with a suggested approach in line with ACSC guidance. The email provided the following suggested response to questions regarding the PSPF and Essential Eight implementation:

Publicly reporting on individual agency's compliance with the Essential 8/Top 4 or specific cyber mitigations in response to these questions on notice would provide a snapshot in time of the entire Federal Government's cyber security maturity and as a result, may provide a heat map for

91 The annual reporting to the Parliament on Australian Government entities' cyber security posture is in response to a JCPAA's recommendation made in *Report 467: Cybersecurity Compliance*. The Australian Government agreed to this recommendation in support of increased transparency in cyber security reporting.

92 ASD informed the ANAO that the report supports the Australian Government's visibility of the overall cyber threat environment.

vulnerabilities that malicious actors may exploit and thus increase an agency's risk of cyber incidents.

Accountability mechanisms for entities' cyber security posture

3.96 The existing reporting mechanisms under the PSPF require entities to provide their PSPF assessment report to their portfolio Minister. AGD considers that the existing accountability mechanisms, including the publishing of the whole-of-government PSPF assessment report, provide the appropriate balance between transparency and the risk of exposing entities to malicious actors through the sharing of entities' cyber security posture publicly. AGD informed the ANAO that entities are held accountable to their Minister as they are required to report to their Minister annually on their self-assessment. There is no framework to support Ministers to determine the appropriateness of entities' self-assessment reports.

3.97 While AGD reviewed the information provided by entities in their PSPF Policy 10 assessment (see paragraphs 3.53 to 3.55), the review was for ensuring completeness and adequacy of the information provided. The review was not for the purpose of validating whether entities had undertaken the cyber security measures or planned strategies detailed in their previous self-assessment, or confirming if entities have improved their maturity within the advised timeframe.⁹³ AGD does not use the data from entities' Policy 10 self-assessments to hold entities accountable for their cyber security postures.

3.98 By responding to the ACSC Cyber Security Survey, entities are provided with an assessment of their Essential Eight maturity by ASD (as discussed in paragraph 3.78). The survey is intended to enable ASD to understand the cyber security posture of entities to help inform the advice, assistance and technical guidance provided to entities. The survey results also inform ASD's annual report on Australian Government entities' cyber security posture to Parliament. With the lack of transparency on individual entities' cyber security maturity level, there has been no improvement in accountability.

Accountability to the Parliament

3.99 To increase the accountability of non-corporate Commonwealth entities to the Parliament on their cyber security compliance, the JCPAA recommended in *Report 467: Cybersecurity Compliance* that AGD and the ASD report annually to the Parliament on entities' cyber security posture.⁹⁴ Consistent with the JCPAA's findings, the ANAO also identified in Auditor-General Report No.53 2017–18 *Cyber Resilience* that there was a need to increase the accountability of entities' compliance with mandatory cyber security requirements.⁹⁵

3.100 Despite the increased public reporting since the 2017 JCPAA inquiry and 2017–18 Auditor-General Report, the status of individual entities' cyber security posture is not transparent. The aggregated public reporting from ASD and AGD does not provide details on individual entities' implementation of mandatory PSPF Policy 10 requirements or effectiveness of their implementation of the Essential Eight mitigation strategies. Consequently, the Parliament does not

93 Entities that have self-assessed an 'Ad hoc' or 'Developing' maturity for PSPF Policy 10 are required to detail the proposed strategies and associated timeframes for improving their maturity level to 'Managing'.

94 As discussed in paragraph 3.91, ASD tabled the inaugural report comprising the results from the 2019 ACSC Cyber Security Survey and the AGD's 2018–19 PSPF Policy 10 assessment reports in April 2020.

95 AGD had since publicly released the consolidated results for the PSPF compliance assessment reports (see paragraph 3.89).

have the necessary information to hold individual entities to account for their cyber security posture.

Upholding of accountability by cyber security governance committees

3.101 As noted in paragraph 1.15, the four whole-of-government governance committees with responsibilities in overseeing PSPF and cyber security initiatives for the improvement of Australian Government entities' cyber security posture are the:

- Government Security Committee;
- Cyber Security Band 3 Inter-Departmental Committee;
- Cyber Security Strategy Delivery Board; and
- Secretaries Board.

Government Security Committee

3.102 As part of the 2018 PSPF reforms, the Government Security Committee agreed that a maturity assessment model for entities' annual PSPF self-assessment was the most effective and efficient manner to provide assurance to the Government on protective security arrangements of entities.

3.103 Matters discussed at the meetings include the development of the PSPF reporting portal, extension of the submission date for entities' PSPF assessment reports, potential ways to minimise duplication between the PSPF assessment and the ACSC Cyber Security Survey, and implementation of the PSPF maturity assessment model. A standing agenda for the Government Security Committee meetings is updates from ASD on the cyber environment and cyber security issues that may affect PSPF requirements.

3.104 AGD provided aggregated reporting on the 2018–19 whole-of-government PSPF maturity assessment to the Government Security Committee at its May 2020 meeting. The committee noted the low maturity assessed for cyber security under Policy 10. The committee was informed that implementation of the Top Four mitigation strategies was an area with low maturity and ongoing vulnerabilities for Australian Government entities, with application control and patching applications being the key mitigation strategies of concern.

