The Auditor-General
Auditor-General Report No.27 2021–22
Performance Audit

Administration of the Revised Protective Security Policy Framework

Attorney-General's Department

Department of Social Services

Services Australia

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76033-721-6 (Print)
ISBN 978-1-76033-722-3 (Online)

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

Or via email:
communication@anao.gov.au.

Australian National
Audit Office

Canberra ACT

12 May 2022

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 in the Attorney-General's Department, the Department of Social Services and Services Australia. The report is titled *Administration of the Revised Protective Security Policy Framework.* 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

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

Natalie Maras
Chay Kulatunge
Amanda Reynolds
Dale Todd
Corinne Horton

Contents

Audit snapshot

Auditor-General Report No.27 2021–22

Administration of the Revised Protective Security Policy Framework

Why did we do this audit?

- Physical security protects people, information and assets enabling safe and secure government business.
- The revised Protective Security Policy Framework (PSPF) was implemented in 2018.
- Previous ANAO audits have identified that too strong a focus on red tape reduction can be at the expense of effective outcomes.

Key facts

- The PSPF applies to 97 Australian non-corporate Commonwealth entities and represents better practice for 71 corporate Commonwealth entities and 18 wholly owned Commonwealth entities.
- The Attorney-General's Department (AGD) has published two whole-of-government maturity reports under the revised framework.

What did we find?

- The administration of the revised PSPF by selected entities was largely effective.
- Advice to government by AGD as policy owner is limited as it is reliant on self-reporting from entities that may not understand and follow the mandated security reporting requirements.
- The Department of Social Services (DSS) and Services Australia have not met all core requirements at their self-assessed maturity levels in safeguarding people, information, and assets.

What did we recommend?

- There were five recommendations, one relating to AGD; two relating to DSS; and two relating to Services Australia.
- AGD agreed to one recommendation, DSS agreed to two recommendations, and Services Australia agreed to two recommendations.

17.5%

of reporting entities assessed their physical security for resources as ad hoc or developing

30%

of reporting entities assessed their protective security for facilities as ad hoc or developing

Summary and recommendations

Background

1. In response to recommendations in the 2015 Independent Review of Whole-of-Government Internal Regulation (Belcher Red Tape Review), to reduce compliance burden and to support entities to better engage with risk, the Attorney-General introduced a revised Protective Security Policy Framework (PSPF) on 1 October 2018.

2. The revised PSPF is underpinned by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requirements to govern an entity in a manner that is 'not inconsistent' with Australian Government policies and promote the proper use and management of public resources. Application of the PSPF is required by the 97 non-corporate Commonwealth entities (NCEs) and represents better practice for the 71 corporate Commonwealth entities and 18 wholly owned Commonwealth companies.

Rationale for undertaking the audit

3. Physical security arrangements underpin secure delivery of government business through the protection of people, information and physical assets. As Australian Government policy, the PSPF applies to all NCEs subject to the PGPA Act, with accountable authorities responsible for physical security arrangements within their own organisations.

4. As the policy owner, the Attorney-General's Department (AGD) has responsibility for monitoring and reporting whether the PSPF meets its intended outcomes. AGD undertakes its role through the provision of general, high-level guidance to entities on the PSPF. AGD also collects and reports entities' annual self-assessments and information on significant security incidents.

5. The Auditor-General has tabled performance audits identifying a low level of oversight and low levels of NCE compliance with mandatory policies. This audit will provide assurance about whether AGD is fostering the intended strong security culture through strategic, diligent, and risk-based administration of the PSPF, including by assessing the accuracy of self-reporting of physical policies by two entities.

Audit objective and criteria

6. The objective of the audit was to assess the effectiveness of administration of physical security in the revised PSPF.

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

- Has the Attorney-General's Department effectively administered the Australian Government's protective security policy framework?
- Are selected entities appropriately monitoring their security maturity and providing a safe and secure physical environment for their people, information and assets?

8. The audit did not include examination of the selected entities' compliance with the pre-October 2018 PSPF or PSPF policies 1 to 3 and 5 to 14.

Conclusion

9. The administration of the revised PSPF by selected entities was largely effective. Advice to government by AGD as policy owner is limited as it is reliant on self-reporting from entities. The risk of optimism bias in entity self-assessment reporting has not been addressed by AGD as part of its administration of the PSPF. The selected entities have not met all core requirements at their self-assessed maturity levels in safeguarding people, information and assets.

10. AGD's administrative arrangements to support the revised PSPF were largely effective. AGD's advice to government about the progress of the framework was limited as AGD relied on self-assessment information, which the ANAO has found can be overstated or inaccurate, to accurately reflect the maturity of implementation of revised PSPF requirements. As policy owner, AGD did not monitor compliance with mandatory requirements. AGD provided a variety of support including detailed written guidance that could be better tailored to low-risk and face-to-face service environments. AGD's role can be strengthened by closer alignment of the self-assessment reporting instrument and policy, and by ensuring that entities understand and follow the mandated security reporting requirements.

11. The Department of Social Services (DSS) was largely effective in implementing requirements that it established for itself under the PSPF at the 'managing' and 'embedded' maturity levels. DSS implemented a variety of physical security measures and integrated physical security considerations into its processes. DSS did not accurately report its maturity level as 'embedded' for policies 4, 15 and 16 because it did not always follow its plan, and documentary evidence of the certification authority's satisfaction with physical security requirements was incomplete.

12. Services Australia was largely effective at implementing requirements that it established for itself under the PSPF at the 'developing' maturity level. Physical security measures to protect people were well established and developing for information and physical assets. Protective security measures were integrated into business-as-usual operations, including at modified facilities. Services Australia's reporting was not accurate because in two years its reporting was based on an outdated security plan, and it did not evidence that most certifications and accreditations met requirements. Services Australia's Security Plan 2020–22 remedied deficiencies in its previous outdated plan. Certification and accreditation documentation is being reviewed and improved.

Supporting findings

Effectiveness of AGD's administration

13. AGD largely established fit-for-purpose governance arrangements to support its administration of the PSPF. AGD established governance bodies with defined roles, and it planned to manage risk, refine policies, and engage with other entities. AGD did not establish a framework for defining the effectiveness of the revised PSPF. The risk framework has not identified all appropriate risks, including the risk of optimism bias in entities' self-assessments (see paragraphs 2.4 to 2.28).

14. AGD collected annual entity self-assessments. In the context of indications that self-assessment information may not be accurate, including discrepancies in the reporting of significant security incidents, the use of self-assessment information to assess the effectiveness of the PSPF is limited (see paragraphs 2.30 to 2.46).

15. AGD was effective in analysing completeness of responses. AGD did not collect information to provide assurance over the self-assessment responses provided by entities. Reports to government and the public on the Australian Government's security culture and maturity were solely based on entity self-assessments. This reduces the level of assurance AGD has on its advice on whether the policy objectives of the PSPF are being met (see paragraphs 2.49 to 2.69).

DSS' security maturity monitoring and provision of a secure physical environment

16. DSS was largely effective at considering its progress against the goals and strategic objectives in its security plans. DSS had established a plan with goals and objectives and monitoring bodies received reports about security capability and risk culture. DSS' reported maturity levels were inaccurate because monitoring was not consistently against the indicators in the security plan and did not cover co-location sites. DSS captured and analysed performance data and used a limited range of performance data to inform change (see paragraphs 3.3 to 3.22).

17. DSS was largely effective at implementing physical security measures for its resources. DSS considered security risks at the enterprise level against its Security Plan 2019–21, as well as specific risk mitigation measures. DSS' reported maturity levels were not accurate because it adopted controls with less assurance where it could not undertake physical site inspections. DSS did not document its rationale for departing from the control in its Security Plan 2019–21, and it did not document the outcomes of its substitute processes (see paragraphs 3.23 to 3.37).

18. DSS was partly effective in implementing its protective security measures at selected facilities. It had integrated protective security measures at its facilities for all reporting years. In all reporting years its reported maturity levels were inaccurate because there were gaps in certification and accreditation documentation (see paragraphs 3.38 to 3.54).

Services Australia's security maturity monitoring and provision of a secure physical environment

19. Services Australia was partly effective at considering its progress against the goals and strategic objectives in its security plans. For the first two reporting periods assessed, Services Australia's reported maturity levels were inaccurate because the security plan was outdated, and Services Australia did not have a consistent and defined approach to monitoring its performance against identified goals and objectives (see paragraphs 4.3 to 4.17).

20. Services Australia was largely effective at implementing physical security measures for its resources at facilities visited by the ANAO. Services Australia's reporting of 'developing' was accurate because it did not implement all site security review recommendations, provide all information to staff, or fully assure itself of building access and usage of ICT facilities (see paragraphs 4.18 to 4.46).

21. Services Australia was largely effective in implementing protective security measures at sites visited by the ANAO. In all reporting years, it considered and substantially integrated physical security requirements into all facilities visited by the ANAO. In all reporting years, its reported maturity levels were inaccurate because certifications and accreditation were partially in accordance with applicable requirements. Documentary records lacked explicit determination and acceptance of residual security risks (see paragraphs 4.47 to 4.70).

Recommendations

Recommendation no. 1
Paragraph 2.47

The Attorney-General's Department review, reconcile and collate all significant security incident reporting data to inform assessments of whether the PSPF adequately supports entities to protect their people, information and assets.

Department response: *Agreed.*

Recommendation no. 2
Paragraph 3.18

The Department of Social Services review and adhere to its planned schedules for assessment and reporting of progress against actions and measures of success in the department's security plan.

Department response: *Agreed.*

Recommendation no. 3
Paragraph 3.55

The Department of Social Services complete its certification and accreditation of its security zone areas, with documentation in accordance with PSPF core requirements.

Department response: *Agreed.*

Recommendation no. 4
Paragraph 4.55

Services Australia undertakes site risk assessments as early as possible in the process of planning, selecting, designing and modifying its facilities.

Entity response: *Agreed.*

Recommendation no. 5
Paragraph 4.64

Services Australia review and strengthen its monitoring and assurance arrangements for key physical security controls that seek to protect agency and Australian Government resources (people, information and assets).

Entity response: *Agreed.*

Summary of entity response

22. Entities' summary responses to the report are provided below and their full responses are at Appendix 1.

Attorney-General's Department

> The Attorney-General's Department acknowledges the ANAO's findings and welcomes the ANAO's assessment that the department has been largely effective in its administration of the Protective Security Policy Framework (PSPF).
>
> As reflected in the Attorney-General's Directive on the security of government business, the policy intent of the PSPF is to ensure the secure delivery of government business. To discharge our role under the Attorney-General's Directive and the PSPF, the department employs a range of mechanisms to assess emerging security risks and refine protective security policy. The department remains committed to setting robust protective security standards to support non-corporate Commonwealth entities to protect their people, information and assets.

The department has accepted recommendation 1 (regarding security incident reporting) and is working towards implementation.

Department of Social Services

The Department of Social Services (the department) acknowledges the insights and opportunities for improvement outlined in the Australian National Audit Office (ANAO) report on Administration of the Revised Protective Security Policy Framework (PSPF).

The department maintains an array of physical security controls and measures to ensure we protect our people, information and assets. We acknowledge the ANAO's overall conclusion that the department was largely effective in implementing requirements established for ourselves in relation to the PSPF. The department accepts Recommendations 2 and 3 and acknowledges the suggested opportunities for improvement within the Report. Remedial activities addressing one recommendation have been completed with certification and accreditation of security zones now fully documented for all the department's sites.

A number of steps have already been undertaken to address the remaining recommendation and suggested opportunity for improvement. These will contribute to further strengthening of the department's security maturity, governance and performance monitoring and reporting.

Services Australia

Services Australia (the agency) welcomes this report and agrees with the ANAO's recommendations. The agency has commenced developing a strategy for a planned approach to uplifting the physical security maturity levels over future years. Our approach will take into consideration the audit findings, and incorporate any broader lessons where appropriate.

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.

Policy implementation

- High quality administration of a mandatory policy framework, such as the PSPF, requires a policy owner to use available evidence to assess the effectiveness of its compliance approach. Where audit activity shows that self-assessed performance information is regularly optimistic or inaccurate, a diligent policy owner provides more than self-assessed information to the Parliament for it to use. To hold the executive government to account, Parliament needs to be able to fully rely on the information provided to it.
- Accountable authorities have responsibility for ensuring that reporting is accurate and supported by appropriately assessed evidence. Where an evidence base is incomplete or under development, accountable authorities should accurately reflect this in their self-assessment, rather than report an aspirational state.

Audit findings

1. Background

Introduction

1.1 Protective security refers to the protection of information, people and physical assets. A security risk is something that could result in compromise, loss, unavailability or damage to information or physical assets, or cause harm to people. Physical security is the provision of a safe and secure physical environment.

1.2 The appropriate application of physical protective security measures by government entities ensures the operational environment necessary to conduct government business.

Overview of the Protective Security Policy Framework

1.3 The Protective Security Policy Framework (PSPF) was introduced to help Australian Government entities to protect their people, information and assets, both at home and overseas. The PSPF sets out the government's protective security policy and comprises five principles, four outcomes and 16 core policies.

1.4 The focus of this audit is the PSPF regarding physical security with a focus on policies 4, 15 and 16. Policy 4 describes how an entity monitors and assesses the maturity of its security capability and risk culture; policy 15 describes the physical protections required to safeguard people, information and assets; and policy 16 describes the approach to be applied to building construction, security zoning and physical security control measures of entity facilities.

1.5 The PSPF is not specifically legislated. The PSPF is underpinned by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requirements to govern an entity in a manner that is 'not inconsistent' with Australian Government policies and promote the proper use and management of public resources. Application of the PSPF is required by the 97 non-corporate Commonwealth entities[1] (NCEs) and represents better practice for the 71 corporate Commonwealth entities and 18 wholly owned Commonwealth companies.[2]

1.6 In 2015, the Independent Review of Whole-of-Government Internal Regulation (Belcher Red Tape Review) made seven recommendations to streamline the administration of the PSPF. The Belcher Red Tape Review recommended a shift from a compliance framework, underpinned by risk management principles, to a principles-based approach. To address the recommendations, to reduce the compliance burden and to support entities to better engage with risk, the Attorney-General introduced a revised PSPF on 1 October 2018.

1.7 Under the Administrative Arrangements Order of 18 March 2021, the Attorney-General's Department (AGD) is responsible for protective security policy. As set out in AGD's Corporate Plan 2021–25, AGD's purpose includes maintenance and improvement of Australia's law,

[1] There are 98 non-corporate Commonwealth entities listed in the Department of Finance flipchart last updated on 16 July 2021. This includes the Australian National Preventative Health Agency which ceased operations on 30 June 2014, with key functions transferring to the Department of Health.

[2] The PSPF also impacts non-government organisations that access classified information as they may be required to enter into a deed or agreement to apply relevant parts of the PSPF for that information.

justice, security and integrity frameworks.[3] The Attorney-General issued a Directive as part of the PSPF updates, which stated that AGD, with oversight of the Government Security Committee, will 'continue to assess emerging security risks and develop and refine protective security policy that promotes efficient secure delivery of government business'.[4] According to the Directive, the Attorney-General expects accountable authorities to implement PSPF requirements and use security measures proportionately to address their unique security environments.

Features of the revised Protective Security Policy Framework

1.8 The revised framework replaced the binary (yes or no) compliance model comprising 36 requirements with a four-scale maturity model (ad hoc, developing, managing, embedded). Both models contained mandatory requirements. Figure 1.1 depicts the four maturity scales in the new model.

1.9 Under the revised PSPF framework, entities are required to assess their security maturity against each of the 16 core policies contained within four security outcomes. Entities are also required to develop tailored plans and strategies, and to continuously update their security posture to reflect their changing risk profile.

1.10 For some entities, such as the Department of Social Services (DSS), physical security involves more than one site, including wholly owned and leased facilities in Australia. In the 2020 Australian Government Office Occupancy Report, Services Australia was the entity with the largest controlled area tenancies.[5] Services Australia is required to safeguard people, information and assets in 429 sites around Australia, including in rural and remote settings.

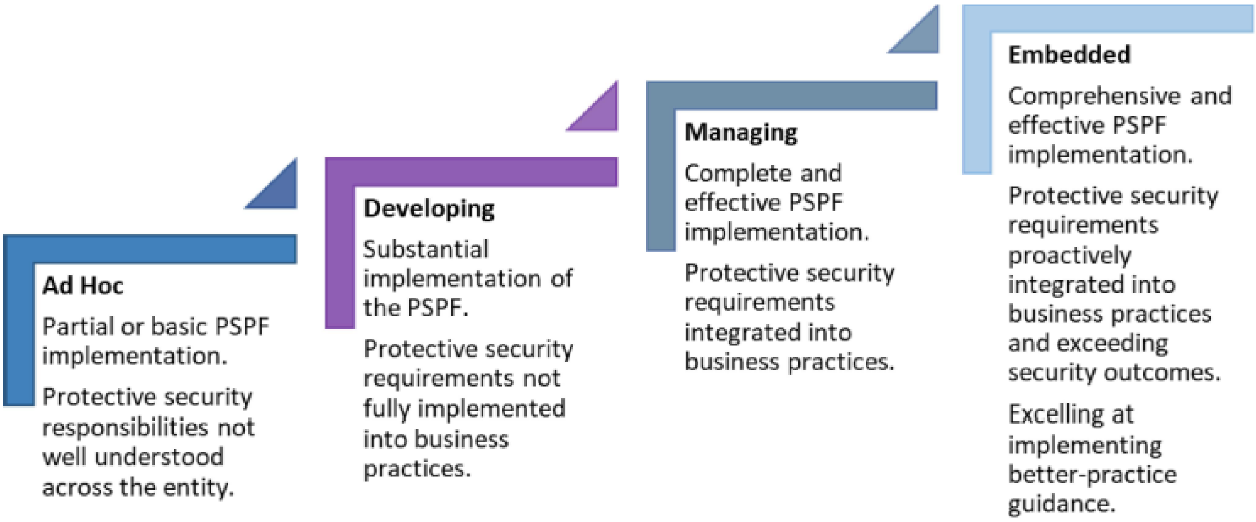
[3] See Attorney-General's Department, *Corporate Plan 2021–25*, AGD, Canberra, 2021. On page 5, the Corporate Plan 2021–25 states that AGD has two purposes.

> 1. Achieve a just and secure society through the maintenance and improvement of Australia's law, justice, security and integrity frameworks.
>
> 2. Facilitate jobs growth through policies and programs that promote fair, productive and safe workplaces.

[4] Attorney-General, *Directive on the Security of Government Business* [Internet], AGD, available from https://www.protectivesecurity.gov.au/about/security-government-business [accessed 2 May 2022].

[5] See Department of Finance, *Australian Government Office Occupancy Report 2020* [Internet], Department of Finance, available from https://www.finance.gov.au/sites/default/files/2021-11/2020-Australian-Government-Occupancy-Report.pdf [accessed 2 May 2022].

Figure 1.1: PSPF maturity assessment model


Ad Hoc
Partial or basic PSPF implementation.
Protective security responsibilities not well understood across the entity.
Developing
Substantial implementation of the PSPF.
Protective security requirements not fully implemented into business practices.
Managing
Complete and effective PSPF implementation.
Protective security requirements integrated into business practices.
Embedded
Comprehensive and effective PSPF implementation.
Protective security requirements proactively integrated into business practices and exceeding security outcomes.
Excelling at implementing better-practice guidance.

Source: Attorney-General's Department, *Protective Security Policy Framework 2019–20 Assessment Report*, p. 2.

1.11 PSPF documentation indicates AGD's expectation that most entities will fluctuate between 'developing' and 'managing' maturity depending on their risk profile, threat environment and resources. The 'embedded' level described in Figure 1.1 is what entities are expected to implement, and requires all core and supporting requirements to be implemented and effectively integrated. AGD reports that entities need to make an individual judgment about whether striving for an 'embedded' maturity level is desirable, based on their risk environment and efficient and effective use of their resources.

1.12 The following are mandatory assessment and reporting responsibilities.

- NCEs must meet the four security outcomes set out in the Protective Security Policy Framework.[6]
- NCEs must annually assess and report the maturity of the entity's security capability.[7]

Whole-of-government maturity reports

1.13 As of March 2022, AGD has published two reports on whole-of-government PSPF maturity on its publicly available website. Table 1.1 summarises the number of entities that reported to AGD each year.

Table 1.1: AGD whole-of-government reports

Reporting year	Number of entities	Date of publication
2018–19	98 (100%)	15 January 2021
2019–20	97[a] (100%)	8 June 2021
2020–21	97 (100%)	Not yet published

[6] Attorney-General, *Directive on the Security of Government Business* [Internet], AGD, available from https://www.protectivesecurity.gov.au/about/security-government-business [accessed 2 May 2022].

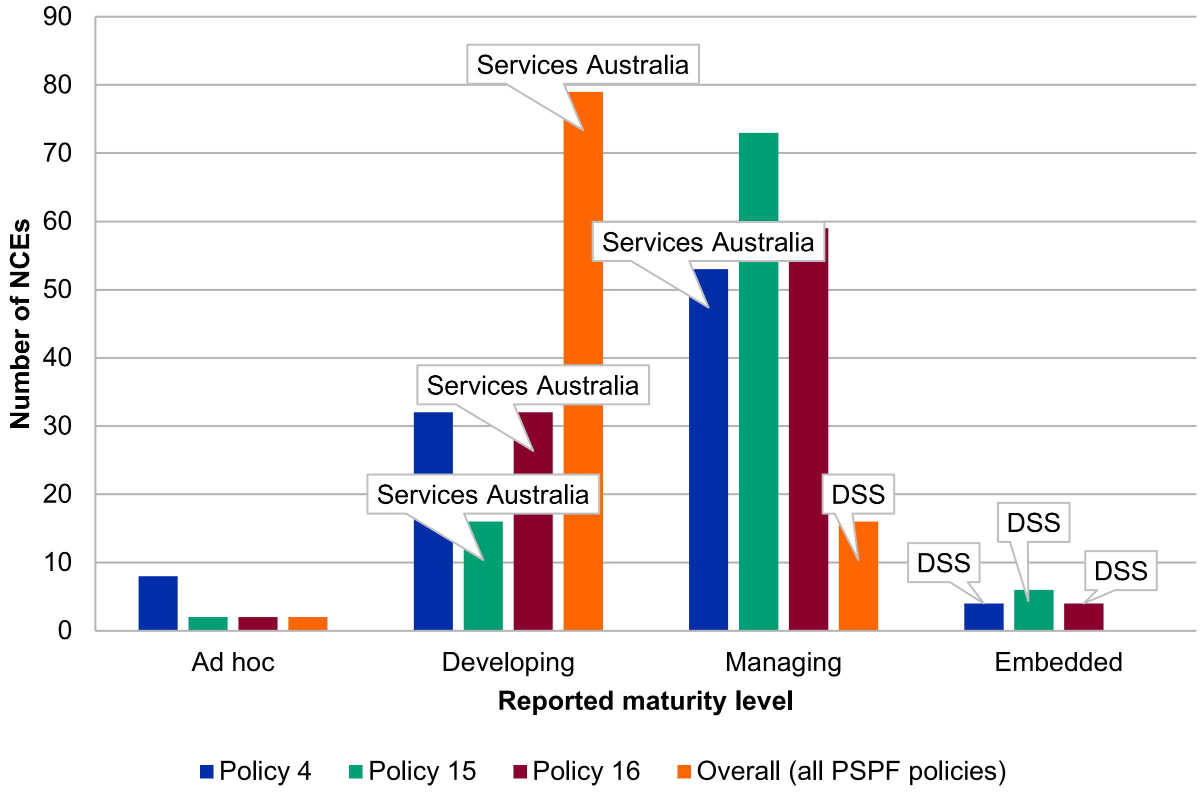
[7] Attorney-General's Department, *PSPF policy 5: Reporting on security*, [Internet], AGD, available from https://www.protectivesecurity.gov.au/publications-library/policy-5-reporting-security [accessed 2 May 2022].

Note a: The difference in the number of entities reporting in 2018–19 and later years is due to Machinery of Government changes in December 2019.

Source: ANAO based on AGD documentation.

1.14 Figure 1.2 illustrates the number of NCEs reporting each maturity level in 2020–21. The figure shows that DSS was in a minority of entities, self-assessing its maturity at the highest degree of implementation for physical security policies. Services Australia reported developing maturity, which was below most NCEs' maturity of 'managing' for physical security policies.

Figure 1.2: Reported physical security maturity among non-corporate Commonwealth entities in 2020–21



Source: ANAO based on PSPF maturity assessment reporting data 2020–21.

Rationale for undertaking the audit

1.15 Physical security arrangements underpin secure delivery of government business through the protection of people, information and physical assets. As Australian Government policy, the PSPF applies to all NCEs subject to the PGPA Act, with accountable authorities responsible for protective security arrangements within their own organisations.

1.16 As the policy owner, AGD has responsibility for whether the PSPF is successful. AGD undertakes its role through provision of general, high-level guidance to entities on the PSPF. AGD also collects and reports entities' annual self-assessments and information on significant security incidents.

1.17 The Auditor-General has tabled performance audits identifying a low level of oversight and low levels of entity compliance with mandatory policies. This audit will provide assurance about whether AGD is fostering the intended strong security culture through strategic, diligent, and risk-based administration of the PSPF, including by assessing the accuracy of self-reporting of physical policies by two entities.

Audit approach

Audit objective, criteria and scope

1.18 The audit approach was to assess the effectiveness of AGD's administration of physical security in the revised PSPF, including as well as compliance with physical security requirements by two entities (Department of Social Services and Services Australia). The ANAO used policy 4 (Security maturity monitoring), policy 15 (Physical security for entity resources) and policy 16 (Entity facilities) to assess this effectiveness.

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

- Has the Attorney-General's Department effectively administered the Australian Government's protective security policy framework?
- Are selected entities appropriately monitoring their security maturity and providing a safe and secure physical environment for their people, information and assets?

1.20 The audit did not include examination of the selected entities' compliance with the pre-October 2018 PSPF or policies 1 to 3 and 5 to 14.

Audit methodology

1.21 The audit involved:

- a review of departmental documentation held by AGD and the selected entities relating to the revised PSPF;
- analysis of entity reporting data collected by AGD from 2018–19 to 2020–21;
- meetings with relevant staff within AGD, selected entities' Chief Security Officers and other relevant entity staff;
- data analysis and observation of physical security measures at selected entities' facilities in the ACT and NSW; and
- a survey of Chief Security Officers from 97 NCEs.

1.22 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately $497,000.

1.23 The team members for this audit were Natalie Maras, Chay Kulatunge, Amanda Reynolds, Dale Todd, and Corinne Horton.

2. Effectiveness of the Attorney-General's Department's administration

Areas examined

This chapter examines the Attorney-General's Department's (AGD) administrative arrangements to support the revised Protective Security Policy Framework (PSPF).

Conclusion

AGD's administrative arrangements to support the revised PSPF were largely effective. AGD's advice to government about the progress of the framework was limited as AGD relied on self-assessment information, which the ANAO has found can be overstated or inaccurate, to accurately reflect the maturity of implementation of revised PSPF requirements. As policy owner, AGD did not monitor compliance with mandatory requirements. AGD provided a variety of support including detailed written guidance that could be better tailored to low-risk and face-to-face service environments. AGD's role can be strengthened by closer alignment of the self-assessment reporting instrument and policy, and by ensuring that entities understand and follow the mandated security reporting requirements.

Areas for improvement

The ANAO made one recommendation aimed at reconciling and collating significant security incident reporting. The ANAO also identified an opportunity to ensure alignment of the self-assessment questionnaire and PSPF policy requirements.

2.1 The *Public Governance Performance and Accountability Act 2013* (PGPA Act) requires entities to demonstrate how public resources have been applied to achieve their purposes.

2.2 The Attorney-General's Directive on the Security of Government Business establishes PSPF as an Australian Government policy.[8] The Attorney-General's Directive also reiterates the PGPA Act requirement for AGD, as policy owner of the PSPF, to develop and refine the policy.

2.3 The ANAO examined whether AGD:

- established fit-for-purpose governance arrangements to support its administration of the PSPF;
- collected information to effectively assess whether the policy objectives of the PSPF are being met; and
- effectively analysed information and reported to government on whether the policy objectives of the PSPF are being met.

[8] The Attorney-General issued the *Directive on the Security of Government Business* in October 2018 as part of updates to the Protective Security Policy Framework.

See Attorney-General, *Directive on the Security of Government Business* [Internet], AGD, available from https://www.protectivesecurity.gov.au/about/security-government-business [accessed 2 May 2022].

Has AGD established fit-for-purpose governance arrangements to support its administration of the PSPF?

AGD largely established fit-for-purpose governance arrangements to support its administration of the PSPF. AGD established governance bodies with defined roles, and it planned to manage risk, refine policies and engage with other entities. AGD did not establish a framework for defining the effectiveness of the revised PSPF. The risk framework has not identified all appropriate risks, including the risk of optimism bias in entities' self-assessments.

2.4 Sound governance arrangements enable a policy owner to put itself in the best position to report to government on the success or otherwise of its policy. Sound governance arrangements also assist a policy owner to build stakeholder and public confidence in the policy for which there is an expectation of compliance. The ANAO examined whether AGD put in place governance arrangements, and whether these supported the administration of the revised PSPF.

2.5 The Attorney-General's Directive from October 2018 stated:

> The Australian Government, through my department with oversight of the Government Security Committee, will continue to assess emerging security risks and develop and refine protective security policy that promotes efficient secure delivery of government business.[9]

2.6 AGD developed the PSPF Reforms Implementation Plan 2018 to support its implementation of the revised PSPF. This plan explained that the Attorney-General had portfolio responsibility for protective security and was the 'final decision maker on protective security policy matters.' The same plan indicated that the Government Security Committee (GSC) provided 'strategic oversight' of whole-of-government protective security policy and promoted the consistent, efficient and effective application of security policies by non-corporate Commonwealth entities (NCEs).

2.7 Under the Administrative Arrangements Orders[10], AGD is responsible for protective security policy.[11] As set out in AGD's Corporate Plans from 2018–22 to 2021–25, AGD's purpose included achieving 'a just and secure society through the maintenance and improvement of Australia's law, justice, security and integrity frameworks.'[12]

2.8 AGD achieved its purpose through five strategic priorities in 2018; six strategic priorities in 2019; and five key activities in 2020 and 2021. AGD positioned the revised PSPF under its strategic 'integrity' priorities in 2018 and 2019; and under its 'administration and implementation of programs and services' activities in 2020 and 2021.

[9] Attorney-General, *Directive on the Security of Government Business* [Internet], AGD, available from https://www.protectivesecurity.gov.au/about/security-government-business [accessed 2 May 2022].

[10] Administrative Arrangements Order 19 April 2018, Administrative Arrangements Order 29 May 2019, Administrative Arrangements Order 18 March 2021.

[11] AGD's responsibility has changed since 30 September 2015, when AGD was responsible for national security, protective security policy and co-ordination. See page 5 of Administrative Arrangements Order 30 September 2015, available at https://www.pmc.gov.au/sites/default/files/publications/AAO-30-September-2015.pdf [accessed 2 May 2022].

[12] Attorney-General's Department, *Corporate Plan 2018–22*, AGD, Canberra, 2018, p. 1.

2.9 According to its terms of reference, the GSC comprises 20 entity members[13], with additional entity representatives invited as needed.[14] AGD coordinated secretariat support for the GSC, which met as required by its terms of reference in the period October 2018 to December 2021.[15] The GSC provided strategic oversight of the PSPF by considering proposed updates to PSPF policies and instructing AGD to consult with other entities on specific matters. AGD informed the Attorney-General of agreed policy revisions and published updates.

Arrangements to assess outcomes of the revised PSPF

2.10 As outlined in paragraph 2.5, AGD's role in the PSPF is to assess emerging security risks and develop and refine protective security policy that promotes efficient secure delivery of government business. AGD did not develop a strategy to guide its assessment of whether the policy was successful in promoting efficient secure delivery of government business.

2.11 In response to ANAO queries about its reviews of the PSPF, AGD advised 'over the past 4 years, the PSPF has been the subject of a number of audits and reviews by the ANAO and Joint Committee of Public Accounts and Audit (JCPAA)'.[16] ANAO audits have found that the maturity levels for entities reviewed were below the required PSPF level of 'managing' and the reporting framework was not driving sufficient improvement in security. The JCPAA raised concerns about the level of entity compliance with mandatory requirements and the absence of internal assurance.

2.12 AGD's corporate plans outline AGD's strategic priorities that support the Attorney-General and assist the Minister. AGD measures the success of its strategic priorities using performance indicators outlined in its corporate plans. Business units are responsible for delivering on performance measures.

2.13 AGD's Corporate Plan 2018–22 and Corporate Plan 2019–22 included performance measures for the revised PSPF. These performance measures focussed on AGD producing community impact or achieving objectives through entities understanding and applying the PSPF.

2.14 In late 2020, AGD updated its performance reporting framework.[17] AGD consolidated its performance measures to focus assessment of policy work at the departmental level. AGD's

[13] Members of the Government Security Committee are: Attorney-General's Department, Australian Commission for Law Enforcement Integrity, Australian Criminal Intelligence Commission, Australian Cyber Security Centre, Australian Federal Police, Australian Public Service Commission, Australian Secret Intelligence Service, Australian Security Intelligence Organisation, Australian Signals Directorate, Bureau of Meteorology (from April 2021–December 2021), CSIRO (from April 2021–December 2021), Department of Defence, Department of Finance, Department of Foreign Affairs and Trade, Department of Home Affairs, Department of the Prime Minister and Cabinet, Digital Transformation Agency, National Archives of Australia, Office of the Australian Information Commissioner, and Office of National Intelligence.

[14] Entities that are co-opted for meetings are: Austrade, Department of Agriculture, Water and Environment, Department of Education, Skills and Employment, Department of Health, Department of Industry, Science, Energy and Resources, Department of Infrastructure, Regional Development and Cities, Department of Social Services, Department of Veteran's Affairs, nbn co, Services Australia, and Treasury.

[15] The GSC met four times in the calendar years 2018 and 2019, and three times in the calendar year 2020 in keeping with a decision by the GSC in December 2019 to change to three meetings per year.

[16] JCPAA, *Report 479: Australian Government Security Arrangements,* April 2019; and JCPAA, *Report 485: Cyber Resilience*, December 2020. Neither of these inquiries assessed the extent to which the implementation of the revised PSPF met objectives.

[17] In August 2019, following the review of the *PGPA Act 2013*, the Minister for Finance requested that the Auditor-General conduct a pilot program of audits of annual performance statements in consultation with the JCPAA. AGD was one of the three entities involved in the pilot program.

Corporate Plan 2020–24 and Corporate Plan 2021–25 no longer include specific performance measures for the PSPF.

2.15 The relevant performance measure for the PSPF in AGD's Corporate Plan 2021–25 is performance measure 3, relating to the legal and policy framework for which AGD has administrative responsibility. AGD's target relates to the average performance rating from stakeholders and the effectiveness of advice to the minister.

2.16 AGD advised that the Integrity and Security Division Protective Security Policy team delivers on AGD's performance measure for the PSPF, being a policy framework relating to criminal justice and national security. The team has a PSPF Quarterly Plan that indicates what will be done, how the team will work as a team, and high-level risks to delivery. The plan does not contain performance targets.

Arrangements to manage risk

2.17 AGD's corporate plans outline AGD's arrangements to manage risk. AGD's Chief Operating Officer is the Chief Risk Officer, accountable to AGD's Secretary for the implementation and maintenance of the department's risk management program. The Executive Board monitors the department's strategic risks, which are also considered as part of business planning, internal audit planning and budget allocation processes. Business units manage risks associated with the department's workforce, finances, infrastructure, and relationships with third parties.

2.18 The AGD protective security policy team managed risks relating to the PSPF through its PSPF Quarterly Plan and a risk register. This approach was consistent with AGD's Risk Management Policy and supporting departmental guidance and templates. AGD's risk register, dated 24 August 2021, reflected 10 risks for the revised PSPF, covering resourcing, access to and compromise of information or data management, and meeting expectations. Five of the 10 risks were rated as 'low' and five were rated as 'medium'.

2.19 AGD implemented treatments to address the risks it identified including:

- provision of a range of policy guidance and mechanisms for NCE feedback (website, PSPF hotline, email and communities of practice discussed in paragraphs 2.23 to 2.25);
- determining the exposure of the reporting portal to cyber-attacks by unauthorised internal and external users; and
- consistent resourcing of the PSPF team to support NCEs and other stakeholders.

2.20 The identified risks and treatments did not include the risk of optimism bias in a self-assessment framework or that entities may not accurately report self-assessment results. Previous ANAO performance audit reports[18] and the following chapters (three and four) indicate that this is a risk.

[18] See Auditor-General Report No.32 2020–21 *Cyber Security Strategies of Non-Corporate Commonwealth Entities*; Auditor-General Report No. 21 2020–21 *Delivery of Security Vetting Services Follow-up*; Auditor-General Report No.1 2019–20 *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*; Auditor-General Report No.53 *Cyber Resilience*; and Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*.

Arrangements to develop and refine protective security policy

2.21 AGD updated the PSPF policies when it identified the need to do so, when Government decisions or other policy changes affected the PSPF, or when requested by the GSC or other key stakeholders.

2.22 Since the revised PSPF commenced, AGD sought GSC approval of refinements to nine of the 16 policies. AGD obtained GSC approval for policy refinements at the second GSC meeting in 2019, 2020 and 2021. There were no refinements to the policies examined in this audit (policies 4, 15, and 16).

Arrangements for stakeholder support and engagement

PSPF website

2.23 The primary purpose of the PSPF website is to make the PSPF policies publicly available, including to NCEs.[19] The website provides public access to policies, guides, news, and updates, and provides links to templates, the reporting portal, and a webform for contact with AGD's PSPF team. AGD's Protective Security Policy team also manages a protective security policy community on GovTEAMS. Access to this community, which is restricted to government personnel, is available through completion of a form on AGD's website.

Direct engagement

2.24 AGD engaged directly with entities through its PSPF Hotline. AGD also responded to entity emails through the PSPF mailbox (group email account), which is linked through AGD's website contact form. PSPF Hotline and PSPF mailbox details were detailed in the Protective Security Guide for Chief Security Officers (CSO).

Forums and communities of practice

2.25 Since launch of the revised PSPF, AGD has established or leveraged existing forums to interact with public officials engaged in security matters across the sector. Stakeholder engagement in these forums and communities of practice raises awareness of PSPF requirements. By participating in these forums and communities, AGD was provided with access to insights about security culture in different entities, including issues of common concern, risk information, new and emerging threats, as well as access to products used to manage risks and address particular security concerns. Table 2.1 summarises AGD's main engagements.

[19] The website is https://www.protectivesecurity.gov.au.

The website also makes the PSPF policies publicly available to corporate Commonwealth entities and wholly owned Commonwealth companies under the PGPA Act, who apply the PSPF as better practice, and to non-government organisations and state and territory government agencies that may be required to apply the PSPF for certain information.

Table 2.1: AGD stakeholder forums and communities of practice 2019–2021

Forum/ Community of Practice	Purpose	2019	2020	2021
Personnel Security Community of Practice	Provide entities with an opportunity to increase their maturity level by discussing issues, engaging on common risk concerns, identify new and emerging threats, and access and share products that may assist to address particular security concerns.	February April May August September November[a]	N/A	N/A
Security Culture Community of Practice	Provide entities with an opportunity to increase their maturity level by discussing issues, engaging on common risk concerns, identify new and emerging threats, and access and share products that may assist to address particular security concerns.	March May September	Nil	Nil
Vetting Officers Community of Practice/Vetting Policy Forum	Provide entities with an opportunity to increase their maturity level by discussing issues, engaging on common risk concerns, identify new and emerging threats, and access and share products that may assist to address particular security concerns.	March May	July[b] October	May
Chief Security Officer (CSO) Forum	CSOs are the Australian Government's security custodians. This forum supports CSOs to implement the PSPF and foster a strong security culture in their entity.	May August November	Nil[c]	December
PSPF Reporting Forum	Support Commonwealth entities to complete and submit their annual security maturity self-assessment online, access benchmarking reports and report significant security incidents.	July August[d]	February June	March July
State and Territory Representatives Meetings	Discuss protective security issues in each jurisdiction with Commonwealth representatives and counterparts in New Zealand.	October	Nil	December

Note a: AGD disbanded the Personnel Security Community of Practice in November 2019.

Note b: In July 2020, the Vetting Officer Community of Practice was replaced by the Vetting Policy Forum.

Note c: During the pandemic, AGD issued CSO newsletters instead of holding forums.

Note d: The August reporting forum was only for CSOs to assist them in interpreting their entity's security maturity results.