3.105 The ANAO's review of meeting minutes also found that no advice was provided by the Government Security Committee to other cyber security governance committees, the Secretaries Board or the government regarding the actions required by individual entities to mitigate cyber security issues identified in the PSPF self-assessments. AGD informed the ANAO that there was no significant cyber security issue from the 2018–19 PSPF assessment report that required attention from the Secretaries Board.⁹⁶

3.106 To fulfil its role in reporting to government on PSPF maturity and entities' security capability, AGD informed the ANAO in September 2020 that it is considering plans for the Attorney-General to write to all portfolio ministers and provide them with the consolidated 2018–19 PSPF assessment report once it has been considered and approved. AGD released the 2018–19 consolidated PSPF

96 The brief to the Attorney-General requesting the release of the 2018–19 PSPF assessment report notes that 'Information security remains an ongoing issue for non-corporate Commonwealth entities, with 13% reporting at the 'ad hoc' level' and that 'Of the information security policies, PSPF Policy 10 - Safeguarding information from cyber threats, which includes a requirement to implement the Australian Signals Directorate's Top 4 strategies to mitigate cyber security incidents (Top 4 strategies), had the lowest maturity.'

maturity assessment report on the PSPF website on 15 January 2021. The provision of a consolidated PSPF assessment report to portfolio ministers does not facilitate an increase in accountability for entities to improve their cyber security posture.

Cyber Security Band 3 Inter-Departmental Committee

3.107 The Cyber Security Band 3 Inter-Departmental Committee has considered the Cyber Uplift Program, Essential Eight+ Sprints⁹⁷, the Host-Based Sensor program, Australia's Cyber Security Strategy 2020, and the hardening of Government's IT systems. In the 27 February 2020 meeting, the committee discussed the 2019 cyber security posture report and outcomes of the ACSC's Cyber Uplift Program. The committee noted the difficulty faced by smaller agencies in implementing effective cyber security risk mitigation strategies due to their lack of capabilities. The committee agreed that Home Affairs and PM&C were to jointly develop a paper to the Secretaries Board on how to address the risks identified in the cyber security posture report and the Cyber Uplift Program.

3.108 The paper on the issues regarding Australian Government cyber security posture was discussed at the 10 June 2020 meeting of the Secretaries Board. The issues identified include a lack of coordination for the uplift of Government's cyber security, lack of realisation of economies-of-scale, budget process inhibition on entities' ICT investment, limitation in the PSPF, and an accumulation of vulnerable legacy systems. The paper discussed the centralisation of Government IT capability through consolidation of Government systems as a measure to mitigate the issues. The Secretaries Board noted the risks and vulnerabilities identified in Government networks and systems. A Hardening Government IT Board was initially established to oversee activities under the initiative to centralise Australian Government entities' IT infrastructure. The Hardening Government IT Board was subsumed by the Secretaries Digital Committee established in August 2020 (see paragraph 3.124).

3.109 Following the Prime Minister's announcement in June 2020 regarding the malicious cyber activity against Australian networks, ASD provided an update at the July 2020 Cyber Security Band 3 Inter-Departmental Committee meeting on the decision to publicly announce the cyber incident and the subsequent positive results achieved based on ASD's statistics.⁹⁸ The committee co-chair highlighted the importance of entities' defences for deterring and responding to cyber security incidents, and whole-of-government cooperation on such issues.

Cyber Security Strategy Delivery Board

3.110 The Cyber Security Strategy Delivery Board, chaired by Home Affairs, was established in August 2020 to drive the implementation of Australia's Cyber Security Strategy 2020. To date, the Cyber Security Strategy Delivery Board has met in September and November 2020 respectively. Items discussed in the initial two meetings include implementation progress update against the key initiatives of Australia's Cyber Security Strategy 2020, the implementation plan and engagement with relevant stakeholders.

97 The Cyber Security Band 3 Inter-Departmental Committee agreed to the selection and prioritisation of the 25 entities for ASD Essential Eight+ Sprints in April 2019.

98 ASD's statistics indicated that there were over 270,000 page views of the joint advisory issued by ASD and Home Affairs on *Copy-Paste Compromises – tactics, techniques and procedures used to target multiple Australian networks*. There were also a six-fold increase in daily visits to the cyber.gov.au website, and over 900 new applications for the ACSC Partnership Program (see footnote 71). There were around 600 existing ACSC partners on the day of the Prime Minister's announcement.

Secretaries Board

3.111 In the period July 2018 to August 2020, the Secretaries Board received regular PSPF updates, and considered the Government cyber security posture and measures to improve cyber security. As noted in paragraph 3.108, the Secretaries Board was presented with a paper in June 2020 on issues in relation to the cyber security posture of Australian Government entities and potential measures to resolve the issues.

3.112 In May 2017, PM&C and ASD engaged Australian cyber security firm Hivint Pty Ltd (Hivint) to conduct a scan of the internet-based profile of Australian Government entities to identify cyber security risks across public facing Government systems from October 2017 to January 2018. Hivint's assessment identified a range of poor cyber hygiene practices in Australian Government entities, with many entities not being compliant with security policies and not consistently implementing effective cyber security practices. Following the delivery of the assessment results to entities in November 2018, department secretaries were required to provide advice to ASD on their management of identified cyber risks in their portfolio. In March 2019, ASD presented a report on 'Cyber Security Vulnerabilities – Portfolio Secretaries advice on managing Hivint findings' to the Secretaries Board. The Secretaries Board noted the report presented.