Source: ANAO analysis.

Chief Security Officer satisfaction with AGD interactions

2.26 The ANAO conducted a survey of CSOs of the 97 NCEs who complete annual maturity assessments for the PSPF. A total of 39 (40 per cent) CSOs responded.

2.27 The ANAO's survey indicated that the majority of CSOs interact with AGD on a six-monthly or yearly basis for advice about the PSPF, mainly during peak reporting time. In addition:

- 90 per cent of CSOs were very satisfied or somewhat satisfied with AGD's responsiveness;
- 85 per cent of CSOs were very satisfied or somewhat satisfied with the clarity of AGD guidance material;
- 92 per cent of CSOs were very satisfied or somewhat satisfied with the comprehensiveness of AGD guidance; and
- 67 per cent of CSOs were satisfied that AGD understands their needs.

2.28 Less satisfied CSOs advised that AGD could improve the tailoring of advice. Some entity CSOs considered that AGD's 'one size fits all' approach to PSPF advice and guidance did not take proper account of the complexity of entity circumstances, or the compliance burden on small entities required to complete the annual questionnaire. Some entity CSOs considered that AGD guidance is not well-tailored to face-to-face service provision. Some entity CSOs noted that the face-to-face forums held by AGD were useful, however these forums ceased when the COVID-19 pandemic hit. Guidance on protecting people comprises three of 85 paragraphs in PSPF policy 15. The paragraphs in the PSPF guidance mainly refer to the *Work Health and Safety Act 2011* and recommend that entities implement appropriate physical security measures.

2.29 AGD advised that the PSPF has been deliberately drafted not to duplicate other government policies, and as such, refers to any relevant policies such as the *Work Health and Safety Act 2011* and provides additional and complementary protective security guidance where required. AGD also advised that specific guidance was developed and distributed to entities to support home-based work, adapting to the COVID-19 pandemic, and return-to-work arrangements.

Has AGD collected information to effectively assess whether the policy objectives of the PSPF are being met?

AGD collected annual entity self-assessments. In the context of indications that self-assessment information may not be accurate, including discrepancies in the reporting of significant security incidents, the use of self-assessment information to assess the effectiveness of the PSPF is limited.

2.30 Information collected by a policy owner assists in determining if the entities required to apply the policy are meeting requirements. Information collected can also assist a policy owner in determining whether contrary evidence exists where the policy owner relies on self-assertions by the entities. This section examines whether AGD collected the information it would need to effectively assess the success of the PSPF for which it is responsible.

Planning for collection of information

2.31 Before implementing the revised PSPF, AGD planned to collect self-assessment reports as the most effective and efficient way to provide assurance to government that effective protective security arrangements were in place. In proposing the self-assessment approach to the GSC in December 2017, AGD recognised that self-assessment is subjective. AGD also recognised that entities are in the best position to report on security risks impacting PSPF implementation because entities have the most comprehensive knowledge of their security risk environment.

2.32 AGD envisaged accountability checks on self-assessments in the form of approvals of entity reports from the entities' accountable authorities and ministers. AGD proposed to the GSC the following additional accountability measures:

- the model more expressly requires entities to demonstrate a cycle of security planning, monitoring, and reporting each year to meet outcomes;
- reporting includes an explanation of security risk context together with a summary of how key risks for entities were managed over the period; and
- the model will require supporting evidence to be provided to validate responses where appropriate.

2.33 The self-assessment questionnaire contains questions, including free text fields, for entities to summarise their risks, explain their management, and evidence. AGD has not undertaken actions to validate the responses provided by entities and is reliant on self-assessment information to 'assess emerging security risks' and 'refine protective security policy' as envisaged by the Attorney-General's Directive. As outlined in paragraph 2.11, ANAO audits have identified issues with the accuracy of entity reporting.

2.34 AGD advised that 'the PSPF does not require AGD to engage in any activities that would involve assessing, validating, or providing assurance of the reliability or accuracy of entity self-assessments'. In addition, it was not a function that the Australian Government had 'asked the department to perform'.

Self-assessment collection instrument

2.35 AGD collected self-assessed maturity ratings and comments from entities using a questionnaire-style instrument accessible through the PSPF online reporting portal or offline reporting template.[20] The questionnaire comprised 17 mandatory modules — one for each of the 16 PSPF policies and a summary module.

2.36 During meetings with the ANAO's survey respondents, two entities observed there was a mismatch between AGD's questionnaire and policy requirements.

2.37 The reporting questions for the revised PSPF were developed between 2017 and 2019 with input from workshops and working groups of representatives from up to 24 entities. The working groups were guided by the PSPF Reporting Reform Project Plan. On 6 June 2019, the GSC nominated a group of Senior Executive representatives from 15 entities to consider the assessment questions.[21] AGD was unable to produce any records of deliberations about specific language or alignment of assessment questions to policy language.

[20] Online reporting is for information up to PROTECTED. Offline reporting is for information classified higher than PROTECTED.

See Attorney-General's Department, *PSPF policy 5: Reporting on security*, [Internet], AGD, available from https://www.protectivesecurity.gov.au/publications-library/policy-5-reporting-security [accessed 2 May 2022].

[21] Representatives were from Australian Taxation Office, Australian Federal Police, Department of the Prime Minister and Cabinet, Home Affairs, Australian Security Intelligence Organisation, Reserve Bank of Australia, Department of Finance, Digital Transformation Agency, Office of the Australian Information Commissioner, Office of National Intelligence, National Archives of Australia, Department of Foreign Affairs and Trade, Defence, Australian Commission for Law Enforcement Integrity, and the Attorney-General's Department.

2.38 AGD advised that it has not changed questionnaire questions for policies 4, 15, and 16 since the working group formed these questions in 2019. Further, to preserve the baseline for year-to-year comparison, AGD preferred not to change assessment questions. AGD also considered there was no need for AGD to map questionnaire questions to the PSPF policy requirements because AGD's reporting portal survey confirmed for AGD that 88 per cent of 484 respondents were satisfied that questions clearly aligned with policy requirements.

2.39 The ANAO compared core requirements in PSPF policy 4, 15 and 16 with the equivalent questions in AGD's 2019–20 questionnaire. The comparison showed 49 inconsistencies between requirements expressed in both documents, 23 of which could be construed to materially overstate, understate, or omit policy requirements.

2.40 The ANAO suggests that AGD undertake a review of questions in the questionnaire instrument that have not already been amended by the GSC, to ensure that results collected with the instrument align with all aspects and the intent of each policy.

Collection of significant security incident reports

2.41 Since 1 October 2018, the PSPF has required entities to report significant[22] or reportable security incidents to the relevant lead security authority and other affected entities at the time they occur. Entities are also required to complete the Australian Signals Directorate's annual cyber security survey.

2.42 AGD guidance provides:

> Information gathered on significant security incidents assists the Attorney-General's Department to:
>
> a. determine the adequacy of protective security policies
>
> b. provide an insight into entity security culture
>
> c. identify potential vulnerabilities in government security awareness training to inform whole-of-government security outreach activities.[23]

2.43 Significant security incidents can be reported to AGD through the PSPF Reporting Portal, by email, or by telephone to the PSPF Hotline. AGD advised the ANAO that significant security incidents can also be reported 'where appropriate, via a classified system' although this is not described in the guidance material.

2.44 Since 2019, AGD has maintained a log of significant security incidents that have been reported. The log captures 14 significant security incidents reported to AGD between 2019 and 2021.[24] ANAO analysis of NCE self-assessment reports shows that entities experienced

[22] According to PSPF policy 5, C.2.1, paragraph 41, a significant security incident is:

> a deliberate, negligent or reckless action that leads, or could lead to, the loss, damage, compromise, corruption or disclosure of official resources. A significant security incident can have wide-ranging and critical consequences for the entity and the Australian Government.

See Attorney-General's Department, *PSPF policy 5: Reporting on security*, [Internet], AGD, available from https://www.protectivesecurity.gov.au/publications-library/policy-5-reporting-security [accessed 2 May 2022].

[23] PSPF policy 5, C.2.1.1, paragraph 43.

[24] It does not include 61 significant security incidents that occurred during 2019–20 but were not reported through the PSPF reporting portal.

more significant security incidents than are captured in AGD's log, and the log does not contain all incidents that were reported to AGD. One entity reported in its self-assessment that it had experienced 42 significant security incidents that it did not report to AGD. Another entity did not report to AGD because it considered the portal inappropriately security classified.

2.45 In July 2021, AGD reminded entities of the requirement to report significant security incidents. AGD updated guidance material on significant security incident reporting on 21 April 2020; and updated the significant security incident reporting template on 8 June 2021.

2.46 AGD can receive reporting on significant security incidents from a variety of sources as outlined previously, however, this information is not collated within its log of significant security incidents. This limits AGD's ability to meet it intended role as outlined in its guidance for 'Policy 5, Reporting on Security'. Reviewing and reconciling security incident reporting data would better inform AGD's assessments of whether PSPF guidance has been effective in supporting entities to protect their people, information, and assets.

Recommendation no. 1

2.47 The Attorney-General's Department review, reconcile and collate all significant security incident reporting data to inform assessments of whether the PSPF adequately supports entities to protect their people, information, and assets.

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

2.48 *The Attorney-General's Department agrees to strengthen the approach to security incident reporting. The department reviews the data it collects from significant security incident reports it receives in accordance with PSPF policy 5: Reporting on security. The department uses that data to identify lessons learned and consider improvements to the PSPF. The department will undertake further outreach and awareness-building activities with entities and increase whole-of-government visibility of security incident reports to drive continuous improvement across the system. Implementation of this recommendation will build on recent departmental initiatives to improve security incident reporting which included regularly advising entities of their obligations, providing advice and transitioning to an online reporting tool. The new reporting tool streamlines reporting for entities, ensures the reporting entity has met their reporting and referral obligations, and provides a uniform data source to improve analysis by the department and inform updates to the PSPF.*

Has AGD effectively analysed information and reported to government and the public on whether the policy objectives of the PSPF are being met?

AGD was effective in analysing completeness of responses. AGD did not collect information to provide assurance over the self-assessment responses provided by entities. Reports to government and the public on the Australian Government's security culture and maturity were solely based on entity self-assessments. This reduces the level of assurance AGD has on its advice on whether the policy objectives of the PSPF are being met.

2.49 Appropriate analysis of relevant information enables a policy owner to provide evidence-based advice to the Australian Government and the public on the extent to which its policy is achieving the desired outcome. This section examines whether AGD's reports to government and the public were supported by effective analysis.

Analysis of information

2.50 As discussed in paragraphs 2.31 and 2.32, AGD did not collect information to analyse accuracy or provide assurance over self-assessment information. Consistent with its self-assessment approach, AGD accepted information from entities as true and correct at the time of submission.

2.51 AGD reviews the completeness of responses and if it finds missing information, returns the incomplete submissions to NCEs for completion. The reporting portal captured information about AGD's reasons for returned submissions. Commonly missing information for which AGD returned submissions included the APS level of the submitting CSO, incomplete modules, missing rationales, missing strategies for improving 'ad hoc' or 'developing' modules, unspecified timeframes, or undefined key risks. Table 2.2 summarises the number of incomplete self-assessments that AGD returned for completion.

Table 2.2: Number of submissions returned by AGD for completion by NCEs

2018–19	2019–20	2020–21
78 of 98 (80%)	45 of 97 (46%)	8 of 97 (8%)

Source: ANAO based on AGD documentation.

2.52 AGD invited entities to complete several free text fields in their annual self-assessment reports. These fields captured the entities' rationale for its self-assessed maturity rating, issues, and strategies to improve their treatment of risks as well as summary comments. Consistent with its advice that 'AGD did not collect information with any intention to provide assurance over self-assessment information', the ANAO was unable to identify analysis of free text fields. AGD advised the ANAO:

> It is not correct to say that AGD does not intend to analyse information. AGD intends to, and does, analyse the information provided by entities, including in the free text fields, to identify the common reasons for low maturity, blockers to improving maturity, and key risks.[25]

2.53 The ANAO analysed free text fields in 2020–21 self-assessment reports for 97 entities. The analysis showed that regardless of size or function, NCEs considered cyber threats in their top two threats. Besides cyber, the analysis of free text fields showed stratification of themes by NCE size and function. Larger entities considered foreign interference among their top threats whereas medium NCEs rated malicious motivated individuals or groups in their top threats; and small NCEs rated unauthorised access or disclosure of information in their top threats. By function, regulatory NCEs rated their transition to remote or working from home arrangements as a top threat; smaller operational NCEs rated staff understanding of compliance with security requirements as a top threat; and policy NCEs rated foreign interference as a top threat.

[25] AGD advice to the ANAO, 12 January 2022.

Public reports

2.54 Three years after the implementation of the revised PSPF, AGD has had an opportunity to compare three years of self-assessment information and consider whether the revised PSPF was meeting objectives. As outlined in Table 1.1 in Chapter 1, AGD has publicly reported twice on the revised PSPF.

2.55 Before AGD had multiple year results to compare, AGD had reported in relation to the revised PSPF:

> The results are promising. Most entities have substantially implemented the core and supporting requirements of the Protective Security Policy Framework. Entities are actively engaged with risk and have a strong understanding of their threat environments. They demonstrate a commitment to improving the security of their information, as well as their people and assets.[26]

2.56 AGD's public reports collated NCE maturity status information from the annual questionnaires and present summary graphs of maturity for each of the 16 policies. The reports refer to the work of other entities, such as the Australian Signals Directorate's Australian Cyber Security Centre, in identifying threats. The reports did not refer to any work that AGD did to identify emerging security risks.

2.57 AGD's 2018–19 report concluded:

> While some entities require additional supports, these results demonstrate that entities are working to continually improve their security posture, and demonstrate a sound understanding of the threat environment in which they operate.[27]

2.58 AGD's 2019–20 report concluded:

> Entities are building resilience, adapting to the rapidly changing environment in which they operate, and continually working to improve their security posture by prioritising efforts to target areas of low security maturity.[28]

2.59 In publishing the 2019–20 report on 8 June 2021, AGD noted that 'entities reported improvement across all four security outcomes and the majority of entities (99 per cent) reported they had substantially implemented the core and supporting PSPF requirements, up from 89 per cent in 2018–19.' AGD noted that the 2019–20 report 'provides assurance to government and the Australian public that entities are implementing security measures that proportionately address their unique security risk environments.'

2.60 The public reports did not contain any explicit statement to indicate that information is based only on self-assessment information and AGD had not independently verified that entities are building resilience, adapting, and continually working to improve their security posture. By comparison, the publicly available Commonwealth Security Posture Report (produced by the

[26] Attorney-General's Department, *Release of the PSPF 2018–19 whole-of-government maturity report* [Internet], AGD, 15 January 2021, available from https://www.protectivesecurity.gov.au/news/release-pspf-2018-19-whole-government-maturity-report [accessed 2 May 2022].

[27] Attorney-General's Department, *PSPF 2018-19 consolidated maturity report* [Internet], AGD, 15 January 2021, available from https://www.protectivesecurity.gov.au/system/files/2021-06/pspf-maturity-report-2018-19.pdf [accessed 2 May 2022], p. 6.

[28] Attorney-General's Department, *PSPF 2019–20 consolidated maturity report* [Internet], AGD, 8 June 2021, available at https://www.protectivesecurity.gov.au/system/files/2021-06/pspf_2019-20_consolidated_maturity_report.pdf [accessed 2 May 2022], p. 11.

Australian Signals Directorate[29]), which refers to the AGD maturity data for policy 10, stated that some 'information in the report is self-reported and has not been independently verified'.

2.61 In response to the ANAO's queries about the transparency of AGD's reliance on self-assessment reports, AGD advised the ANAO in February 2022 that:

> The department has never suggested that the self-assessments are independently verified. On the contrary, the 2019–20 PSPF assessment report explicitly stated it was based on consolidated entity self-assessments. Similarly, the department's ministerial submission that sought approval to publish the 2019–20 assessment report stated that the department used the self-assessments submitted by entities to prepare the report.

Reporting to Government

2.62 AGD reported to the Attorney-General, seeking ministerial approval for GSC-approved updates to the PSPF and annual reports prior to publication on the PSPF website.

2.63 AGD's advice to the Attorney-General that security maturity is improving was based exclusively on self-assessment reports of entities. AGD did not use other public information (such as NCE corporate information or media), or information from its engagements with stakeholders to make evidence-based reports to the Attorney-General about the sufficiency of the mandatory reporting framework in meeting the objectives of the PSPF.

2.64 On 18 September 2020, AGD advised the Attorney-General that it had developed minor and technical amendments to six of the 16 PSPF core and supporting requirements and guidelines to respond to emerging security risks. The advice did not elaborate on what the emerging security risks were; how emerging security risks were identified; or how the amendments responded to identified risks.

2.65 While seeking the Attorney-General's approval to publish the 2018–19 PSPF assessment report on the PSPF website, on 3 December 2020 AGD summarised the consolidated view of protective security self-assessments. AGD advised that its 'experience with the 2018–19 report has indicated it would be desirable to make further refinements to the maturity model to better represent progress by entities and the achievement of substantial maturity.' AGD stated 'we will undertake that work now'. AGD also advised that it is working with the Australian Security Intelligence Organisation and the Australian Cyber Security Centre (ACSC) to develop and implement strategies to assist entities to improve security maturity results, including:

- biannual briefings on the threat environment;
- sharing PSPF results on cyber security requirements with ACSC; and
- policy and implementation advice and assistance offered to entities that self-assessed as 'ad hoc'.

2.66 On 24 May 2021, AGD reported to the Attorney-General that 'there was a clear increase in security maturity during 2019–20' and '[e]ntities achieved improvements in their level of implementation'. AGD expected that entities 'will continue to improve their maturity year-on-year'. These statements repeat publicly available summaries of self-assessment reports. AGD also noted that with two years of reporting data available to it, the department was 'considering whether the

[29] Australian Signals Directorate, *The Commonwealth Cyber Security Posture Report in 2020,* ASD, Canberra, 2021.

PSPF maturity model meets its purpose and whether any enhancement could be made to improve the model.'

Improvements to assurance of self-reporting data

2.67 In March 2021, AGD commenced a procurement process for evaluation services addressing how the PSPF maturity model could be improved. The evaluation did not address the whole PSPF framework and was not intended to determine if alternatives to the self-assessment model should be implemented.

2.68 The evaluation report was delivered in June 2021. To improve the model's design, the report made 16 recommendations including for self-assessment accuracy; guidance, education, and support; and reporting process and reporting outputs. AGD advised the Attorney-General that findings will inform updates for the 2020–21 PSPF reporting period.

2.69 AGD responded to the report's recommendations by taking to the GSC proposals for changes to self-assessment reporting, guidance, peer support and external moderation. Minutes from the 20 July 2021 meeting of the GSC record that AGD was working on updates to the reporting portal. The GSC noted AGD's proposal to formalise the assurance arrangements undertaken by entities with 'an additional question about the accuracy of the self-assessment.' On 24 November 2021, the GSC agreed to the following action items for AGD, without accompanying timeframes.

- AGD to update the PSPF maturity model, including changing the calculation methodology, a review of the yes or no questions, and updating maturity level descriptors.
- AGD to progress work on a new starter guide to reporting, and Best Practice Evidence Guide to support entities in improving the accuracy of their self-assessments.
- AGD to develop an opt-in peer review option to support information sharing and explore a pressure testing framework.

3. Department of Social Services' security maturity monitoring and provision of a secure physical environment

Areas examined

This chapter examines whether the Department of Social Services (DSS) has implemented the requirements for security maturity monitoring, physical security measures for entities and protective security measures at its facilities under the revised Protective Security Policy Framework (PSPF).

Conclusion

DSS was largely effective in implementing requirements that it established for itself under the PSPF at the 'managing' and 'embedded' maturity levels. DSS implemented a variety of physical security measures and integrated physical security considerations into its processes. DSS did not accurately report its maturity level as 'embedded' for policies 4, 15 and 16 because it did not always follow its plan, and documentary evidence of the certification authority's satisfaction with physical security requirements was incomplete.

Areas for improvement

The ANAO made two recommendations aimed at adherence to plans for assessing and reporting progress against indicators set in the security plan; and completion of certification and accreditation and documentation in accordance with core requirements of the PSPF.

The ANAO made two suggestions aimed at consistently documenting responsibilities for implementing the PSPF at co-location sites; and using a broader variety of performance data to evidence its assessments of risk culture.