3.113 The report presented to the Secretaries Board in March 2019 consolidated the advice provided by the portfolio secretaries and provided high level common themes observed from the risk management plans of the portfolio.⁹⁹ The portfolio plans indicated that improvements were to occur over a period of three to six months, primarily through configuration management, active contract management and staff training. ASD has subsequently developed an in-house capability — Cyber Hygiene Improvement Programs— to identify and measure changes in cyber hygiene across Australian Government entities.¹⁰⁰

3.114 The Secretaries Board did not adopt a similar approach for entities that had self-assessed a low maturity for cyber security and Top Four implementation under PSPF Policy 10. There was no obligation for individual entities with low maturity for PSPF Policy 10 to take actions to mitigate cyber security risks and report back on any such actions taken. Non-corporate Commonwealth entities have not been held to account for not meeting mandatory cyber security requirements under PSPF Policy 10.

99 All portfolios advised ASD of their actions to manage cyber risks for email security, digital certificates and Transport Layer Security (TLS) configuration, open or sensitive services (open ports), third party breaches and hosting of public-facing digital services from locations outside Australia.

100 The Cyber Hygiene Improvement Programs (CHIPs) is an automated discovery and reporting process that identify cyber hygiene issues in federal, state and territory, and local government internet facing IT services. As of August 2020, ASD has conducted vulnerability scanning on the following cyber hygiene indicators: email security; website encryption; email encryption; dormant websites; and critical vulnerabilities in public-facing websites. At the completion of a CHIPs assessment, ASD provides a report on vulnerability findings to entities that includes targeted mitigation and remediation guidance.

Recommendation no.13

3.115 The Australian Government strengthens arrangements to hold entities to account for the implementation of mandatory cyber security requirements.

Attorney-General's Department response: *Noted.*

3.116 *Any changes to the current accountability arrangements are a matter for Government.*

Australian Signals Directorate response: *Noted.*

3.117 *ASD will work with the Attorney-General's Department and the Department of Home Affairs to support efforts relating to the strengthening of entity cyber security arrangements. ASD is neither a regulatory body nor a compliance reporting agency and is not legally empowered to perform such functions. ASD provides technical advice and assistance to entities consistent with ASD's functions as set out in section 7(1) of the Intelligence Services Act 2001 (Cth).*

Department of Home Affairs response: *Noted.*

3.118 *Under the Minister for Home Affairs, the Department of Home Affairs is responsible for national cyber security policy and overseeing implementation of Australia's Cyber Security Strategy 2020 which aims to uplift cyber security for the whole of economy, including government through the Hardening Government IT Program. The Department will brief the Government on the ANAO's findings and recommendations as they relate to national cyber security policy and implementation of Australia's Cyber Security Strategy 2020.*

Establishment of 'cyber hubs'

3.119 As discussed in paragraph 1.13, Home Affairs is responsible for coordinating the implementation of Australia's Cyber Security Strategy 2020. A key initiative within the Cyber Security Strategy 2020 for Australian Government entities is the hardening of Government's ICT systems against cyber threats. The Digital Transformation Agency (DTA) is responsible for leading the Hardening Government IT Program, which focusses on centralising government networks through secure hubs, with support by Home Affairs, AGD and ASD in their respective roles as cyber policy and operational entities.

3.120 The centralisation of Government networks seeks to reduce opportunities for malicious actors to target agencies that have less secure ICT systems and drive greater efficiencies in the Australian Government's cyber security investment. It was intended that the 'cyber hubs' will improve the ability of Government entities to identify, protect, detect, respond and recover from malicious intrusions. According to Home Affairs, the 'cyber hubs' are to help ensure baseline cyber security standards are met by improving entities' implementation of the mandatory Top Four mitigation strategies.

3.121 The indicative implementation roadmap for the 'cyber hubs' includes the consolidation of secure Internet gateways and services into 'cyber hubs' to create a strengthened perimeter for Australian Government networks. Existing business systems are then planned to be transferred to 'cyber hub' providers, and the development of a Government Cloud in later phases of the initiative to allow agencies to transition obsolete or at-risk services to modern, secure operating environments.

3.122 In September 2020, the DTA completed a six-week discovery activity to inform the design of the 'cyber hubs' model. Home Affairs, Services Australia and the Department of Defence have been identified as pilot 'cyber hub' providers to test the monitoring, detection and reporting capabilities on client entities' networks. The pilot hubs are expected to be established by 30 June 2021.

3.123 The 'cyber hub' providers would be responsible for securing, assessing and certifying their own infrastructure in line with the ISM and for mandatory reporting of protective security capability under the PSPF. ASD plans to create a 'cyber visibility centre' to provide strategic whole-of-government cyber security advice to the 'cyber hub' providers.

3.124 A Secretaries Digital Committee has been established to oversee the activities under the initiative to harden Government ICT systems. The Secretaries Digital Committee is a sub-committee of the Secretaries Board and is chaired by the Secretary of the Department of Social Services, with secretariat support provided by the DTA. The committee's role is to provide strategic leadership to promote an enterprise approach to the planning, coordination and delivery of trusted and secure digital and ICT capabilities across Australian Government entities. The committee held its first meeting in September 2020.

3.125 Under the Hardening Government IT Program, AGD is responsible for working with DTA and other stakeholders to ensure the 'cyber hubs' are in alignment with the PSPF. AGD plans to update the PSPF by the end of June 2021 in consideration of:

- the lines of accountability under the proposed 'cyber hub' model;
- opportunities to support more effective management of cyber security risks across government; and
- potential improvements to arrangements for addressing shared and enterprise risks.

3.126 The ANAO's discussions with Home Affairs, AGD and ASD identified that the establishment of the 'cyber hubs' is at an early stage with further details on the operation of the hub model yet to be developed.