3.1 The PSPF requires entities to comply with physical security requirements in policy 4 (security maturity monitoring), policy 15 (physical security for entity resources) and policy 16 (entity facilities).

3.2 To assess whether DSS met requirements, the ANAO examined whether:

- assessments of security capability and risk culture were aligned with security plans and demonstrated routine consideration of progress against set goals;
- risks were assessed and physical security measures were selected and implemented at facilities visited by the ANAO; and
- protective security was fully integrated into planning, selection, modification and design of facilities and certifications and accreditations were undertaken.

Did DSS effectively implement security maturity monitoring at the 'managing' and 'embedded' maturity level?

DSS was largely effective at considering its progress against the goals and strategic objectives in its security plans. DSS had established a plan with goals and objectives and monitoring bodies received reports about security capability and risk culture. DSS' reported maturity levels were inaccurate because monitoring was not consistently against the indicators in the security plan and did not cover co-location sites. DSS captured and analysed performance data and used a limited range of performance data to inform change.

3.3 The PSPF policy 4 core requirement is that each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan. The entity should set indicators in its entity security plan against which to evidence and document its assessment. The supporting requirement of this policy is that entities document and evidence their assessment of the entity's security maturity. Monitoring security maturity is an ongoing process that involves routine assessment of security capability and risk culture against set indicators.

3.4 In 2018–19, DSS reported in its PSPF self-assessment that it had a maturity level of 'managing'. At this maturity level, the entity's implementation of policy 4 should demonstrate a consistent and defined approach to monitoring the entity's security performance which is tailored to the entity's risk environment. The entity should have clearly defined its security goals and objectives in the security plan, and performance should be tracked and measured to assess security capability and risk culture maturity.

3.5 In 2019–20 and 2020–21, DSS reported that it had reached an 'embedded' maturity level. This maturity level means that the entity actively engages in ongoing monitoring and improvement of security capability and culture through long-term planning to predict and prepare for security challenges. It also means that performance data is captured, analysed, and informs change.

3.6 The ANAO examined DSS' security plans, documentation, and evidence of its implementation of policy 4, including its assessments of security capability and risk culture maturity, at the reported levels. Table 3.1 outlines findings for policy 4.

Table 3.1: DSS' implementation of policy 4

Policy requirement	ANAO assessment	ANAO comment
Assess the maturity of security capability against the goals and strategic objectives identified in its security plan.	▲	In 2018–19 DSS undertook assessments. Assessments were not against goals and objectives in its security plan.
	▲	In 2019–20 and 2020–21 DSS' assessments were not always tracked against its security goals and indicators. The frequency of DSS' consideration of its progress was inconsistent.
Assess the maturity of risk culture by considering its progress against the goals and strategic objectives identified in its security plan.	▲	In 2018–19 DSS assessed its risk culture. Its assessments were not clearly linked to the security plan, making it difficult for DSS to show that it considered its progress against the goals and strategic objectives in its security plan.
	▲	In 2019–20 and 2020–21 DSS developed an enterprise-wide Threat and Vulnerability Risk Assessment to predict and prepare for security challenges. Its monitoring was not aligned to the security plan and infrequent.

Key: ◆ Appropriately implemented. ▲ Partly implemented. 🟥 Not implemented.

Source: ANAO analysis of DSS activities.

Monitoring of security capability and risk culture in 2018–19

3.7 DSS had a Security Plan 2018–2020 that was not finalised. In this plan, DSS clearly defined security goals for the period between 1 July 2018 and 30 June 2019. Security goals address both DSS' security capability and risk culture. The Security Plan 2018–2020 also contained key actions and measures of success for each goal.

3.8 DSS' Security Plan 2018–2020 did not include internal audits as part of its monitoring activities. DSS undertook an internal audit on its compliance with the PSPF between October 2018 and April 2019. The internal audit found that for PSPF policy 4, DSS was achieving a 'developing' maturity level because it had not undertaken an annual security capability and enterprise-wide security risk assessment as stated in its Security Plan 2018–2020.

3.9 DSS upgraded its self-assessment to 'managing' based on enhancements to its security governance by appointing a Deputy Secretary CSO, incorporating security policies and guidelines into procurement processes, and implementing a designated assessment register. DSS had agreed to the recommendation in the internal audit — that the Security Plan should form the basis for DSS' security reporting framework — and it was implemented in the Security Plan 2019–21. An accurate self-assessment would have been for DSS to maintain the 'developing' maturity level until it had implemented the recommendation, rather than when it had agreed to the recommendation. As such, DSS' self-assessment was inflated and unsubstantiated at the 'managing' level for 2018–19.

3.10 DSS established a Security Working Group (SWG)[30] to monitor the strategic direction and execution of all DSS' security functions to ensure that security risks to its people, information and resources are managed effectively. DSS planned for the SWG to meet monthly. The SWG received two reports to monitor its security capability and risk culture. These were:

- monthly reports which covered security capability and risk culture related topics, including preparation of an annual enterprise-wide security risk assessment, conduct of protective security reviews for facilities and risk training for the DSS security team; and
- occasional Security Action Plan updates, which recorded the progress of security activities.

3.11 The SWG meetings and monthly reports did not occur monthly as intended. This was partly due to SWG transitioning to the Implementation Committee from December 2018. The Implementation Committee is an advisory body that reports to the Secretary through the Executive Management Group.[31] Overall, monitoring activities and reports were available for most of the year, except for May and June 2019.

3.12 The activities addressed in monthly reports did not explicitly align to DSS' security goals, and monthly reports did not comment on DSS' overall progress, making it difficult for DSS to substantiate that its assessments of security maturity related to its security plan. SWG meetings included discussion of security activities. These meetings did not directly cover the key actions and measures of success from the Security Plan 2018–2020.

[30] SWG members included senior executive level branch managers from Security and Business Continuity, IT operations, Assurance and Performance, and Organisation Strategy Services. SWG advisors included the Agency Security Advisor and IT Security Advisor.

[31] The Executive Management Group (EMG) is DSS' most senior governance committee. It provides the department with guidance, including guidance on monitoring performance and risks, and ensuring accountability and regulatory requirements are met.

Monitoring of security capability and risk culture in 2019–20 and 2020–21

3.13 In its Security Plan 2019–21, DSS defined its strategic objective to: 'protect our people, information, and assets so that the department is able to deliver on our mission to improve the wellbeing of individuals and families in Australian communities'. DSS clearly defined its security goals, which aligned to the four security outcome themes of the PSPF.[32] As shown in Table 3.2, DSS' key performance indicators address monitoring and assessment for both security capability and risk culture.

Table 3.2: Security goals, key actions and performance indicators related to security capability for 2019–20 and 2020–21

Security goal	Key actions	Key performance indicators
Governance — Manage security risks and support 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.	Bi-annually review and update the Security Plan and associated Security Risk Assessment for the Secretary's approval.	The Security Plan, Security Risk Assessment, and associated security risk mitigations are approved by the Secretary.
	Monitor our performance against the actions identified in the Security Plan through the Implementation Committee and Executive Management Group on a quarterly basis.	Security performance reported quarterly to Implementation Committee.
		Improvements in compliance with security requirements noted between reporting periods.
	Performance reporting includes number of security incidents and staff participation in mandatory annual security training (at departmental, stream and group levels).	100% of staff complete the security awareness training by 30 June 2020 and 2021.
Physical security — Provide a safe and secure physical environment for our people, information and assets.	Undertake bi-annual Threat and Vulnerability Assessments (T&VA) and Security Zone Assessments for all facilities.	All facilities are certified in accordance with Physical Security Guidelines contained in the PSPF.
		Risks identified through T&VA are mitigated to as low as possible in accordance with security risk tolerance.
	Undertake a rolling six-month security asset audit and maintenance program	100% of security assets are sighted.
		100% of assets in use are certified as compliant with Security Construction Equipment Committee (SCEC) requirements.[a]
	Develop and implement risk assessment policies and procedures for staff travelling off-site for work, or working in high-risk environments (remote	100% of staff are briefed and familiar with standard operating procedures on working in high-risk environments.

[32] The four security outcome themes are governance, information (including ICT), personnel, and physical. Attorney-General's Department, *PSPF policy 5: Reporting on security*, [Internet], AGD, available from https://www.protectivesecurity.gov.au/publications-library/policy-5-reporting-security [accessed 2 May 2022], paragraph 11.

Security goal	Key actions	Key performance indicators
	communities, service providers, hostile or highly political community environments).	

Source: DSS Security Plan 2019–21.

3.14 At DSS' self-reported 'embedded' maturity level, DSS should have actively engaged in ongoing monitoring and improvement of security capability and risk culture through long-term planning to predict and prepare for security challenges. DSS engaged in long-term planning to predict and prepare for security challenges when it developed an enterprise-wide Threat and Vulnerability Risk Assessment as part of its Security Plan 2019–21 (discussed at paragraphs 3.29 and 3.30). It identified risks, included risk analysis and considered risk mitigation measures.

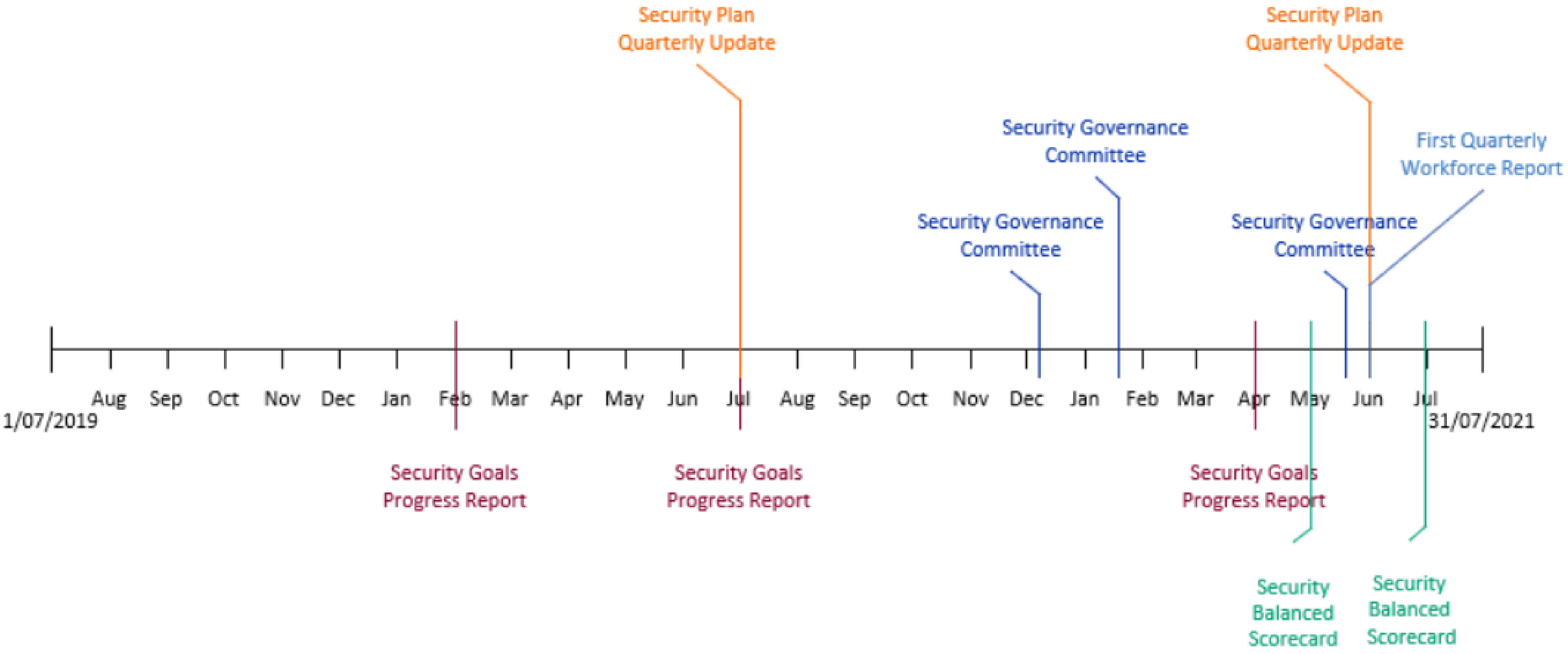
3.15 DSS did not always monitor its security capability and risk culture against the key actions and measures of success that it established in its Security Plan 2019–21 (shown in Table 3.2). DSS prepared four types of security reports to document its assessments. One of these (Security Goal Progress Report) was explicitly structured to align with the indicators from the Security Plan 2019–21. The reports covered general progress for activities related to governance and physical security:

- Security Goals Progress Reports — provided commentary on the implementation status of key performance indicators from the security plan;
- Security Balanced Scorecards — tracked the status and trends of DSS' maturity levels against each PSPF policies. It reported on key activities conducted under each security goal. The Security Balanced Scorecards had a more succinct reporting format compared to the Security Goals Progress Reports;
- Quarterly Workforce Report — included a security component, which covered security incidents, clear desk inspections, key security projects underway, status of staff security clearances, and status of zone certifications; and
- Security Plan Quarterly Updates — covered updates on the implementation of some of the measures outlined in the Security Plan.

3.16 In November 2020, DSS established the Security Governance Committee to monitor DSS' performance against the security plan and updated risk and vulnerability assessments. Minutes indicate that the committee discussed items such as progress against elements of the DSS Security Plan 2019–21, trends in security maturity and security reports. During 2020–21, DSS regularly monitored its Threat and Vulnerability Risk Assessment at meetings of the Security Governance Committee and through some of DSS' security reports.

3.17 DSS' monitoring activities over 2019–20 and 2020–21 is shown at Figure 3.1. The Security Governance Committee did not meet quarterly as planned and DSS' Security Plan Quarterly Update was not prepared quarterly. During 2019–20, one Security Goal Progress Report was prepared, and the Security Working Group and its successor the Security Governance Committee did not meet during 2019–20. In 2020–21, DSS' monitoring activities were concentrated towards the second half of the year. The infrequency and gaps in DSS' monitoring make it difficult for DSS to substantiate that it was actively engaged in ongoing monitoring.

Figure 3.1: DSS' monitoring of security maturity in 2019–20 and 2020–21


Security Plan Quarterly Update
Security Plan Quarterly Update
Security Governance Committee
First Quarterly Workforce Report
Security Governance Committee
Security Governance Committee
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
1/07/2019
31/07/2021
Security Goals Progress Report
Security Goals Progress Report
Security Goals Progress Report
Security Balanced Scorecard
Security Balanced Scorecard

Source: ANAO analysis based on DSS documentation.

Recommendation no. 2

3.18 The Department of Social Services review and adhere to its planned schedules for assessment and reporting of progress against actions and measures of success in the department's security plan.

Department of Social Services response: *Agreed.*

3.19 The department has revised its assessment and reporting documentation to clearly demonstrate progress directly against the measures of success contained in the department's security plan. The department is committed to adhering to governance and oversight arrangements established in the security plan as a key mechanism for strengthening performance monitoring, reporting and continual improvement.

3.20 Maturity of security capability considers how holistically and effectively each entity implements and meets the intent of the PSPF requirements. In DSS' circumstances 'holistic' consideration needs to incorporate DSS' 16 co-location sites in operation since 1 October 2018.[33] Co-location arrangements are captured in Memoranda of Understanding (MOUs) or shared premises guides. The ANAO examined 10 MOUs and shared premises guide documentation. The ANAO found that MOU documents did not consistently address physical security. DSS relied on the host agency to implement the requirements of the PSPF. Analysis also found DSS placed inconsistent responsibilities on host agencies to report on or provide assurance on PSPF implementation.

3.21 To enable DSS to better substantiate its self-assessed maturity level of 'embedded', the ANAO suggests that DSS consistently document responsibilities (including assurance activities and reporting), for the PSPF at all its co-location sites.

3.22 When an entity reports that it 'excelled' at its implementation of policy 4, it is expected that the entity captured and analysed performance data to inform change. DSS captured performance data for only mandatory staff security awareness participation and clear desk compliance in 2019–20 and 2020–21. DSS has systems in place to capture data for swipe card usage, visitor escorting, document classification and destruction, but did not use that data to inform change. The ANAO suggests that DSS use a broader variety of performance data to evidence its assessments of risk culture at the embedded level.

Did DSS implement mandatory physical security measures for its resources, at the 'managing' and 'embedded' maturity levels?

DSS was largely effective at implementing physical security measures for its resources. DSS considered security risks at the enterprise level against its Security Plan 2019–21, as well as specific risk mitigation measures. DSS' reported maturity levels were not accurate because it adopted controls with less assurance where it could not undertake physical site inspections. DSS

[33] DSS advised that when its staff co-locates with the host agency, staff may share an open floor space with non-DSS staff members, or there may be a wall separating DSS staff from non-DSS staff.

did not document its rationale for departing from the control in its Security Plan 2019–21, and it did not document the outcomes of its substitute processes.

3.23 Policy 15 describes the physical protections required to safeguard people (consistent with the requirements of the *Work Health and Safety Act 2011*), information and assets (including ICT equipment) to minimise or remove security risk. The core requirement of policy 15 is that each entity must implement physical security measures that minimise or remove the risk of harm to people, and information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

3.24 In 2018–19, DSS reported in its PSPF self-assessment that it had a maturity level of 'managing'. At this maturity level entities are expected to apply physical security measures that minimise or remove the risk of resources being made inoperable, inaccessible, accessed or removed without proper authorisation in accordance with requirements. It also requires that risks to the compromise of resources are mitigated to a level consistent with entity risk tolerance levels, in accordance with the entity's security plan.

3.25 In 2019–20 and 2020–21, DSS reported that it had reached an 'embedded' maturity level. To substantiate this maturity level, entities are required to apply physical security measures at the 'managing' level, as well as apply better practice guidance to minimise or remove risks. These measures are to be proportionate to the level of risk and scalable to changes in the threat environment.

3.26 The ANAO examined DSS' security plans and documentation and evidence of its implementation of physical security measures at the reported maturity level. The ANAO conducted site visits at three selected DSS facilities. Table 3.3 shows findings for these sites for policy 15.

Table 3.3: DSS' implementation of policy 15

Policy requirement	ANAO assessment	ANAO comment
Implement physical security measures that minimise or remove the risk of harm to people, and information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without proper authorisation.	▲	In 2018–19 DSS considered security risks at all sites selected for review by the ANAO. For two of the three selected sites, risk assessments concluded that security controls in place were 'effective' or 'partially effective' and a remediation program was put in place to address identified gaps or deficiencies. DSS did not identify specific physical security measures for enterprise-wide risks in its Security Plan 2018–2020.
	▲	In the 2019–20 and 2020–21 reporting periods, DSS' also considered security risks at the enterprise level, this time against its Security Plan 2019–21, as well as specific risk mitigation measures. DSS did not undertake its regular documented risk assessments for its facilities during this period. DSS implemented all except one of the physical security measures that were identified in its Security Plan 2019–21.

Key: ◆ Appropriately implemented. ▲ Partly implemented. 🟥 Not implemented.

Source: ANAO analysis of DSS activities.

DSS' assessment of security risks and selection of appropriate physical security measures

DSS enterprise-level risk assessment and selection of measures

3.27 During 2018–19, in accordance with its Security Plan 2018–2020, DSS was to review the enterprise-wide security risk assessment. DSS did not do this. The Security Plan did not specify measures to address the physical security risk that was identified in the plan.

3.28 In August 2018, in response to changes in its security risk environment, DSS commenced a risk assessment for when the Department of Health's grants administration function transitioned into DSS. Almost 270 transitioning staff from the Department of Health required access to DSS sites. The risk assessment identified eight security risks and three risks of harm to people. The risk assessment documented DSS' risk analysis, risk evaluation, risk treatments and the status of each risk.

3.29 For 2019–21 and 2020–21, DSS identified measures in an enterprise-wide Threat and Vulnerability Risk Assessment that was attached to its DSS Security Plan 2019–21. These are outlined at Table 3.4. This risk assessment clearly identified risks, included risk analysis, and considered risk mitigation measures.

3.30 In 2019–2020, in response to changes in its security risk environment, a review of the Threat and Vulnerability Risk Assessment was conducted to reflect a potential increased risk to staff working in the National Redress Scheme and Cashless Debit Card teams. DSS updated its Security Plan to include an additional risk source and treatment (see Table 3.4). In September 2020, the Secretary noted the review and that the overall risk to DSS remained 'low'.

Table 3.4: Enterprise-wide risks and selected mitigation measures in the Security Plan 2019–21

Risk sources and acts	Risk mitigation measures and treatments	
	Scalable measures to address changes in threat environment	Treatment to strengthen existing control environment
• Unauthorised release of information • Bomb threats and hoaxes • Theft • Vandalism • Verbal assault • Organised crime • Foreign intelligence services • Threat from disgruntled participants[b]	• Clear desk checks • Emergency response training and emergency control organisation • Individual security risk management plans for at risk personnel • Mandatory security awareness briefings • Security guards and patrols	• Access controls • Alarm and monitoring systems • Closed circuit television (CCTV)[a] • Control layers • Emergency warning system to warn visitors and staff not to enter the building during emergencies • Protocols, procedures, and policies for working with disgruntled participants[b]

Note a: The DSS Security Plan 2019–21 states that implementation of these measures was specific to one site.

Note b: This risk source and risk mitigation measures were added in a review of the Security Risk Assessment, as discussed at paragraph 3.30.

Source: DSS Security Plan 2019–21.

Risk assessment and physical security measures at selected DSS facilities

3.31 In 2018–19, DSS conducted physical site inspections to complete risk assessments at the selected sites. These risk assessments covered risk identification, risk assessment and assessment of physical security controls in place.

3.32 DSS' Security Plan for 2019–21 (see Table 3.2), stated that it planned to undertake bi-annual risk assessments (Threat and Vulnerability Assessments) for all its facilities. Its regular approach involved conducting physical inspections of its facilities. Risk assessments for selected sites were not completed. DSS advised that due to COVID-19 travel restrictions it was not possible to conduct physical inspections, therefore assessments were done remotely. DSS advised that it did not document the change and risk assessments were 'based on previous physical inspections and determination as to whether any physical modifications had been carried out'. Outcomes of risk assessments undertaken in this manner were not documented. The absence of physical site inspection leads to reduced assurance that other physical measures were operating as intended. DSS continued to report 'managing' and 'embedded' maturity.

Physical security measures that minimise or remove risk of harm to people, information, and physical assets

3.33 The ANAO conducted site visits to selected DSS facilities in November and December 2021 to examine the implementation of physical security measures in accordance with DSS' Security Plan 2019–21 (see Table 3.4). The ANAO found that DSS had implemented all planned risk mitigation measures and treatments except for the emergency warning system (used to warn visitors and staff not to enter the building during emergencies) for one building.

3.34 In 2018–19 DSS assured itself that the physical security measures it put in place were effective through its risk assessment process. For 2019–20 and 2020–21, DSS could not evidence that it had undertaken controls testing of physical security measures in place, partly because DSS did not document any risk assessments (as noted in paragraph 3.32).

Disposal of physical assets

3.35 Under an arrangement with Services Australia, the Services Australia Chief Information Officer was responsible for all DSS' ICT disposals and the cleansing of DSS' ICT equipment prior to disposal. As of February 2022, DSS is reviewing operational procedures and assurance framework for the Service Schedule for ICT Shared Services with Services Australia to address reporting and assurance requirements. The revised framework and schedule are due to be completed by the end of financial year.

3.36 DSS did not have a standard operating procedure for the decommissioning of its sites. DSS had a checklist that covers security and property requirements during decommissioning. The checklist included a check of any safes, a visual inspection and check that all documents have been removed. DSS also had a process for sanitising security containers and for combination resets. Of the selected sites, DSS decommissioned one floor at one location. DSS filled a decommissioning checklist for this floor on this site, which was signed by an SES officer in accordance with DSS requirements.

3.37 During site visits to DSS facilities in November and December 2021, the ANAO observed that DSS had in place destruction equipment for paper-based information.

Did DSS implement mandatory protective security measures at its facilities, at the 'managing' and 'embedded' maturity levels?

DSS was partly effective in implementing its protective security measures at selected facilities. It had integrated protective security measures at its facilities for all reporting years. In all reporting years its reported maturity levels were inaccurate because there were gaps in certification and accreditation documentation.

3.38 Policy 16 requires that a consistent and structured approach be applied to building construction, security zoning and physical security control measures of entity facilities.

3.39 In 2018–19, DSS reported that it had a maturity level of 'managing'. At this maturity level, all stages of selection, planning, designing, and modifying facilities are required to have physical security requirements integrated into them. Entity facilities are expected to be certified and accredited and these processes documented. DSS had further reported that it 'fully' implemented the requirements (that were applicable) for policy 16, and that its implementation was effective and requirements are integrated into business practices.

3.40 In 2019–20 and 2020–21, DSS reported that it had reached an 'embedded' maturity level. At this maturity level, physical security requirements are a key driver for selection, design or modification of entity facilities. The entity also actively ensures certification and accreditation of entity facilities in accordance with the PSPF, with upgrades implemented as a priority. DSS reported that it had 'excelled' at implementing each applicable requirement under policy 16, meaning that better-practice guidance and requirements are proactively implemented in accordance with the entity's risk environment. To have 'excelled', implementation is effective in mitigating security risks, and requirements are integrated into business practices.

3.41 The ANAO examined DSS' security plans and documentation and evidence of its implementation of protective security measures at the reported maturity level. The ANAO conducted site visits at three selected DSS facilities. Table 3.5 shows findings for policy 16 for these sites.

Table 3.5: DSS' implementation of policy 16

Policy requirement	ANAO assessment	ANAO comment
Fully integrate protective security in the process of planning, selecting, designing and modifying its facilities for the protection of people, information and physical assets.	◆	In 2018–19, 2019–20 and 2020–21 DSS had integrated physical security considerations into its processes.
In areas where sensitive or security classified information and assets are used, transmitted, stored or discussed, certify its facility's physical security zones in accordance with the applicable Australian Security Intelligence Organisation Technical notes.	▲	DSS largely implemented mandatory PSPF protective security measures such as guards, alarms, perimeter doors and hardware, as well as limiting access to authorised personnel, visitors, vehicles, and equipment. Across all reporting years, DSS did not finalise certification documentation.
Accredit its security zones.	■	DSS did not document its accreditation across all years.

Key: ◆ Appropriately implemented. ▲ Partly implemented. ■ Not implemented.

Source: ANAO analysis of DSS activities.

Integration of protective security at facilities

3.42 DSS has integrated physical security requirements into its processes for planning, selecting, designing, and modifying facilities. DSS had procedures for all its new leases or buildings, and refurbishments of existing departmental accommodation, which require that a Security Brief is prepared. The Security Brief was to cover physical security requirements.

3.43 Of the sites selected for ANAO review, DSS advised that it only undertook minor internal design and modification works at one site. Security briefings were not prepared for this site as required.

3.44 In accordance with PSPF requirements, DSS integrated a security alarm and access control system across its facilities, which was used in conjunction with security guards. DSS also limited access to authorised personnel, visitors, vehicles, and equipment.

3.45 The ANAO examined a sample of alarm privileged user reports, security clearance information and alarm response report data from the selected sites between 1 January 2020 and 30 June 2020. This analysis found that users of the alarm system had appropriate security clearances. Examination of users accessing and operating the alarm system found that they were all authorised to do so. DSS advised that it did not use the data from its alarm and building access monitoring system to review terminated staff access, in order to assure DSS that unauthorised users (terminated staff) are not improperly accessing information and resources. Alarm and building access data was not used to support overall maturity ratings in DSS' PSPF self-assessment.

3.46 DSS implemented physical security measures (discussed at paragraph 3.33) to ensure that perimeter doors and hardware were secured. The zone assessment tools included sections addressing whether relevant hardware, approved by the Security Construction and Equipment Committee (SCEC), was installed. As discussed at paragraph 3.49, certification documentation was incomplete, making it difficult for DSS to substantiate that SCEC requirements were integrated in all instances to the satisfaction of the DSS Chief Security Officer or Agency Security Adviser.

Certification of security zone areas

3.47 Certification establishes the zone's compliance with the minimum PSPF physical security requirements to the satisfaction of the Chief Security Officer or Agency Security Advisor. DSS established an assessment tool for certifying its security areas. The zone assessment tool is to be signed by the Agency Security Adviser and quality assured by a security officer. The tool contains a checklist to identify whether physical security measures are compliant with the PSPF.

3.48 Since 1 October 2018, DSS has maintained a physical security register which recorded zone information for each of its lease sites. Across all its facilities, DSS did not have a zone five security area and had one zone four security area.

3.49 ANAO analysis of DSS documentation and zone assessment tools for the selected DSS sites found that 39 per cent of certification documentation was not signed or dated, making it difficult for DSS to substantiate that certification was completed in a timely and compliant manner. Certification documentation was not available for five of seven zones across three sites in 2018–19.

3.50 For the 2019–20 and 2020–21 periods, DSS planned to undertake bi-annual security zone assessments for all its facilities (see Table 3.2). Its regular approach involved conducting physical inspections of its facilities. As discussed in paragraph 3.32, DSS advised that its regular physical inspection plans were not conducted due to COVID-19. Outcomes of these assessments were not documented. DSS did not document the change to its zone assessment approach.

3.51 DSS has outsourced its ICT facilities under an arrangement with Services Australia. From 19 December 2019, DSS obtained from Services Australia accreditation from the Services Australia Chief Security Officer, which stated that the relevant ICT facilities were certified in accordance with the PSPF.

3.52 The ANAO was unable to determine whether certification was completed prior to the security zone areas being operational as DSS did not retain details of the first operational use of its security zone areas.

Accreditation of security zones

3.53 The Chief Security Officer or Agency Security Adviser can accredit the facility's security zone areas by compiling and reviewing all applicable certifications and other deliverables for the zone and determining and accepting the residual security risks.

3.54 Across all reporting periods, DSS did not accredit its security zones for its facilities with appropriate documentation. There was also irregular reporting for accreditation certification of security zones for ICT sensitive and security classified information with extreme business impact, when DSS advised that such security zones were not applicable to the department.

Recommendation no. 3

3.55 The Department of Social Services complete its certification and accreditation of its security zone areas, with documentation in accordance with PSPF core requirements.

Department of Social Services response: *Agreed.*

3.56 The department acknowledges the requirement to certify and accredit facilities in line with requirements established in the department's security plan and to ensure appropriate supporting evidence is maintained to demonstrate Protective Security Policy Framework core requirements being met. The department has completed the recertification and accreditation of all facilities and documented this in accordance with requirements.

4. Services Australia's security maturity monitoring and provision of a secure physical environment

Areas examined

This chapter examines whether Services Australia has implemented the requirements for security maturity monitoring, physical security measures for entities resources and protective security measures at its facilities, under the revised Protective Security Policy Framework (PSPF).

Conclusion

Services Australia was largely effective at implementing requirements that it established for itself under the PSPF at the 'developing' maturity level. Physical security measures to protect people were well established and developing for information and physical assets. Protective security measures were integrated into business-as-usual operations, including at modified facilities. Services Australia's reporting was not accurate because in two years its reporting was based on an outdated security plan, and it did not evidence that most certifications and accreditations met requirements. Services Australia's Security Plan 2020–22 remedied deficiencies in its previous outdated plan. Certification and accreditation documentation is being reviewed and improved.

Areas for improvement

The ANAO made two recommendations aimed at Services Australia undertaking site risk assessments before it modernises facilities; and reviewing its assurance arrangements and recordkeeping of measures to protect security classified interactions.

4.1 The PSPF requires entities to comply with physical security requirements in policy 4 (security maturity monitoring), policy 15 (physical security for entity resources) and policy 16 (entity facilities).

4.2 To assess whether Services Australia met requirements, the ANAO examined whether:

- assessments of security capability and risk culture were aligned with security plans and demonstrated routine consideration of progress against set goals;
- risks were assessed and physical security measures were selected and implemented at facilities visited by the ANAO; and
- protective security was fully integrated into planning, selection, modification and design of facilities and certifications and accreditations were undertaken.

Did Services Australia effectively implement security maturity monitoring at the 'developing' and 'managing' maturity level?

Services Australia was partly effective at considering its progress against the goals and strategic objectives in its security plans. For the first two reporting periods assessed, Services Australia's reported maturity levels were inaccurate because the security plan was outdated, and Services Australia did not have a consistent and defined approach to monitoring its performance against identified goals and objectives.

4.3 The PSPF policy 4 core requirement is each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan. The entity should set indicators in its entity security plan against which to evidence and document its assessment. The supporting requirement of this policy is that entities document and evidence their assessment of the entity's security maturity. Monitoring security maturity is an ongoing process that involves routine assessment of security capability and risk culture against the set indicators.

4.4 In 2018–19, Services Australia self-assessed and reported its maturity for policy 4 as 'developing', which remained at 'developing' maturity in 2019–20 and increased to 'managing' in 2020–21.

4.5 At 'developing' level, security capability and risk culture is addressed in the entity's security plan; and performance and progress against the security plan's goals and strategic objectives is substantially monitored regularly. At 'managing' level there is a consistent and defined approach to monitoring the entity's security performance which is tailored to the entity's risk environment. An entity at 'managing' level also has clearly defined security goals and objectives in its security plan and has tracked and measured performance to assess its security capability and risk culture maturity.

4.6 The ANAO examined Services Australia's security plans and documentation and evidence of its implementation of policy 4, including its assessments of security capability and risk culture maturity at the reported levels. Table 4.1 outlines findings for policy 4.

Table 4.1: Services Australia's implementation of revised PSPF policy 4

Policy requirement	ANAO assessment	ANAO comment
Assess the maturity of security capability against the goals and strategic objectives identified in its security plan.	▲	For all reporting years, Services Australia undertook and documented assessments of its security position in relation to its specific risk environment. It did not undertake these assessments against goals and objectives in its security plan. Services Australia has not had a consistent and defined approach to monitoring its security capability.
Assess the maturity of risk culture by considering its progress against the goals and strategic objectives identified in its security plan.	▲	For all reporting years, Services Australia undertook and documented assessments of personnel behaviours, attitudes and understanding. It did not undertake assessments against goals and objectives in its security plan. Services Australia has not had a consistent and defined approach to monitoring its security risk culture.

Key: ◆ Appropriately implemented. ▲ Partly implemented. 🟥 Not implemented.

Source: ANAO analysis of Services Australia activities.

Goals and objectives in Services Australia's security plans

4.7 Since 1 October 2018, Services Australia has had two security plans in place. The first plan titled Agency Security Plan 2014–16 was created by the Department of Human Services (DHS). This was before the revised PSPF commenced and before Services Australia was renamed under machinery of government changes that took effect on 1 February 2020. The plan remained in place beyond its stated expiry (of December 2016) to December 2020, when the new plan came into effect. In 2019, DHS recommended a 'deep review' of the document suite to update for the revised PSPF. After machinery of government changes, Services Australia commenced a review and update of its plan in 2020.

4.8 In October 2020, Services Australia presented its accountable authority with a revised Protective Security Control Plan 2020–22. This plan was endorsed by Services Australia's accountable authority and is current until December 2022.

4.9 The Agency Security Plan 2014–16, outlined an 'overall security philosophy' rather than specific security goals and objectives. The plan did not address security capability or risk culture as needed to substantiate a self-assessment of 'developing', or the lower 'ad hoc' maturity. The plan did not clearly specify how the 'overall security philosophy' intersected with the entity's business objectives and priorities or address the entity's tolerance to security risks; and did not outline strategies to implement security risk management.

4.10 The Protective Security Control Plan 2020–22 described a two-year agenda to 'lift our protective security culture and more strongly embed protective security into our business and culture'. Services Australia's stated goal was to manage protective security risk 'while continuing to innovate and improve customer experience'. This plan indicated Services Australia's intention to 'deliver initiatives over the life of this plan to meet in full all 16 Framework core requirements by 2022'. The 2020–22 plan appropriately addressed 10 of 11 elements recommended by AGD for inclusion in a security plan.[34] It lacked strategic objectives (or purpose statements) for the activities it planned to complete (see Table 4.2).

4.11 The plan did not define an approach to monitoring the entity's security performance that is clearly linked to performance measures. This makes it difficult for Services Australia to substantiate that its monitoring activities were consistent with its plan and were achieving planned objectives.

4.12 Services Australia's 'broad security strategy' is articulated in the plan as 'predict, prevent, control and assure, and disrupt'. The entity's approach to strengthening its protective security maturity is defined in the 'Summary of the Protective Security Action Plan 2020–22' which is attached to the security plan. An extract of relevant policy 4, 15 and 16 strategies is presented in Table 4.2.

[34] AGD's Protective Security Guide for Chief Security Officers published in 2020 recommends that security plans contain:

> security goals and strategic objectives, including how security risk management intersects with and supports broader business objectives and priorities; threats, risks and vulnerabilities that impact the protection of your entity's people, information and assets; your entity's tolerance to security risks; maturity of your entity's capability to manage security risks, and strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.

See Attorney-General's Department, *Protective Security Guide for Chief Security Officers*, AGD, Canberra, 2020, p. 18, available from https://www.protectivesecurity.gov.au/system/files/2021-06/protective-security-guide-chief-security-officers.pdf [accessed 2 May 2022].

Table 4.2: Selected strategies and activities in Services Australia's security plan 2020–22

Responsible Division	Strategies and activities	PSPF policy	Planned completion
Business Integrity	Coordinate a review of the agency's protective security governance and reporting arrangements and develop a two-year change agenda to more strongly embed protective security into the agency's business and culture. As the first step, present the new agency security plan to the accountable authority for approval.	4	In 2020 In October 2020
Portfolio Shared Services	Conduct an audit of all Security Construction and Equipment Committee (SCEC) endorsed A and B class containers and shredders across the agency.	15	30 June 2021
	Ensure the agency has commenced reviews of both physical and administrative arrangements across all identified areas processing security classified information and/or assets.	15	30 June 2021
	Undertake trials of networked intruder alarm and access control systems across select sites to strengthen and standardise access and response arrangements.	15	30 June 2021
	Complete physical security zone certifications for 11 outstanding agency sites under the agency's rolling program of site security reviews.	15	30 June 2021
	Review existing physical security policies and procedures in accordance with the requirements of the 2018 Protective Security Policy Framework.	16	30 June 2021
	Develop and embed a process that incorporates timeframes for commissioning and zone certification prior to agency sites being used operationally.	16	30 June 2021
	Certify all 11 Zone Two and all 6 Zone Three compartmentalised areas.	16	30 June 2021
	Finalise reviews of physical and administrative security arrangements to all identified Zone Three areas processing security classified information or assets, (including completing zone certification of these areas).	16	31 July 2021

Source: ANAO based on Services Australia's Protective Security Control Plan 2020–22.

4.13 As outlined in Table 4.2, the timing of activities in the plan was shorter than the stated two-year life of the plan. PSPF policy 4 strategies pre-date the commencement of the plan in December 2020. Strategies for PSPF policies 15 and 16 cover only the first six months of the plan.

Monitoring of security capability and risk culture

4.14 Under policy 4, Services Australia is required to assess its security capability maturity, which is its security position in relation to its specific risk environment and risk tolerances. Policy 4 also requires Services Australia to assess its risk culture. Services Australia's risk culture is its system of values and its personnel behaviours, attitudes and understanding that are related to its security risk that shapes the risk decisions of its leadership and personnel.

Documented assessments 2018–20

4.15 As stated in paragraphs 4.7 and 4.9, between October 2018 and December 2020, Services Australia did not have a security plan against which it reviewed its performance and progress of security capability or risk culture. In this period, Services Australia undertook some activities to assess its specific risk environment, security capability and risk culture, which did not meet core requirements because they were not identified in a security plan. In addition, Services Australia undertook some security control reviews and post incident reviews to evaluate and learn from security incidents; and it undertook some scheduled site security reviews to understand and manage security risks.

Documented assessments in 2021

4.16 Throughout 2021, Services Australia had an endorsed security plan that captured the entity's goals, objectives, risk tolerance and strategies. Services Australia continued to undertake and document its activities to assess its security position in relation to its risk environment and risk tolerances. Box 1 indicates the activities related to strategies in the plan. The absence of targets and performance indicators renders it difficult for Services Australia to know how it is performing against plan targets. The core requirement of policy 4 is to assess maturity of security capability and risk culture against the security plan.[35]

Box 1: Services Australia's assessments of security capability and risk culture (January 2021–December 2021)

Services Australia undertook fraud and corruption activities including investigations, referrals for prosecution and a staff survey. Services Australia also provided staff training on security and it undertook monitoring and reporting of property damage, assaults, and cyber security incidents.