Grant Hehir
Auditor-General

Canberra ACT
19 March 2021

Appendices

Appendix 1 Entity responses



Australian Government
Attorney-General's Department
Acting Secretary

20/3285-3

19 February 2021

Mr Grant Hehir
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Mr Hehir *Grant*

Section 19 Proposed Audit Report - Cyber Security Strategies of Non-Corporate Commonwealth Entities

Thank you for the opportunity to review and provide comment on the proposed audit report on Cyber Security Strategies of Non-Corporate Commonwealth Entities. I acknowledge the findings in the report and have separately provided responses to each of the recommendations.

The Attorney-General's Department places a high priority on cyber security through its responsibility for administering the Protective Security Policy Framework (PSPF), and its own implementation of the framework.

The department will continue to undertake activity to progressively uplift AGD's maturity level with the view of achieving 'Managing' level for PSPF Policy 10 (Recommendation 7). In doing so, AGD will develop a strategy and set internal timeframes for implementation which will be monitored by the department's Audit and Risk Management Committee and the Security and Risk Management Committee. AGD also agrees to improve processes for documenting ICT security risk assessments undertaken (Recommendations 2 and 4). Consideration will be given to ensure that documentation is consistent, fit for purpose and appropriate for the department's risk context.

The department also remains committed to setting robust protective security standards for non-corporate Commonwealth entities. The department will continue to support entities to accurately self-assess and report on their implementation of cyber security requirements under the PSPF (Recommendations 9, 10 and 11).

I thank the ANAO for the constructive and transparent nature of its engagement throughout this audit. The department acknowledges there are opportunities for improvement as identified by the recommendations. The department has commenced work to address these areas.

The action officers for this matter are Rai Basu and Aileen Wang who can be contacted on 02 6141 3001 and 02 6141 2969 respectively.

Yours sincerely

Iain Anderson



Australian Government
Australian Signals Directorate

OFFICE OF THE
 DIRECTOR-GENERAL
ASD

Office of the Director-General
 PO Box 5076, Kingston ACT 2604
DGASD@defence.gov.au
 02 6265 0299

Mr Grant Hehir
 Auditor-General
 Australian National Audit Office
 GPO Box 707
 Canberra ACT 2601

Dear Mr Hehir,

Australian National Audit Office Section 19 Proposed Report: Cyber Security Strategies of Non-Corporate Commonwealth Entities

Thank you for your correspondence of 14 January 2021, containing the Proposed Report for the Australian National Audit Office (ANAO) report on Cyber Security Strategies of Non-Corporate Commonwealth Entities.

As highlighted in the report, the Australian Signals Directorate (ASD) continues to support the whole of economy, including Commonwealth entities, to make Australia the safest place to connect online. We continue to enhance our capabilities to automate threat detection and intelligence sharing arrangements across the Commonwealth, coupled with our ongoing technical uplift program and engagements to harden Commonwealth entity networks against malicious cyber activity.

Cyber espionage remains a substantial threat to Australia's economic prosperity and the confidentiality, integrity and availability of key networks and data across government. Adversaries are constantly adapting their tradecraft to exploit vulnerabilities and avoid detection.

ASD has considered the details of the proposed report and accompanying recommendations carefully and agrees with recommendation 12 and notes recommendation 13.

In relation to recommendation 12, ASD will work with the Attorney-General's Department to support their assurance processes on entities' reporting obligations under the Protective Security Policy Framework (PSPF).

ASD notes recommendation 13. ASD will work with the Attorney-General's Department and the Department of Home Affairs to support efforts relating to the strengthening of entity cyber security arrangements. ASD notes that it is neither a regulatory body nor a compliance reporting agency and is not legally empowered to perform such functions. ASD provides technical advice and assistance to entities consistent with ASD's functions as set out in section 7(1) of the *Intelligence Services Act 2001* (Cth).

Attached to this letter is ASD's Response to the Proposed Recommendations (**Enclosure 1**). Please contact Ms Abigail Bradshaw CSC, Head of the Australian Cyber Security Centre, if you require further information in relation to ASD's response.

ASD remains committed to assisting you with the successful completion of this report. I look forward to the upcoming tabling of the Final Report.

Yours sincerely,



Rachel Noble PSM
Director-General
Australian Signals Directorate
19 February 2021

Enclosure 1 – ASD's Response to the Proposed Recommendations



Australian Government
Department of Home Affairs

Grant Hehir
 Auditor-General
 Australian National Audit Office
 GPO Box 707
 Canberra ACT 2601

Dear Mr Hehir

Thank you for the opportunity to provide comments on the proposed audit report (the Report) on *Cyber Security Strategies of Non-Corporate Commonwealth Entities*. The Department of Home Affairs (the Department) welcomes this ANAO performance audit and acknowledges the valuable role the ANAO plays in providing independent insights into potential areas for improvement.

We also welcome the ANAO conclusion that cyber policy entities have worked together to support the implementation of cyber security requirements under the Protective Security Policy Framework.

Under the Minister for Home Affairs, the Department is responsible for national cyber security policy and overseeing the implementation of Australia's Cyber Security Strategy 2020 (the Strategy). The Strategy outlines a range of initiatives to uplift Australia's cyber security, including hardening government IT systems. This initiative is led by the Digital Transformation Agency and supported by the Australian Signals Directorate, the Department of Home Affairs and the Attorney-General's Department.

The Hardening Government IT Program involves the development of a new operating model to address the varying levels of cyber security maturity across Commonwealth entities, and through centralised 'cyber hubs' unifying the level of cyber resilience provided to all users of the hub.

While this initiative aims to strengthen Government's cyber security posture across Commonwealth entities, it is still under development. Any increase in accountability or transparency of mandatory cyber security requirements can be measured once this capability is operational.