4.17 The restructure and expansion of the Security Branch in March 2021 and reporting through the Security Sub-Group to the Enterprise Business and Risk Committee have the potential to improve Services Australia's ability to assess its security capability and risk culture maturity. The Security Branch has undertaken security awareness and outreach campaigns to increase staff understanding of security risks and obligations. The Security Sub-Group, which was established in November 2020, is performing its monitoring functions consistent with its terms of reference and consistent with the security plan.

Did Services Australia implement mandatory physical security measures for its resources at the 'developing' maturity level?

Services Australia was largely effective at implementing physical security measures for its resources at facilities visited by the ANAO. Services Australia's reporting of 'developing' was accurate because it did not implement all site security review recommendations, provide all information to staff, or fully assure itself of building access and usage of ICT facilities.

[35] PSPF policy 4, B.1 Core requirement states: Each entity **must assess the maturity** of its security capability and risk culture by considering its progress **against** the goals and strategic objectives identified in **its security plan** [ANAO emphasis added].

4.18 Policy 15 describes the physical protections required to safeguard people (consistent with the requirements of the *Work Health and Safety Act 2011*), information and assets (including ICT equipment) to minimise or remove security risk. The core requirement of policy 15 is that each entity must implement physical security measures that minimise or remove the risk of harm to people, and information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

4.19 In 2018–19, Services Australia self-assessed and reported its maturity for policy 15 as 'developing' and remained at 'developing' in 2019–20 and 2020–21.

4.20 At 'developing' level an entity has in place physical security measures that minimise or remove the risk of resources being made inoperable, inaccessible, accessed, or removed without proper authorisation. At 'developing' level, most physical security measures are implemented according to requirements.

4.21 The ANAO examined the accuracy of Services Australia's three self-assessment reports through its implementation of policy 15 requirements at the reported maturity level. Table 4.3 outlines findings for policy 15.

Table 4.3: Services Australia's implementation of revised PSPF policy 15

Policy requirement	ANAO assessment	ANAO comment
Implement physical security measures that minimise or remove the risk of harm to people.	◆	Physical security measures, particularly in face-to-face service environments, were implemented and mature and regular reporting indicates the measures are minimising the risk of harm to staff and customers.
Implement physical security measures that minimise or remove the risk of information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without proper authorisation.	▲	Physical security measures were in place. Services Australia did not fully implement all recommendations in site security reviews, provide information to staff that it stated it provided, use access data to monitor the effectiveness of physical measures, and restrict use of designated ICT facilities.

Key: ◆ Appropriately implemented. ▲ Partly implemented. 🟥 Not implemented.

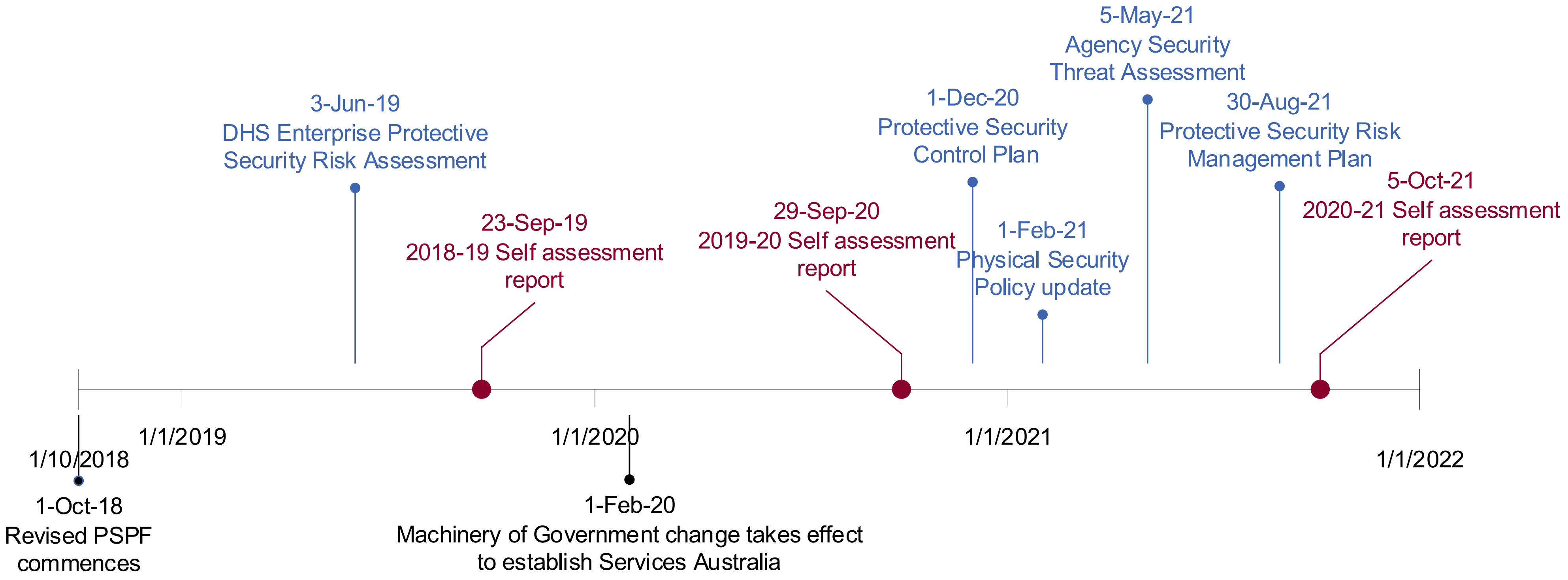
Source: ANAO analysis of Services Australia activities.

Services Australia's assessment of security risks and selection of appropriate security measures

4.22 Until it was updated in February 2021, the DHS Physical Security Policy, dated 26 June 2018, articulated Services Australia's requirements for all ongoing and non-ongoing Services Australia staff, contractors, and other entity staff working under shared premises arrangements at Services Australia sites. The policy required that the application of physical security measures must be appropriate and proportionate to the value of the asset, person and information being protected. The Physical Security Policy requires that Services Australia put in place physical security measures 'commensurate with the assessed business impact level of their compromise, loss or damage.'

4.23 In accordance with the DHS policy, an Enterprise Protective Security Risk Assessment was undertaken in 2018–2019 to assess protective security risks in accordance with the revised PSPF and to formulate measures to enhance its security arrangements. Services Australia followed this in May 2021 with an Agency Security Threat Assessment. Services Australia's latest risk assessment was its Protective Security Risk Management Plan formed in August 2021. Figure 4.1 summarises the finalisation dates of key documents considering completed self-assessment reports.

Figure 4.1: Finalisation dates of key enterprise threat and risk assessments



Source: ANAO analysis of Services Australia documentation.

4.24 As Figure 4.1 demonstrates, most risk assessment documents were finalised after the first two self-assessment reports were submitted to AGD.

4.25 Services Australia completed site security reviews to determine protective security issues at sites and provide advice about appropriate strategies to treat these risks (discussed at paragraphs 4.28 to 4.29).

Physical security measures that minimise or remove the risk of harm to people

4.26 Services Australia has identified physical injury (assault, attack with weapon or vehicle attack) and psychological harm to staff and customers among its enterprise security risks. This is due to Services Australia's provision of face-to-face services at service centres around Australia. Services Australia has developed controls and treatments to address the risks of harm to people.

4.27 The physical security measures to protect people that are included in the entity's enterprise-level assessment and plan relate to and include those outlined in PSPF policy guidance. Table 4.4 depicts the correspondence between protective security elements in the revised PSPF and Services Australia's controls and treatments.

Table 4.4: Services Australia's protective security controls corresponding to PSPF measures for people

Elements in PSPF policy guidance	Services Australia controls and treatments
Threat and risk assessment of specific situations (C.1.1.5a)	Enterprise security risk assessment External guarding capability Site security reviews Security risk assessments for home-based work
Reporting incidents to management, human resources, security and law enforcement (C.1.1.5b)	Customer aggression reporting Security incident reporting
Providing information to employees (C.1.1.5c)	Emergency Response Procedures Physical security policies and procedures Preventing and managing customer aggression policy Security Hub Services Australia Security hotline Standard operating procedures for travel into remote areas
Providing training to employees (C.1.1.5c)	Code grey and black training[a] Mandatory refresher program Ongoing personnel security awareness training
Providing counselling to employees (C.1.1.5c)	Employee Assistance Program[b] Mind tools database and libraries Work health and safety strategy 2021–2026
Maintaining thorough records and statements on reported incidents (C.1.1.5d)	Fraud and Corruption Detection program Security incident reporting

Note a: Codes grey and black denote specific responses during emergencies. During code grey emergencies, people take shelter in the site's secure back of house. In the event of a code black emergency, people evacuate.

Note b: Counselling is part of Services Australia's enterprise approach and is not in place solely to address security risks. Counselling is not mentioned in the Enterprise Security Risk Assessment and Protective Security Risk Management Plan.

Source: ANAO based on Services Australia documentation.

Threat and risk assessments: site security reviews

4.28 The aim of Services Australia's site security reviews is to 'identify protective security issues at the nominated site and provide advice in regards [sic] to appropriate strategies designed to treat these risks.' Site security reviews were undertaken for all sites visited by the ANAO.

4.29 During site visits, the ANAO identified that some recommendations in completed site security reviews had not been implemented to treat identified risks. For example, vehicle bollards had not been installed along the frontage of one site, which the April 2019 site security review indicated was vulnerable to vehicle intrusion and required attention within three months of the final report date (pending landlord and Council approval). October 2018 recommendations to de-clutter and position items such as stationery and general office equipment out of customer reach were not fully implemented. Recent security issues involving out-of-hours customer usage of an entrance ramp at one building are not reflected in the current site security review for that site.

4.30 Services Australia advised the ANAO that the 'documentation of agreed actions in response to recommendations included in completed site security reviews could be improved to demonstrate the closing out of responses.'

Maintaining records and reporting incidents

4.31 Services Australia's mechanisms for reporting incidents included the Customer Incident Recording System (first implemented in April 2017), security incident reporting process, cyber security incident reporting, work health and safety reporting, privacy incident reporting, fraud reporting process and bullying reporting process. Records from 1 October 2018 to September 2021 indicated there were 16,318 injuries or incidents recorded for Services Australia employees and 250 accepted workers compensation claims for Services Australia employees. Nine of the accepted workers compensation claims were due to exposure to workplace or occupational violence or assault.

4.32 Services Australia had daily, weekly, and monthly operational reporting to its Executive Committee on security incidents in service centres. Historically, security reporting was undertaken quarterly. In 2021, this frequency increased during the COVID-19 pandemic. Services Australia reporting indicates that during 2019–20 there were 202 reported incidents of assault where the customer's identity was known and in 2020–21 there were 164 reported incidents.

Providing information on physical security policies and procedures

4.33 Services Australia listed 15 policies and procedures in its Protective Security Control Plan 2020–22 relevant to minimisation and removal of the risk of harm to people, information and physical asset resources. The Protective Security Control Plan indicated that all policies and procedures are located on Services Australia's Security Hub. The ANAO identified two standalone policies related to protective security on the Hub. Services Australia's Control Plan indicated that staff security and physical security policies and procedures are subject to review in 2020–21. Review is not yet completed.

Providing training

4.34 Services Australia offered staff a variety of security training in its online Learning Management System. The available modules include the Mandatory Refresher Program which runs every two years. As of 31 December 2021, 94 per cent of all Services Australia staff had completed the mandatory modules, up from 77 per cent in June 2020.

Physical security measures that minimise or remove risk to information and physical asset resources

4.35 Services Australia had in place a range of physical security measures that minimise or remove the risk of resources being made inoperable, inaccessible, accessed, or removed without proper authorisation. The entity implemented most measures described in the PSPF policy 15 guidance.

4.36 Staff guidance material addressed some of the measures (site security, identification and building access cards, and working away from the office). During site visits, the ANAO observed most physical security measures implemented according to PSPF requirements. Exceptions are described in paragraphs 4.37 to 4.41.

Layers of physical security in facilities

4.37 The entity used a 'security-in-depth' principle, incorporating a multi-layered security design in the protection of people, information and assets. Building swipe access data was collected in Canberra. The ANAO compared a sample of employee termination records to building swipe access data from 1 January 2020 to 30 June 2020. The ANAO did not identify any exceptions in the sample.

4.38 There was variability in the availability of building access data. Data for Canberra corporate buildings was accessible onsite by Services Australia staff. Services Australia does not have a network system that provides agency-wide assurance that only authorised individuals have access to all sites.

4.39 In response to queries from the ANAO about whether the data was used to substantiate PSPF reporting, Services Australia advised that it accessed the data to support incident response or investigation. The entity advised that 'effective analysis of the data would assist Services Australia lift its maturity to the desired 'managing' level'.

Measures for the protection of ICT equipment

4.40 Designated local area network (LAN) rooms were operating at each of the six selected facilities visited by the ANAO. Server equipment including racks and network cables were open to tampering or inadvertent damage once inside the LAN room because lockable rack doors were left open at all sites visited by the ANAO. All LAN rooms inspected by the ANAO were being used as temporary storage for building and cleaning activities as well as temporary storage for surplus ICT equipment.

Disposal of physical assets

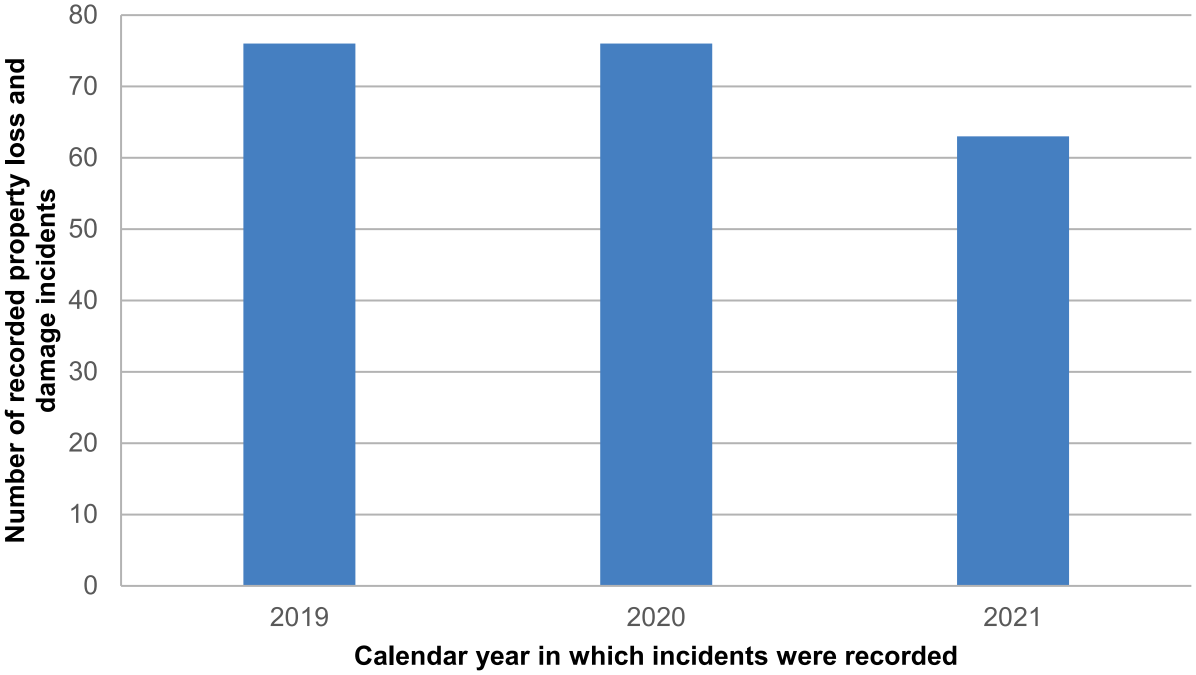
4.41 Asset disposal procedures and templates were in place at the enterprise and site level. The enterprise-level procedures did not include requirements to undertake sample tests of sanitised devices. Services Australia advised that asset disposal procedures in place included the engagement of a service provider to perform IT asset disposals. This service provider was contractually required to comply with the Australian Government Information Security Manual (ISM) as outlined in the head agreement to perform IT asset disposals. Services Australia advised that assurance is gained when a reconciliation report from the service provider is reconciled against internal records.

Property loss and damage incidents

4.42 To determine whether Services Australia's physical security measures are minimising or removing risk in the manner intended, the entity monitors property loss and damage incidents and undertakes stocktakes of portable and attractive items every three years.

4.43 In the period 2019–2021, Services Australia recorded 215 property loss and damage incidents with a six per cent decrease in the number of incidents between 2020 and 2021. This is illustrated in Figure 4.2.

Figure 4.2: Property loss and damage incidents 2019–2021



Source: ANAO based on Services Australia documentation.

Personal Issue Stocktake

4.44 Apart from asset stocktakes undertaken for financial reporting purposes, Services Australia's Asset Management Policy and Procedures Guide requires a personal issue stocktake to be conducted on a six-monthly basis every financial year. Personal issue items include mobile computing devices, mobile phones, equipment used in a home office, data cards, cameras, USBs, and external hard drives. These are deemed portable and attractive and high profile to the entity because they may be removed from the workplace, may contain agency data and may be subject to high probability of misuse or re-sale outside the workplace. The personal issue stocktake was a control measure and confirmation that personal issue items were correctly recorded, sighted and a business need continued to exist.

4.45 Services Australia did not undertake personal issue stocktakes every six months as planned. A full stocktake of assets was undertaken in the 2018–19 financial year and a personal issue stocktake was undertaken in October 2019 and April 2021. In April 2021, the value of unsighted assets totalled $2.9 million. The entity advised in relation to 2019–20:

> The entity advised that no personal issue stocktakes were undertaken during 2020 due to the impact of disaster response and COVID-19 responses that eventuating in multiple successive lockdowns. During 2021–22 the entity commenced a transition to an electronic systems-based approach to asset identification.[36]

4.46 Services Australia advised that as at 10 March 2022, 86 per cent of personal computing assets by volume and 92 per cent by net book value have been verified using this approach.

Did Services Australia implement mandatory protective security measures at its facilities at the 'developing' maturity level?

Services Australia was largely effective in implementing protective security measures at sites visited by the ANAO. In all reporting years, it considered and substantially integrated physical security requirements into all facilities visited by the ANAO. In all reporting years, its reported maturity levels were inaccurate because certifications and accreditation were partially in accordance with applicable requirements. Documentary records lacked explicit determination and acceptance of residual security risks.

4.47 Policy 16 provides the consistent and structured approach to be applied to building construction, security zoning and physical security control measures of entity facilities. This ensures the protection of Australian Government people, information and physical assets secured by those facilities. Each entity must:

- ensure it fully integrates protective security in the process of planning, selecting, designing, and modifying its facilities for the protection of people, information and physical assets;
- in areas where sensitive or security classified information and assets are used, transmitted, stored, or discussed, certify its facility's physical security zones in accordance with the applicable Australian Security Intelligence Organisation (ASIO) Technical Notes; and
- accredit its security zones.

4.48 In 2018–19, Services Australia self-assessed and reported its maturity for policy 16 as 'developing', which remained at 'developing' in 2019–20 and 2020–21.

4.49 At 'developing' level an entity considers physical security when planning, selecting, designing and modifying facilities in the majority of cases, with physical security requirements substantially integrated into all facilities. Certification and periodic review of the majority of entity facilities is in accordance with ASIO Technical Notes. The majority of security zones are accredited.

4.50 The ANAO examined the accuracy of Services Australia's three self-assessment reports for the implementation of policy 16 requirements at the reported maturity level. Table 4.6 outlines findings for policy 16.

[36] Services Australia's advice to the ANAO, April 2022.

Table 4.6: Services Australia's implementation of revised PSPF policy 16

Policy requirement	ANAO assessment	ANAO comment
Fully integrate protective security in the process of planning, selecting, designing and modifying its facilities for the protection of people, information and physical assets.	◆	Services Australia considered physical security when modifying selected facilities and has documented specifications in place for when it designs, plans and chooses new facilities. Physical security requirements such as alarms, security guards, access control locks and door hardware, closed circuit television are integrated into all facilities visited by the ANAO.
In areas where sensitive or security classified information and assets are used, transmitted, stored or discussed, certify its facility's physical security zones in accordance with the applicable ASIO Technical notes.	▲	Services Australia began to certify and periodically review selected facilities in 2021. Certifications were complete for two sites visited by the ANAO.
Accredit its security zones.	▲	Of the six facilities visited by the ANAO, two facilities were accredited as required, and four were partially accredited as required.

Key: ◆ Appropriately implemented. ▲ Partly implemented. ■ Not implemented.

Source: ANAO analysis of Services Australia activities.