The Department notes recommendation 13, and will brief the Government on the ANAO's findings and recommendations as they relate to national cyber security policy and implementation of Australia's Cyber Security Strategy 2020.

Of relevance, we also note and welcome Recommendation 4 of the Joint Committee of Public Accounts and Audit Report 485 *Cyber Resilience*, that the ANAO consider conducting an annual limited assurance review into the cyber resilience of Commonwealth entities.

I would like to thank you and your officers for the collaborative approach taken in conducting this audit.

Yours sincerely

Ben Wright
 Chief Audit Executive

17 February 2021

6 Chan Street Belconnen ACT 2617
 PO Box 25 Belconnen ACT 2616 • Telephone: 02 6264 1111 • Fax: 02 6225 6970 • www.homeaffairs.gov.au



Australian Government
Department of the Prime Minister and Cabinet

SECRETARY

Ref: EC21-000043

Mr Grant Hehir
Auditor-General
Australian National Audit Office
Office of the Auditor-General
OfficeoftheAuditorGeneralPerformanceAudit@anao.gov.au

Dear Mr Hehir

Thank you for the opportunity to respond to the proposed report, Cyber Security Strategies of Non-Corporate Commonwealth Entities. As outlined in the correspondence on 15 January 2021, I am providing the below response for further consideration before your preparation of the final report. We note and appreciate the further active engagement of your team to include the considerations of the Australian Signals Directorate and the appropriate level of disclosure in the report.

Cyber threats are an increasing risk across all levels of government. I take those threats and the implementation of management processes to mitigate those threats very seriously. This means maintaining the highest standard of security, reliability and resilience of our systems and networks given their criticality to our national security, as well as the importance of maintaining public trust in public services.

At the Department of the Prime Minister and Cabinet (PM&C) we work very hard to maintain the highest standards in cyber security, underpinned by strong privacy and security protections, particularly as threats and targets rapidly evolve and shift. We work collaboratively with our staff to enhance the cyber security culture, constantly making sure our staff are cyber aware and vigilant, embedding behaviours as standard work practices.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5111 Fax: +61 2 6271 5414 www.pmc.gov.au ABN: 18 108 001 191

With regard to the findings generally, we note that the Australian Cyber Security Centre (ACSC) provides broad guidance through the Information Security Manual (ISM) on control mechanisms that entities should put in place. We recognise agencies are encouraged to take a risk-based approach regarding the implementation of ACSC's security controls based on the agency's risk framework. On this basis, PM&C considers that it is compliant with all Top 4 Cyber Mitigations as effective risk controls are in place.

The ANAO assessed in its audit that PM&C is non-compliant with one of the Top 4 Cyber Mitigations. PM&C does not agree with the ANAO's assessment.

Specifically, the ANAO proposed additional processes regarding the detailed implementation of certain security controls, and on that basis considered PM&C non-compliant with one of the Top 4 Cyber Mitigations. PM&C has validation processes in place which adhere to the recommendations of the Information Security Manual and believes that this meets the requirement of the ISM and ACSC guidance.

We note that we will continue to make every effort to improve our processes and it is with this context I provide our response to the draft report. I accept recommendation 1 and 3 as they apply to the Department.^a

Recommendation 1

The Department of the Prime Minister and Cabinet strengthens its validation of privileged user access, specifically documenting the confirmation of the requirement for access from those who are responsible for approving privileged access.

Agreed

PM&C has made changes to the revalidation process of administrative accounts, with additional processes being added to the PM&C primary network system security plan. PM&C considers that the process assessed by the ANAO was consistent with ACSC and ISM control recommendations. We note that no administrator access was found by the ANAO during the course of the audit that exceeded that individual's requirement to perform their duties.

Recommendation 3

The Department of the Prime Minister and Cabinet:

- a) improve its risk assessment of security events; and
- b) improve testing of security configurations and reviews of user access to ensure that the configurations are operating as intended.

Agreed

Anomalies in our security event reporting (from our technical logging system) found by ANAO during the course of this audit have been investigated and addressed. Security event reporting is now working as intended. A risk assessment on the current security event system and processes has been completed, with any residual risk accepted by the department.

As part of our scheduled hardware upgrade process there is an active project in place to enhance our security event systems within PM&C which will also improve and streamline the risk assessment process.

The highlighting of these issues via the audit has provided valuable information for our consideration. As always, we appreciate the courteous and collaborative approach from your colleagues to the audit process.

Yours sincerely



Philip Gaetjens
10 March 2021

ANAO comment on Department of the Prime Minister and Cabinet response

- (a) As noted in paragraph 1.33, to meet the requirement of the PSPF, the ACSC's Essential Eight Maturity Model requires a minimum set of security controls be implemented to achieve 'Maturity Level Three'. PM&C was unable to provide evidence of the effective implementation of one of the security controls.



Australian Government

Future Fund

Mr Grant Hehir
Auditor-General
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Mr Hehir

ANAO Report on Cyber Security Strategies of Non-Corporate Commonwealth Entities

Thank you for providing the opportunity to comment on the proposed audit report on the Cyber Security Strategies of Non-Corporate Commonwealth Entities, prepared by the Australian National Audit Office ("**ANAO**").

The Future Fund Management Agency ("**Agency**") is committed to providing a secure cyber environment to safeguard the assets of the Commonwealth. Underpinning this is the full implementation of the Top Four of the Essential Eight mitigation strategies. The Agency expects to achieve full implementation of the Top Four mitigation strategies by the end of calendar year 2021.

The Agency welcomes and agrees with the ANAO's findings and Recommendation 8. The Agency's Operational Risk & Compliance Committee ("**ORCC**") now receives quarterly status reports to monitor the progress of the Essential Eight improvement activities against the timeframes set. The first such report was received by the ORCC in November 2020. In addition, from 2021, the Board Audit & Risk Committee will receive such status reports at least annually.

Attachment 1 to this letter outlines an editorial matter we wish to bring to the attention of the ANAO for consideration in finalising the report.

I would like to thank the ANAO for the cooperation of the audit team and the professional manner in which the audit was conducted.

Yours sincerely

Hon Peter Costello AC
Accountable Authority
15 February, 2021

Level 14/447 Collins Street, Melbourne VIC 3000 • Locked Bag 20010, Melbourne Vic 3001
Telephone: +61 3 8656 6400 • Facsimile +61 3 8656 6500
Internet www.futurefund.gov.au

A865296



Australian Government

Australian Trade and Investment Commission

15/2/2021

Grant Hehir
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Mr Hehir

Austrade's response to ANAO Audit Report: Cyber Security Strategies of Non-Corporate Commonwealth Entities.

Thank you for providing the Australian National Audit Office's (ANAO) proposed report under Section 19 of the Auditor-General Act 1997 on Cyber Security Strategies of Non-Corporate Commonwealth Entities.

Austrade appreciates the opportunity to respond to the matters raised in the proposed report. In general we support the findings of the report, with specific comments attached below.

Austrade has in place a comprehensive program of work to mature our cyber security posture. This report acknowledges and supports the work we are undertaking and will help focus on clear delivery timeframes for increasing our maturity levels.

Yours sincerely

A handwritten signature in blue ink, appearing to read 'T. Beresford'.

Tim Beresford

Acting Chief Executive Officer

T +61 (2) 939 22379

Level 7, Tower 3, International
Towers, 200 Barangaroo Ave,
Sydney NSW 200, Australia

ABN: 11 764 698 227

If you are not the intended addressee of this letter, please notify the sender immediately and destroy this. Australia's anti-bribery laws operate overseas and Austrade will not provide business related services to any party who breaches the law and will report credible evidence of bribery.



Australian Government
Department of Education,
Skills and Employment

Our Ref: EC21-000212

Secretary
Dr Michele Bruniges AM

Mr Grant Hehir
Auditor-General
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Grant
Dear Mr Hehir

Cyber Security Strategies of Non-corporate Commonwealth Entities

Thank you for the opportunity to respond to the proposed Australian National Audit Office (ANAO) audit report on the Cyber Security Strategies of Non-corporate Commonwealth Entities. The department recognises the importance of cyber security and is committed to continuing to improve its cyber security maturity and build its cyber resilience.

The department's summary response to the report is below:

The Department of Education, Skills and Employment ('the department') welcomes the ANAO's report on Cyber Security Strategies of Non-corporate Commonwealth Entities.

The department notes the key messages to all Australian Government entities in the audit report and agrees with the one recommendation provided to it.

The department is committed to managing cyber security risks and building a resilient cyber security posture. The department notes that, building on its Protective Security Policy Framework (PSPF) 2019-20 self-assessment report and associated external assessment, a workplan with timeframes for improving security maturity and achieving a 'Managing' maturity rating for PSPF Policy 10 has been developed and endorsed by the department's Executive Board. The department has implemented arrangements to monitor progress of the workplan.

I have also enclosed the department's response to the recommendation as requested.

I would like to thank the review team of the ANAO for their work and acknowledge the collaboration between both departments in the drafting of this report.

50 Marcus Clarke Street, Canberra ACT 2601
GPO Box 9880, Canberra ACT 2601 | Phone 1300 566 046

If you would like further information on the department's response, please contact Scott Wallace, First Assistant Secretary, Technology Services Division, on (02) 6240 3620.

Yours sincerely

A handwritten signature in black ink that reads "Michele Bruniges". The script is cursive and fluid.

Dr Michele Bruniges AM

15 February 2021



Australian Government

Department of Health

Secretary

Mr Grant Hehir
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Mr Hehir

Department of Health response to the Proposed Audit Report – Performance Audit of Cyber Security Strategies of Non Corporate Entities.

Thank you for providing the Australian National Audit Office's (ANAO) proposed report pursuant to section 19 of the *Auditor-General Act* (1997) on the performance audit of Cyber Security Strategies of Non-corporate Entities. I appreciate the opportunity to respond to the report.

The department acknowledges the methodology and approach taken by the ANAO and appreciates the careful consideration of the feedback provided and the balanced approach to reporting audit findings.

The wording provided for the Summary Response can be found at [Attachment A](#).

I would like to thank the ANAO for its professionalism throughout the audit. If you have any questions regarding the department's response please contact Narelle Smith, Chief Audit Executive, Corporate Assurance Branch on (02) 6289 5342.

Yours sincerely

Brendan Murphy

19 February 2021

Phone: (02) 6289 8400 Email: Brendan.Murphy@health.gov.au

Scarborough House, Level 14, Atlantic Street, Woden ACT 2606 - GPO Box 9848 Canberra ACT 2601 - www.health.gov.au



Australian Government
IP Australia



Delivering a world leading IP system

ABN: 38 113 072 755

Phone: 1300 651 010

International: +61 2 6283 2999

www.ipaustralia.gov.au

17 February 2021

Mr Grant Hehir
Auditor-General
Australian National Audit Office

Dear Mr Hehir

Thank you for the opportunity to comment on the proposed audit report on Cyber Security Strategies of Non-corporate Commonwealth Entities.