Consideration of physical security requirements

4.51 In December 2021, Services Australia had 429 sites around Australia. Most Services Australia sites (94 per cent) restrict public access with unrestricted access for authorised personnel.

4.52 Services Australia maintained specification documents to inform the design and construction of its sites. In its self-assessment 2020–21, the entity reported that it plans to refine its property strategy and framework before June 2023.

4.53 After a December 2019 commissioned review of face-to-face services, and trials of newly branded low-risk centres, Services Australia began modifying its service centre environments. Modifications were intended to create a more open, attractive, and comfortable environment for customers. Services Australia considered physical security in the redesign process and identified the security focus of some centres as a 'key pain point'.

4.54 The assessment of low-risk trial sites concluded that the trialled concepts 'had a satisfactory outcome without compromising security or compliance'. In accordance with the core requirement, entities must consider protective security measures as early as possible, preferably during the concept and design stages of significant modifications to facilities. The trialled concepts from low-risk environments were being implemented in higher risk locations. At the time the ANAO visited one of Services Australia's higher risk service centres, a physical risk assessment had not been completed before the site was used operationally.

Recommendation no. 4

4.55 Services Australia undertakes site risk assessments as early as possible in the process of planning, selecting, designing, and modifying its facilities.

Services Australia response: *Agreed.*

4.56 Services Australia has commenced operating in line with this recommendation. This includes instigating early engagement across all internal business areas in the process of planning, selecting, designing and modifying its facilities. Undertaking site risk assessments as early as possible in our process will simplify and improve the transparency of residual risk determination, and acceptance by the relevant risk owner. In turn, this will also improve Services Australia's maturity levels in relation to certification and accreditation of sites in accordance with PSPF requirements.

Integration of physical security requirements

4.57 Physical security requirements were integrated into all facilities visited by the ANAO, including:

- defined restricted access areas and layering;
- security alarms;
- security guards;
- interoperable alarms and other building management systems;
- access control systems;
- locks and door hardware; and
- closed circuit television.

Security alarms

4.58 The ANAO examined a sample of alarm privileged user reports, security clearance information and alarm response report data from Canberra between 1 January 2020 and 30 June 2020. The ANAO found fictional names and pseudonyms in the alarm user data. Services Australia advised that fictional names and pseudonyms are used for temporary pass allocation labelling in the system. A hard copy pass register documents the allocation of the temporary pass to a specific person instead of a fictional name or pseudonym. Services Australia advised that the pass register provides a mechanism to link the use of the temporary card to an individual.

4.59 Services Australia confirmed that it does not use alarm data to substantiate its self-assessment reports. Services Australia undertakes reviews of access by alarm operators on an exception basis, for example, during fraud control activities.

Security classified interactions

4.60 Services Australia assured itself that security classified resources were appropriately protected by managing access to storage locations using multi-factor authentication, and a clear desk program in Canberra sites only. These assurance activities were not consistently undertaken outside Canberra at the sites visited by the ANAO. The entity advised this is because 'classified documents are rarely created and stored outside of its Canberra corporate sites'. The entity did not track the creation or storage of classified documents. Services Australia provided staff with guidance about information security markings, correct procedures for storing classified documents and record management issues.

4.61 The entity applied appropriate processes to share secret level documents between relevant staff across agency sites and other secure areas offsite.

4.62 At one site, Services Australia relied on a 2016 sound insulation survey for assurance that classified conversations were not audible if held within a certain conference room. The survey indicated that acoustic control elements that had been implemented were operating effectively. The survey did not address other control elements, establish the zone's compliance with minimum physical requirements, and lacked explicit acceptance that requirements were satisfactory to the certification authority. It did not meet PSPF requirements for 'certification' of areas where sensitive or security classified information was discussed.

4.63 Services Australia has advised that the zone was documented and met the PSPF requirements for certification and accreditation in 2021.

Recommendation no. 5

4.64 Services Australia review and strengthen its monitoring and assurance arrangements for key physical security controls that seek to protect agency and Australian Government resources (people, information and assets).

Services Australia response: *Agreed.*

4.65 Services Australia will review and strengthen its monitoring and assurance arrangements for key physical security controls that seek to protect agency and Australian Government resources (people, information and assets).

Certification of physical security

4.66 Certification of physical security establishes a facility's compliance with the minimum physical security requirements to the satisfaction of the relevant certification authority. In Services Australia's circumstances, the Chief Security Officer (CSO) or security advisor can certify that the control elements have been implemented and are operating effectively. Certification is time-limited and specific to the facility and assets within the facility at the time of certification.

4.67 Services Australia's physical security policy did not specifically address certification until February 2021. The subsequent policy stated that the relevant delegate must certify facilities before they are used operationally, to establish compliance with the minimum physical security requirements.

4.68 Half the necessary certifications were completed for two of six facilities visited by the ANAO. Two of the four zone certifications at two facilities were completed during the audit. For the other four facilities, the entity advised the ANAO that the sites were certified and accredited under the 'Agency Security Plan 2014–16', using a process which incorporated the site security review process. While accreditation documentation was included in the site security reviews, no explicit reference to certification was included. Services Australia has reported to AGD that a review of physical and administrative arrangements, as well as certification of operational Zone 3 areas, is due for completion in July 2022.

Accreditation of security zones

4.69 Security zone accreditation involves compiling and reviewing all applicable certifications and other deliverables for a zone to determine and accept residual security risks. In February 2021, Services Australia implemented an accreditation process in its new Physical Security Policy. The policy states that the CSO has delegated authority to the agency Deputy CSO – security advisor physical security and personnel security to certify and accredit most of the agency’s areas.

4.70 Accreditations were completed as required for two facilities, and partially completed as required under the Agency Security Plan 2014–16 for four facilities visited by the ANAO. Available accreditation certificates for two sites do not contain a statement to indicate that all applicable certifications were reviewed before the relevant officer accepted the residual security risk. Services Australia was not able to provide evidence of explicit consideration and acceptance of residual risk.

Grant Hehir

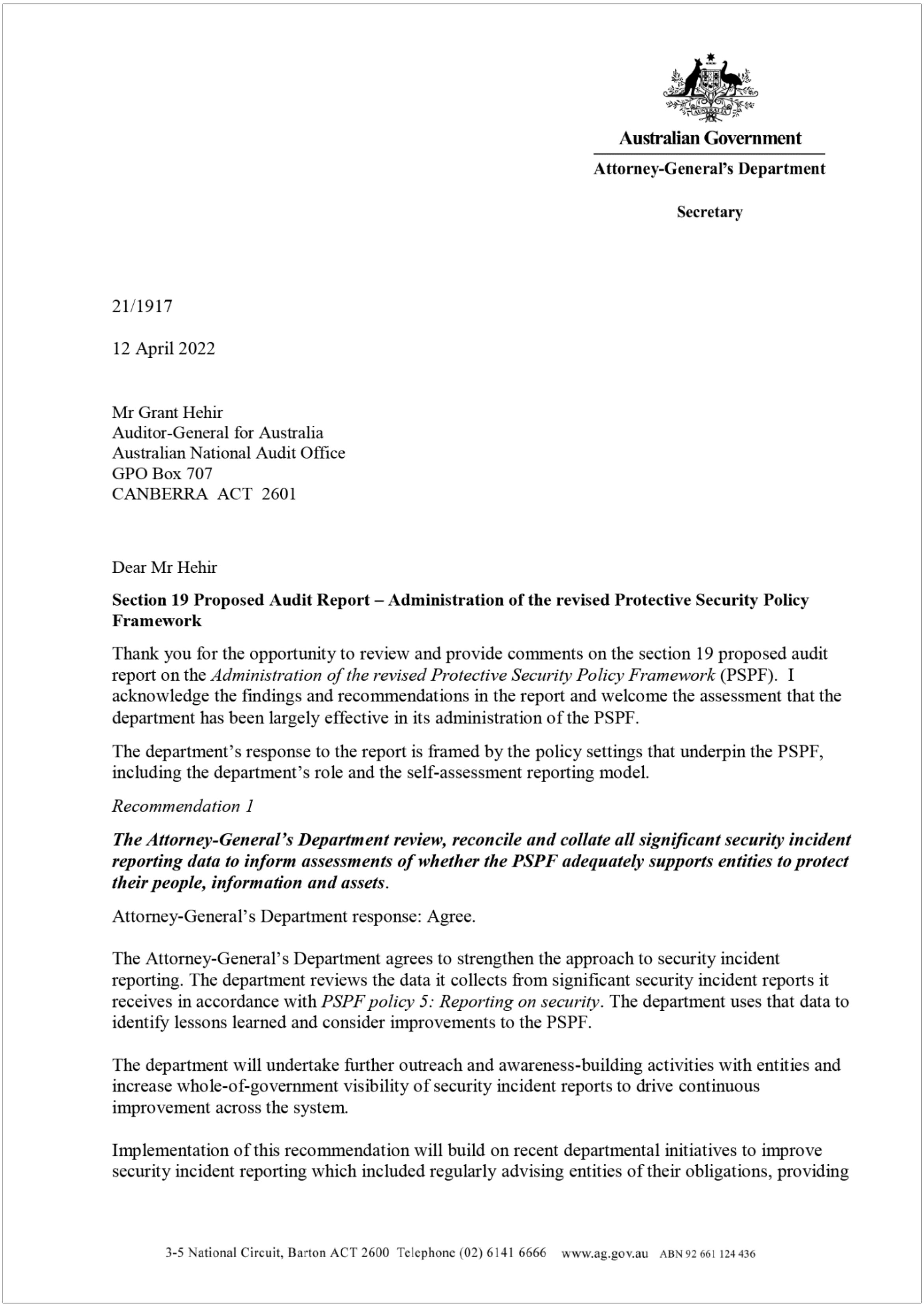
Grant Hehir
Auditor-General

Canberra ACT
12 May 2022

Appendices

Appendix 1 Entity responses

Attorney-General’s Department



Australian Government

Attorney-General’s Department

Secretary

21/1917

12 April 2022

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

Dear Mr Hehir

Section 19 Proposed Audit Report – Administration of the revised Protective Security Policy Framework

Thank you for the opportunity to review and provide comments on the section 19 proposed audit report on the *Administration of the revised Protective Security Policy Framework* (PSPF). I acknowledge the findings and recommendations in the report and welcome the assessment that the department has been largely effective in its administration of the PSPF.

The department’s response to the report is framed by the policy settings that underpin the PSPF, including the department’s role and the self-assessment reporting model.

Recommendation 1

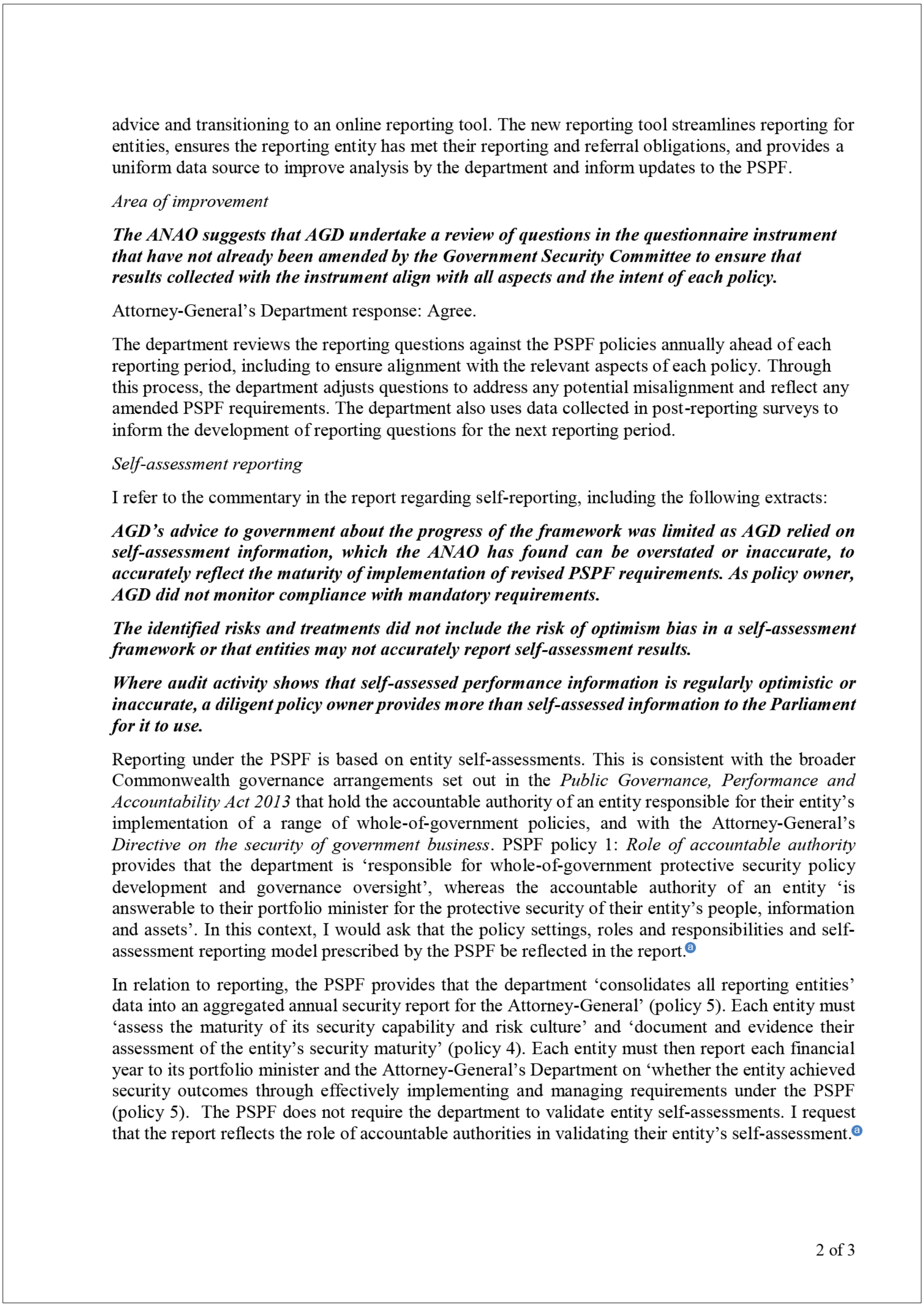
The Attorney-General’s Department review, reconcile and collate all significant security incident reporting data to inform assessments of whether the PSPF adequately supports entities to protect their people, information and assets.

Attorney-General’s Department response: Agree.

The Attorney-General’s Department agrees to strengthen the approach to security incident reporting. The department reviews the data it collects from significant security incident reports it receives in accordance with *PSPF policy 5: Reporting on security*. The department uses that data to identify lessons learned and consider improvements to the PSPF.

The department will undertake further outreach and awareness-building activities with entities and increase whole-of-government visibility of security incident reports to drive continuous improvement across the system.

Implementation of this recommendation will build on recent departmental initiatives to improve security incident reporting which included regularly advising entities of their obligations, providing



advice and transitioning to an online reporting tool. The new reporting tool streamlines reporting for entities, ensures the reporting entity has met their reporting and referral obligations, and provides a uniform data source to improve analysis by the department and inform updates to the PSPF.

Area of improvement

The ANAO suggests that AGD undertake a review of questions in the questionnaire instrument that have not already been amended by the Government Security Committee to ensure that results collected with the instrument align with all aspects and the intent of each policy.

Attorney-General's Department response: Agree.

The department reviews the reporting questions against the PSPF policies annually ahead of each reporting period, including to ensure alignment with the relevant aspects of each policy. Through this process, the department adjusts questions to address any potential misalignment and reflect any amended PSPF requirements. The department also uses data collected in post-reporting surveys to inform the development of reporting questions for the next reporting period.

Self-assessment reporting

I refer to the commentary in the report regarding self-reporting, including the following extracts:

AGD's advice to government about the progress of the framework was limited as AGD relied on self-assessment information, which the ANAO has found can be overstated or inaccurate, to accurately reflect the maturity of implementation of revised PSPF requirements. As policy owner, AGD did not monitor compliance with mandatory requirements.

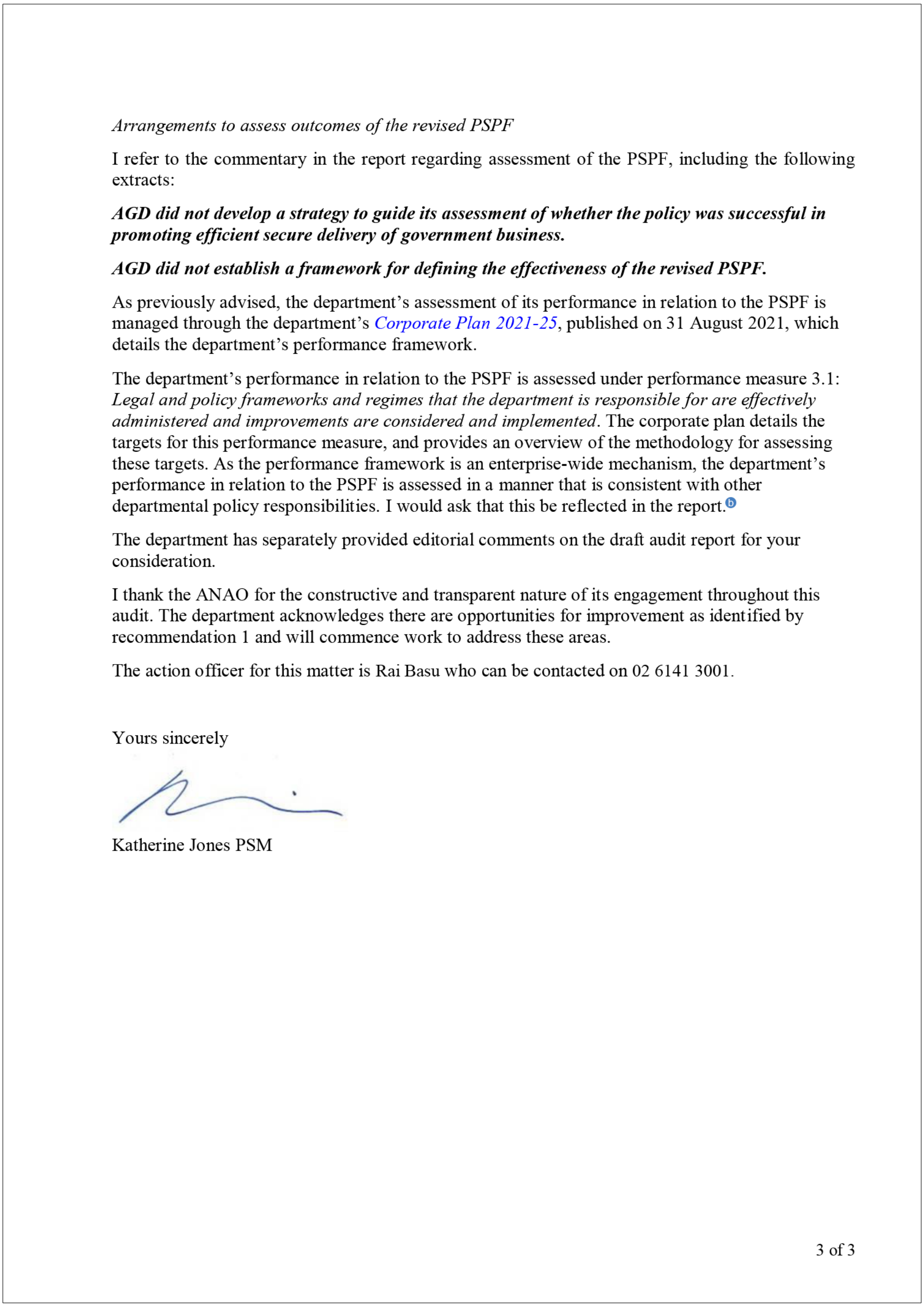
The identified risks and treatments did not include the risk of optimism bias in a self-assessment framework or that entities may not accurately report self-assessment results.

Where audit activity shows that self-assessed performance information is regularly optimistic or inaccurate, a diligent policy owner provides more than self-assessed information to the Parliament for it to use.

Reporting under the PSPF is based on entity self-assessments. This is consistent with the broader Commonwealth governance arrangements set out in the *Public Governance, Performance and Accountability Act 2013* that hold the accountable authority of an entity responsible for their entity's implementation of a range of whole-of-government policies, and with the Attorney-General's *Directive on the security of government business*. PSPF policy 1: *Role of accountable authority* provides that the department is 'responsible for whole-of-government protective security policy development and governance oversight', whereas the accountable authority of an entity 'is answerable to their portfolio minister for the protective security of their entity's people, information and assets'. In this context, I would ask that the policy settings, roles and responsibilities and self-assessment reporting model prescribed by the PSPF be reflected in the report.[a]

In relation to reporting, the PSPF provides that the department 'consolidates all reporting entities' data into an aggregated annual security report for the Attorney-General' (policy 5). Each entity must 'assess the maturity of its security capability and risk culture' and 'document and evidence their assessment of the entity's security maturity' (policy 4). Each entity must then report each financial year to its portfolio minister and the Attorney-General's Department on 'whether the entity achieved security outcomes through effectively implementing and managing requirements under the PSPF (policy 5). The PSPF does not require the department to validate entity self-assessments. I request that the report reflects the role of accountable authorities in validating their entity's self-assessment.[a]

2 of 3



Arrangements to assess outcomes of the revised PSPF

I refer to the commentary in the report regarding assessment of the PSPF, including the following extracts:

AGD did not develop a strategy to guide its assessment of whether the policy was successful in promoting efficient secure delivery of government business.

AGD did not establish a framework for defining the effectiveness of the revised PSPF.

As previously advised, the department's assessment of its performance in relation to the PSPF is managed through the department's *Corporate Plan 2021-25*, published on 31 August 2021, which details the department's performance framework.

The department's performance in relation to the PSPF is assessed under performance measure 3.1: *Legal and policy frameworks and regimes that the department is responsible for are effectively administered and improvements are considered and implemented*. The corporate plan details the targets for this performance measure, and provides an overview of the methodology for assessing these targets. As the performance framework is an enterprise-wide mechanism, the department's performance in relation to the PSPF is assessed in a manner that is consistent with other departmental policy responsibilities. I would ask that this be reflected in the report.[b]

The department has separately provided editorial comments on the draft audit report for your consideration.

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 recommendation 1 and will commence work to address these areas.

The action officer for this matter is Rai Basu who can be contacted on 02 6141 3001.

Yours sincerely

Katherine Jones PSM

3 of 3

ANAO Comment on the Attorney-General's Department response

(a) *Self-assessment reporting*.

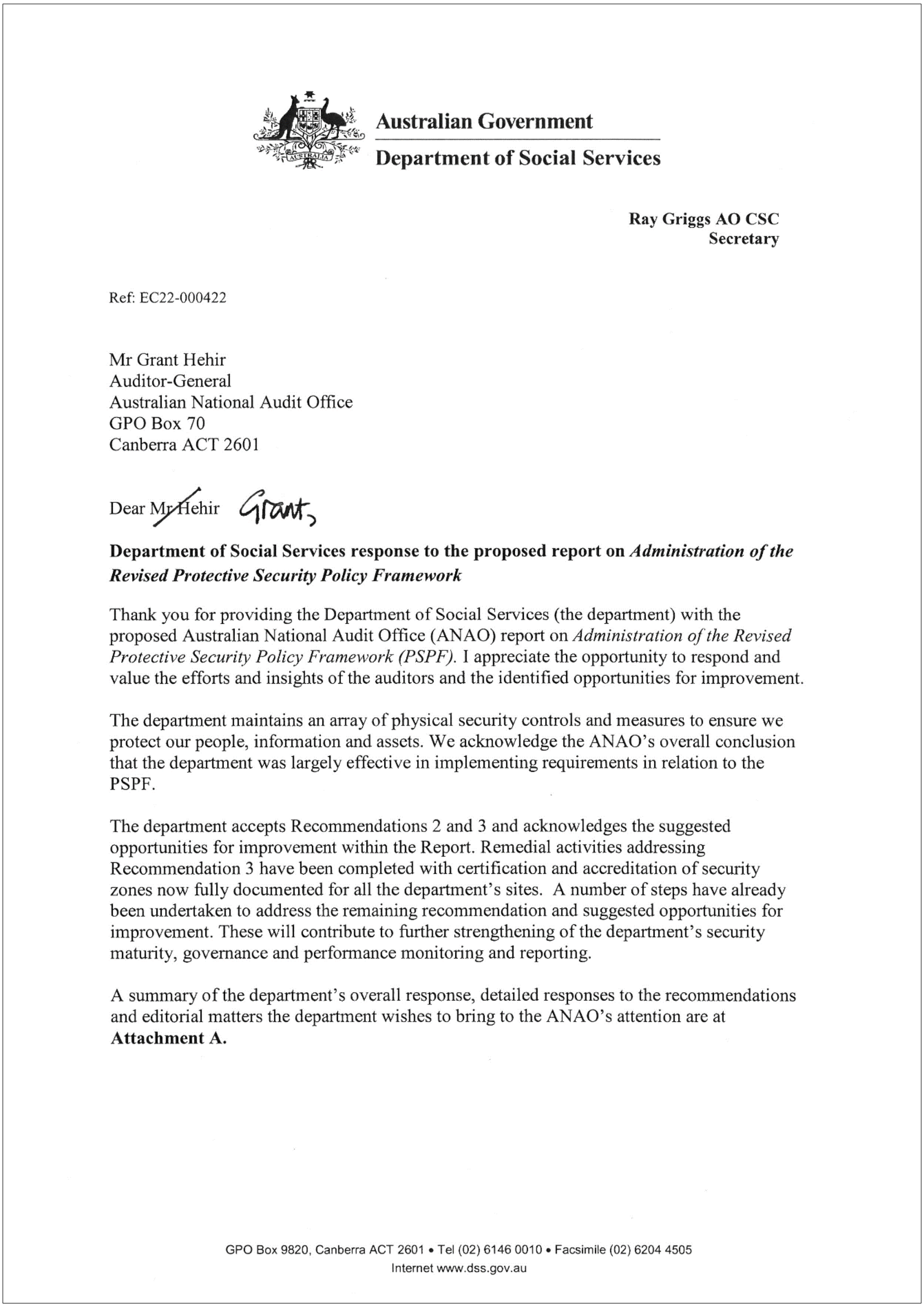
As discussed in paragraph 1.17, this audit provides assurance about whether AGD is fostering the intended strong security culture through strategic, diligent, and risk-based administration of the PSPF, including by assessing the accuracy of self-reporting of physical policies by two entities. See paragraphs 1.7, 2.1 to 2.7, and 2.10 to 2.16 for the relevant PSPF policy settings and roles and responsibilities. See paragraphs 2.49 to 2.61 for the self-assessment reporting model.

As concluded in the summary box on page 23 of the report, in the context of indications that self-assessment information may not be accurate, including discrepancies in the reporting of significant security incidents, the use of self-assessment information to assess the effectiveness of the PSPF is limited. See paragraphs 2.30 to 2.34.

(b) *Arrangements to assess outcomes of the revised PSPF.*

The ANAO acknowledges the AGD's Corporate Plan 2021–25, published on 31 August 2021. The corporate plan was published in the closing stages of audit fieldwork and does not apply retrospectively to the arrangements examined in the report, which began with the implementation of the revised PSPF in October 2018. See paragraphs 2.10 to 2.15 for AGD's previous Corporate Plans.

Department of Social Services



Australian Government

Department of Social Services

Ray Griggs AO CSC
Secretary

Ref: EC22-000422

Mr Grant Hehir
Auditor-General
Australian National Audit Office
GPO Box 70
Canberra ACT 2601

Dear ~~Mr Hehir~~ Grant,

Department of Social Services response to the proposed report on *Administration of the Revised Protective Security Policy Framework*

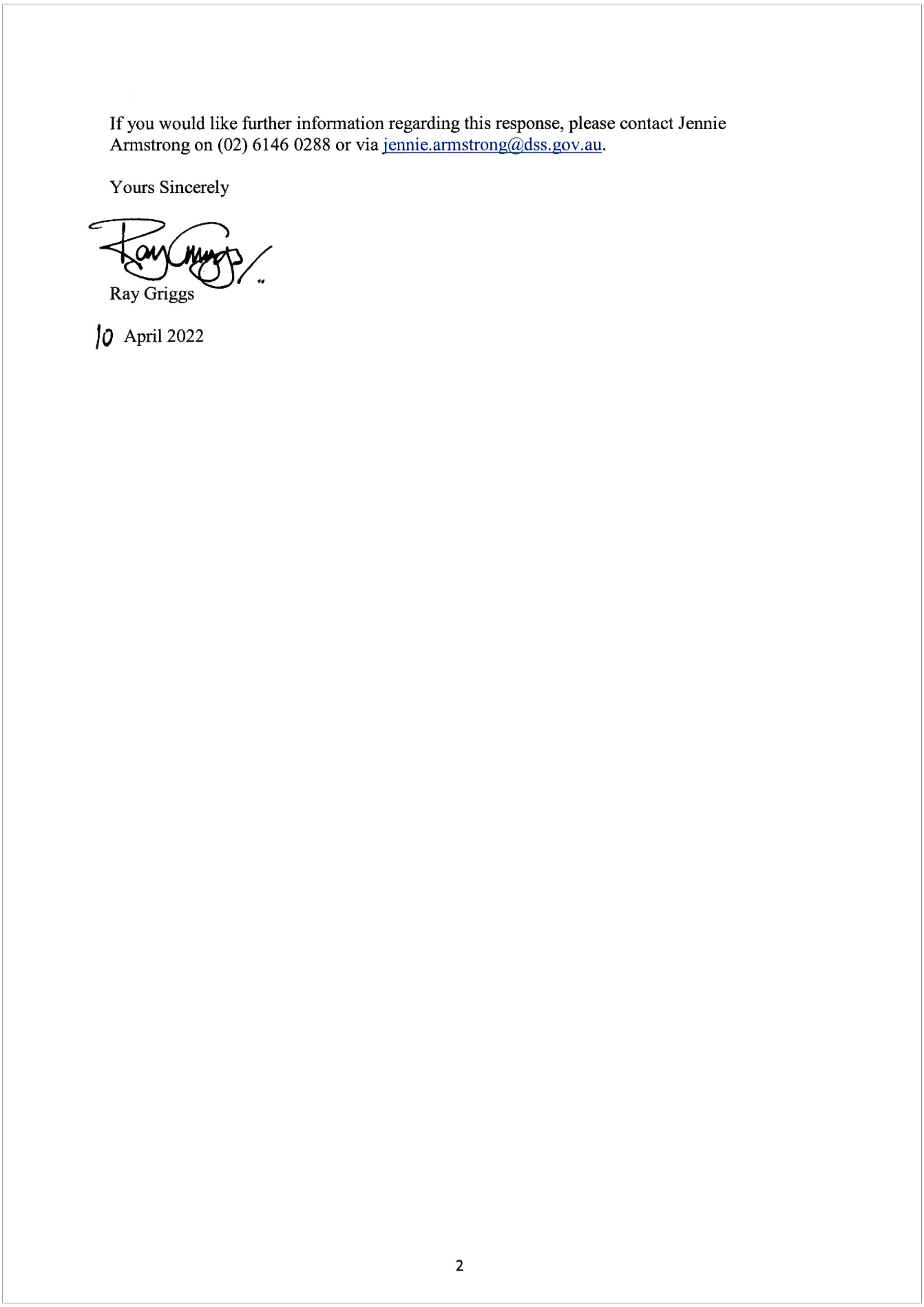
Thank you for providing the Department of Social Services (the department) with the proposed Australian National Audit Office (ANAO) report on *Administration of the Revised Protective Security Policy Framework (PSPF).* I appreciate the opportunity to respond and value the efforts and insights of the auditors and the identified opportunities for improvement.

The department maintains an array of physical security controls and measures to ensure we protect our people, information and assets. We acknowledge the ANAO's overall conclusion that the department was largely effective in implementing requirements in relation to the PSPF.

The department accepts Recommendations 2 and 3 and acknowledges the suggested opportunities for improvement within the Report. Remedial activities addressing Recommendation 3 have been completed with certification and accreditation of security zones now fully documented for all the department's sites. A number of steps have already been undertaken to address the remaining recommendation and suggested opportunities for improvement. These will contribute to further strengthening of the department's security maturity, governance and performance monitoring and reporting.

A summary of the department's overall response, detailed responses to the recommendations and editorial matters the department wishes to bring to the ANAO's attention are at **Attachment A.**

GPO Box 9820, Canberra ACT 2601 • Tel (02) 6146 0010 • Facsimile (02) 6204 4505
Internet www.dss.gov.au



If you would like further information regarding this response, please contact Jennie Armstrong on (02) 6146 0288 or via jennie.armstrong@dss.gov.au.

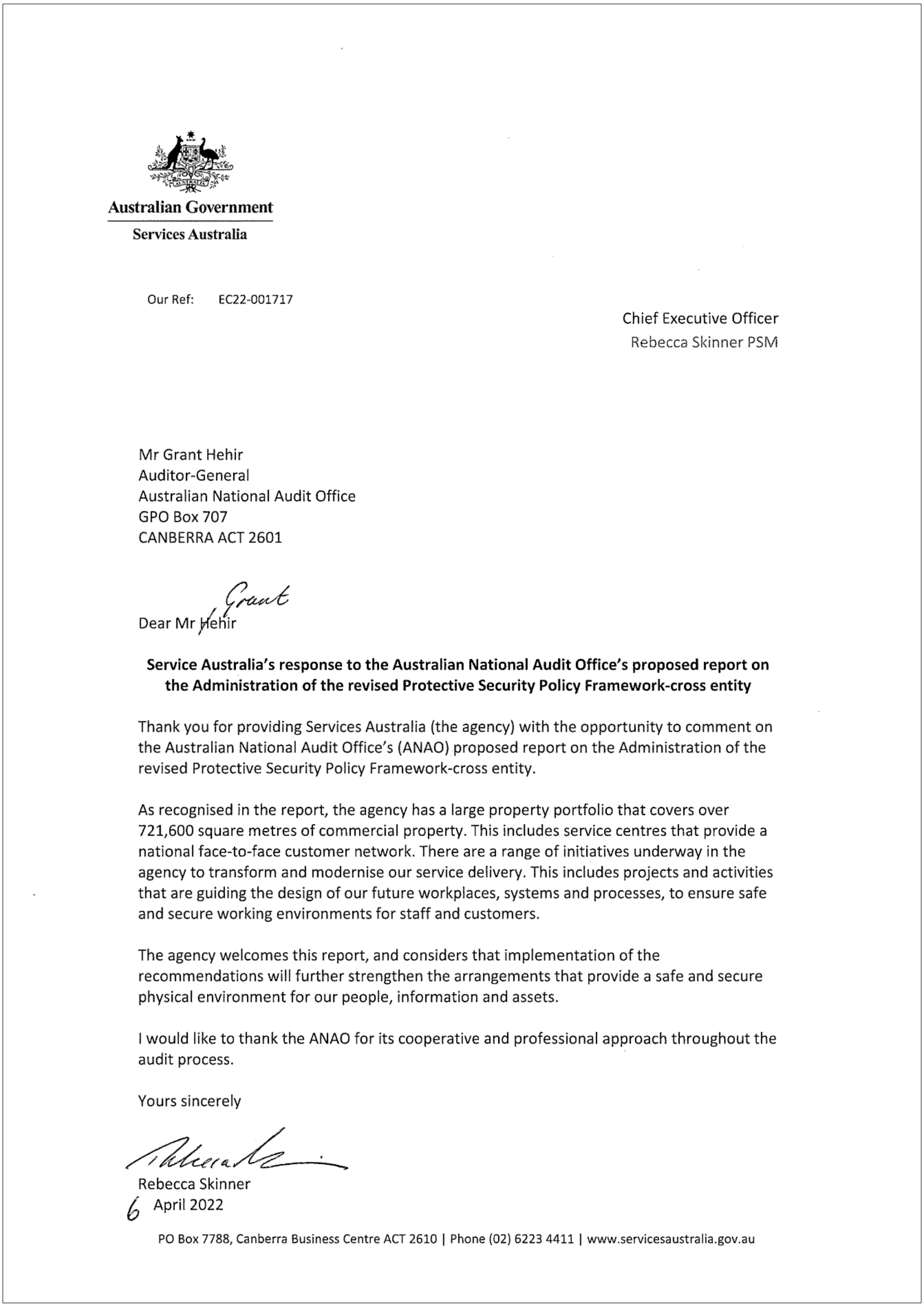
Yours Sincerely

Ray Griggs

Ray Griggs

10 April 2022

Services Australia



Australian Government

Services Australia

Our Ref: EC22-001717

Chief Executive Officer
Rebecca Skinner PSM

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

Dear Mr ~~Hehir~~ Grant

Service Australia's response to the Australian National Audit Office's proposed report on the Administration of the revised Protective Security Policy Framework-cross entity

Thank you for providing Services Australia (the agency) with the opportunity to comment on the Australian National Audit Office's (ANAO) proposed report on the Administration of the revised Protective Security Policy Framework-cross entity.

As recognised in the report, the agency has a large property portfolio that covers over 721,600 square metres of commercial property. This includes service centres that provide a national face-to-face customer network. There are a range of initiatives underway in the agency to transform and modernise our service delivery. This includes projects and activities that are guiding the design of our future workplaces, systems and processes, to ensure safe and secure working environments for staff and customers.

The agency welcomes this report, and considers that implementation of the recommendations will further strengthen the arrangements that provide a safe and secure physical environment for our people, information and assets.

I would like to thank the ANAO for its cooperative and professional approach throughout the audit process.

Yours sincerely

Rebecca Skinner
6 April 2022

PO Box 7788, Canberra Business Centre ACT 2610 | Phone (02) 6223 4411 | www.servicesaustralia.gov.au

Appendix 2 Improvements observed by the ANAO

1. The existence of independent external audit, and the accompanying potential for scrutiny improves performance. Improvements in administrative and management practices usually occur in anticipation of ANAO audit activity; during an audit engagement; as interim findings are made; and/or after the audit has been completed and formal findings are communicated.

2. The Joint Committee of Public Accounts and Audit has encouraged the ANAO to consider ways in which the ANAO could capture and describe some of these impacts. The ANAO's 2021–22 Corporate Plan states that the ANAO's annual performance statements will provide a narrative that will consider, amongst other matters, analysis of key improvements made by entities during a performance audit process based on information included in tabled performance audit reports.

3. Performance audits involve close engagement between the ANAO and the audited entity as well as other stakeholders involved in the program or activity being audited. Throughout the audit engagement, the ANAO outlines to the entity the preliminary audit findings, conclusions and potential audit recommendations. This ensures that final recommendations are appropriately targeted and encourages entities to take early remedial action on any identified matters during the course of an audit. Remedial actions entities may take during the audit include:

- strengthening governance arrangements;
- introducing or revising policies, strategies, guidelines or administrative processes; and
- initiating reviews or investigations.

4. In this context, the below actions were observed by the ANAO during the course of the audit. It is not clear whether these actions and/or the timing of these actions were planned in response to proposed or actual audit activity. The ANAO has not sought to obtain assurance over the source of these actions or whether they have been appropriately implemented.

Improvements observed in AGD

- Proposal to the Government Security Committee in November 2021 that AGD develop additional reporting guidance and a best practice evidence guide ahead of the 2021–22 reporting period.
- Resumption in November 2021 of virtual Chief Security Officer Forums after a pause during the COVID-19 pandemic period.
- Progress of work to amend the core requirement of policy 10 to implement the Essential Eight to commence from 1 July 2022.
- Progress of work to update the Secure Internet Gateway requirement and associated guidance within policy 11 of the PSPF, to align with the work being undertaken by the Hardening Government IT initiative.
- Publication of amendments to PSPF policy 12 on 30 November 2021, PSPF policy 8 on 15 November 2021, and PSPF policies 12, 13 and 14 on 2 August 2021.

Improvements observed in DSS

- Amendment of the zone assessment tool to explicitly capture the delegated authority's acknowledgment that sufficient treatments and controls are in place to determine and accept residual risk.
- Resumption of site risk assessments. DSS had conducted a site risk assessment where it had 15 staff co-locating with Services Australia and other agencies.
- Planning and quotes for the installation of CCTV at DSS' partially controlled sites and co-location sites by April 2022. This includes installation of CCTV at the base of the building, as well as on floors where DSS staff are located.

Improvements observed in Services Australia

- Updates to physical security policies and procedures on Services Australia intranet.
- Extraction and review of alarm and building access data for Services Australia to gain assurance over control measures.
- Consideration of a learning academy or security faculty to teach entity staff about security matters.
- Commencement or re-commencement of certification and accreditation process.
- Asset stocktakes for physical security policy purposes.
- Planning for an internal audit on the veracity of PSPF self-assessment reports.