IP Australia welcomes the report and its findings and the key messages for all Australian Government entities. We are committed to reaching our target maturity in line with the requirements of the Protective Security Policy Framework.

I would like to thank your officers for their professionalism and engagement during the audit process.

Yours sincerely

Michael Schwager

Appendix 2 Recommendation for the cyber policy entities in Auditor-General Report No.53 2017–18 *Cyber Resilience* and their respective responses

The following Recommendation no.2 from Auditor-General Report No.53 2017–18 *Cyber Resilience*, tabled in the Parliament on 28 June 2018, was made to the three cyber policy entities — Attorney-General's Department, Australian Signals Directorate and Department of Home Affairs. The responses of the three entities to the recommendation are also replicated below.

Recommendation no.2

In revising security reporting and cyber-related requirements under the *Protective Security Policy Framework*, the Attorney-General's Department, Department of Home Affairs and Australian Signals Directorate work together to improve compliance with the framework by:

- (a) providing adequate technical guidance to support entities to accurately self-assess compliance with the Top Four mitigation strategies and their underlying controls contained in the Information Security Manual;
- (b) developing a program for verifying entities' reported compliance with the mandatory cyber security requirements; and
- (c) increasing transparency and accountability about entities' compliance with those requirements.

Attorney-General's Department's response

(a): *Agreed.*

Proposed reforms to the Protective Security Policy Framework (PSPF), which are to take effect later this year, more clearly articulate the policy requirements for safeguarding information from cyber threats, as well as the links to underlying controls contained in the information security manual. The department notes the ANAO's paragraph 3.35 finding that 'it is important that the Australian Signals Directorate (ASD) develops such guidance (providing detailed control assessment test plans) to support the reporting changes underway'; the department agrees to support ASD in this work.

(b): *Agreed in principle.*

To support verification, the department's proposed reforms to the PSPF will introduce enhanced reporting obligations designed to provide greater assurance of the accuracy of entities' self-assessed reporting. For example, entities will be required to provide supporting evidence to demonstrate a cycle of security planning, monitoring and reporting each year, and explain how key security risks are managed.

Developing a verification program for cyber security is a matter for the Australian Cyber Security Centre. The department supports ASD and Department of Home Affairs considering possible further verification mechanisms and will provide assistance as appropriate.

(c): *Agreed.*

The department acknowledges the importance of improving transparency and accountability. To support this, the department agrees to publicly release the 2017–18 consolidated annual whole-of-government Protective Security Compliance Report (and future maturity reports).

Australian Signals Directorate's response: Agreed.

ASD agrees with Recommendation 2. ASD acknowledges the inconsistent mapping between the 2017 Australian Government Information Security Manual and the Essential Eight Maturity Model. ASD is currently consulting on proposed changes to address this in the 2018 Australian Government Information Security Manual and continues to work with the Attorney General's Department to ensure alignment with Protective Security Policy Framework reforms. While ASD provides cyber security advice to a variety of audiences, it remains the responsibility of Commonwealth entities to maintain a workforce of competent cyber security practitioners capable of assessing the effective implementation of security controls for their information and communication technology systems.

ASD agrees to continue working with the Attorney-General's Department and the Department of Home Affairs but notes that it is neither a regulatory body nor a compliance reporting agency. ASD works to provide better practice cyber security guidance to Commonwealth entities. ASD commends Commonwealth entities which achieve full compliance with mandatory requirement INFOSEC 4 from the Protective Security Policy Framework and also recognises the achievements of those making significant and sustained annual improvements to their cyber security posture.

ASD supports mature risk management frameworks for cyber security over compliance-based programs. Further, ASD encourages positive and sustained improvements to Commonwealth entities' cyber security posture over time. From experience we acknowledge that in some circumstances the application of all Top Four mitigation strategies may not be practicable, or introduces additional risks, and that other mitigating controls may achieve a similar outcome. ASD agrees to work with the Attorney-General's Department and the Department of Home Affairs to assist both entities further their compliance measurement goals.

Department of Home Affairs response: Agreed.

The Department of Home Affairs (Home Affairs) supports this recommendation. Home Affairs agrees there should be adequate technical guidance to support entities and a verification program for reported compliance. Home Affairs further supports the [ANAO's] view that there should be increased transparency and accountability regarding entities' compliance.

Home Affairs will continue to work closely with the Australian Signals Directorate and Attorney General's Department to strengthen the standard of cyber security of Australian Government networks.

Home Affairs has responsibility for cyber security policy and coordination. In this capacity, Home Affairs will support the Attorney-General's Department efforts to update the Protective Security Policy Framework and the Australian Signals Directorate's efforts to update the Information Security Manual, including ensuring these policies are mutually supportive of the goal of improved cyber security standards across government.

Home Affairs supports the Attorney-General's Department undertaking to publish the 2017-18 consolidated annual whole-of-Government Protective Security Compliance Report (and future maturity reports).

Home Affairs will work with the Attorney-General's Department and the Australian Signals Directorate to develop a fit-for-purpose mechanism for verifying entities reported compliance and provide advice to the Secretaries' Cyber Security Board.

Appendix 3 2019–20 PSPF assessment questions for ‘Policy 10: Safeguarding information from cyber threats’

The following questions, known as the security maturity questions, are asked in the ‘Detailed Assessment’ section of Policy 10. The questions require the entity to assess the level of the entity’s implementation of the mandatory and supporting requirements for Policy 10.

Box 2: Policy 10 questions for the 2019–20 PSPF assessment

- 10.1 The entity implemented 'application control' (also known as ‘application whitelisting’) in accordance with the Strategies to Mitigate Cyber Security Incidents.
- 10.2 The entity implemented 'patching applications' in accordance with the Strategies to Mitigate Cyber Security Incidents.
- 10.3 The entity implemented 'restricting administrative privileges' in accordance with the Strategies to Mitigate Cyber Security Incidents.
- 10.4 The entity implemented 'patching operating systems' in accordance with the Strategies to Mitigate Cyber Security Incidents.
- 10.5 The entity configured ‘Microsoft Office macro settings’ in accordance with the Strategies to Mitigate Cyber Security Incidents.
- 10.6 The entity implemented ‘user application hardening’ in accordance with the Strategies to Mitigate Cyber Security Incidents.
- 10.7 The entity implemented 'multi-factor authentication' in accordance with the Strategies to Mitigate Cyber Security Incidents.
- 10.8 The entity implemented ‘daily backups’ in accordance with Strategies to Mitigate Cyber Security Incidents.
- 10.9 The entity had measures in place to reduce the risk of harm to the public when transacting online with the entity.
- 10.10 The entity has considered which of the remaining Strategies to Mitigate Cyber Security Incidents it needed to implement in order to protect the entity.
- 10.11 Which of the remaining Strategies to Mitigate Cyber Security Incidents did your entity implement?

Source: 2019–20 PSPF assessment questions for ‘Policy 10: *Safeguarding information from cyber threats*’.

Appendix 4 Entities' views on the supporting guidance for PSPF Policy 10 self-assessment

The ANAO sought the views of the selected entities under this audit regarding the supporting guidance available for their PSPF Policy 10 self-assessment. The views expressed by the entities are outlined in Box 3.

Box 3: Views of the selected entities regarding the guidance for PSPF Policy 10 self-assessment

- 'It is complex. There are questions about the Top Four, which we are rated on, the other of the Essential Eight which we are rated on but not in our aggregated rating, and the other of the 37 mitigation strategies which are not rated on. It is not clear how those answers contribute to our maturity, or why they are asked. My understanding of the 37 strategies is that we select them and implement them in a way that manages the risk in our environment. Asking which ones we have in place does not reveal whether we risk manage the controls. The PSPF deferring to the ACSC Essential Eight advice does not help to make this clear.'
- 'The previous Essential Eight Maturity Model was highly prescriptive, more of a checklist, and contrary to the PSPF maturity model. However the new ISM maturity model can align and we have referenced it in ... It will be useful in measuring our progress and completeness levels of various controls. However, we are still aware of minor inconsistencies between the PSPF and ISM leading to unnecessary deliberation over the interpretation and application in our own context.'
- 'The guidance provided by AGD on the PSPF self-assessment is open to interpretation, which may lead to some entities reporting lower or higher levels of maturity. There is clarity around the requirements to meet the four levels of maturity including ad hoc, developing, managing and embedded. In order for entities to be benchmarked accurately there needs to be a common understanding of how entities should arrive at their maturity rating. We interpreted the requirements for accurate reporting to mean the department should take a holistic view of their environment and reports its maturity based on its weakest link. For example the department has a complex environment and operates a number of segmented domains, where a control has been fully implemented in some domains but not others the department reports the lowest level of maturity. Our view is that AGD could provide additional clarity around whether this is the expected approach to ensure all entities are reporting the same way for benchmarking.'
- 'Our view is that there is some misalignment between the guidance provided by ACSC and AGD around the implementation of the Essential Eight controls including:
 - AGD mandates the implementation of the Top Four controls, whereas ACSC recommends the implementation of all Essential Eight mitigations on a risk based approach.
 - AGD mandates the department secretary must sign off on all non-compliances with the mandatory control, the ISM risk based approach allows the Department Chief Security Officer (CSO) to accept residual risk.

- AGD uses a four tiered approach to assessing controls, where ACSC recommendations for the implementation of Essential Eight use a three tier approach. Reaching Maturity Level 3 across any of the Essential Eight controls should equate to embedded rating in the PSPF, however it would also be assumed the Maturity Level 1 against any of these controls would only achieve a partial rating in PSPF.

Further guidance on the mapping and correlation between the ISM and PSPF would assist entities in reporting accurately, and ensuring the governance requirements are achieved.'

- 'The guidance is sufficient and clear. However, it would be useful and easy for agencies if there was a direct "mapping" between various Essential Eight maturity levels (1, 2 & 3) and PSPF maturity levels.'
- 'From our perspective, there is a difference in view between the PSPF and ISM on roles and responsibilities. PSPF states that only the "Accountable Authority" is authorised to accept residual security risks on behalf of the agency, (not even the Chief Security Officer), however, the ISM states that the CISO [Chief Information Security Officer] can be the "Authorising Officer" (previously known as "Accreditation Authority" for systems). In which case, are Authorising Officers also permitted to accept residual security risks on behalf of the agency? This requires alignment.'
- 'The guidance provided by AGD on the PSPF self-assessment is reasonable. Both the PSPF and the Essential Eight are regularly changed and updated, which is necessary and makes reaching a target level of maturity challenging. Additionally, the PSPF refers to the Essential Eight and the two may not necessarily be in total alignment when it comes to self-assessment questions and guidance.'
- 'There is, in some cases, some latitude for interpretation that can be made around the self-assessment of individual controls, which can result in questions around whether the essence and intent of the particular controls are being met, but this is preferable to being overly prescriptive. It is important that, in developing any improved maturity scoring models, AGD and ACSC do not move back towards compliance-based frameworks that do not allow for the consideration of risk in determining an agency's approach.'