The Auditor-General
Auditor-General Report No.38 2025–26
Performance Audit

Management of Cyber Security in the Department of Parliamentary Services

Department of Parliamentary Services

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76192-033-2 (Print)
ISBN 978-1-76192-034-9 (Online)

Chief Operating Officer
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

11 June 2026

Dear 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 Department of Parliamentary Services. The report is titled *Management of Cyber Security in the Department of Parliamentary Services.* 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

Dr Caralee McLiesh PSM
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 their 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

Ben Siddans
Edwin Apoderado
Jay Banpel
Kelvin Le
Adam Reddiex
Jane Wiles
Lesa Craswell

Contents

Audit snapshot

Auditor-General Report No.38 2025–26

Management of Cyber Security in the Department of Parliamentary Services

Why did we do this audit?

- The Department of Parliamentary Services (DPS) provides essential services to the Australian Parliament. In 2019 DPS was subject to a high-profile cyber security incident, and cyber security remains a top priority for the department.
- DPS provides IT services to users with differing business and security needs.
- This audit provides independent assurance to the Parliament on whether DPS has an effective baseline of cyber security strategies to mitigate cyber security risks.

Key facts

- The 'Essential Eight' are key cyber security strategies non-corporate Commonwealth entities must implement to a required standard under the Protective Security Policy Framework.
- The Essential Eight are the measures that the Australian Signals Directorate considers most effective for entities to mitigate key cyber security risks.

What did we find?

- At the time of the audit, DPS had a partly effective baseline of essential cyber security strategies.
- Governance processes for cyber security were established but risk assessment, acceptance and communication were of limited effectiveness.
- The Essential Eight cyber security strategies were not fully implemented in accordance with the requirements of the Protective Security Policy Framework.
- The department was relying on compensating controls without adequate coverage of all systems and risk management of identified vulnerabilities.
- DPS had an outdated policy framework and shortcomings in tracking and assessing areas for improvement. It had limited ability to apply controls and governance for some of the users it supports.

What did we recommend?

- The ANAO made two recommendations to improve governance arrangements, and prioritise and implement measures to address known cyber security risks.
- DPS agreed to all recommendations.

4,817

users of IT services provided by DPS.

10,951

end-user devices managed by DPS.

7

Essential Eight strategies that DPS implemented below the standard required.

Summary and recommendations

Background

1. The Department of Parliamentary Services (DPS) is responsible for implementing cyber security strategies critical for safeguarding Information and Communications Technology (ICT) services across Parliament House. The scale of operations at the Parliament requires robust governance and controls to protect parliamentarians, staff, and partner entities.

2. The Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) establish a framework of mandatory security standards and maturity requirements for government entities.[1] They provide technical guidance and prioritised controls to help government entities strengthen their cyber defences. Non-corporate Commonwealth entities such as DPS are subject to PSPF requirements. The DPS Security Plan 2025–27 states that the department's protective security must be applied in alignment with PSPF requirements.

3. This audit examined whether DPS has an effective baseline of cyber security strategies to mitigate cyber security risks affecting the Parliamentary Computing Network and other ICT services.

Rationale for undertaking the audit

4. The Australian Government's 2023–2030 Cyber Security Strategy identifies cyber security as an urgent and growing national problem and sets the agenda for strengthening national cyber resilience.

5. Previous ANAO cyber-related audits have identified gaps in entity management of essential cyber security controls. With emerging technologies introducing new risks and shifting focus from core controls, ongoing assessment is needed. This audit informs the Parliament about whether DPS has effectively implemented essential cyber security controls.

Audit objective and criteria

6. The objective of the audit was to assess whether the Department of Parliamentary Services has an effective baseline of cyber security controls.

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

- Has the Department appropriately assessed essential cyber security risks?
- Has the Department implemented appropriate essential cyber security controls?
- Does the Department have appropriate assurance as to the effectiveness of their essential cyber security controls?

Information disclosed in this report

8. Independent timely reporting on the implementation of the cyber security policy framework supports public accountability by providing an evidence base for the Parliament to hold the executive government and individual entities to account. Previous ANAO reports on

1 The Department of Home Affairs administers the PSPF, while the Australian Signals Directorate produces the ISM.

cyber security have drawn to the attention of Parliament and relevant entities the need for change in entity implementation of mandatory cyber security requirements, at both the individual entity and framework levels.

9. The extent to which this report details cyber security vulnerabilities was a matter of careful consideration. In preparing audit reports to the Parliament on cyber security in Australian Government entities, the interests of accountability and transparency must be balanced with the need to manage cyber security risks. ASD has advised the ANAO that adversaries use publicly available information about cyber vulnerabilities to more effectively target their malicious activities. In considering the information in this report, the ANAO engaged with ASD to better understand the potential risks that may arise through the disclosure of technical information.

10. This report therefore focuses on matters material to the audit findings against the objective and criteria and contains less detailed technical information. Detailed technical information flowing from the audit was provided to the accountable authority during the audit process to assist them to gain their own assurance that their remediation plans are focused on improving cyber resilience as required and support reliable reporting through the existing cyber security policy framework.

Conclusion

11. The Department of Parliamentary Services had a partly effective baseline of essential cyber security strategies. The Essential Eight cyber security strategies had not been fully implemented in accordance with the requirements of the Protective Security Policy Framework, and compensating controls were not sufficiently effective to mitigate the full extent of risk. The department has identified work to re-assess and re-authorise its ICT environment and in the 2026–27 Budget the department received additional resourcing to deliver necessary enhancements for critical information technology systems.

12. DPS is a service provider to other Parliamentary entities, and Parliamentarians and their staff. The differing business and security requirements of these user groups were not reflected in the department's IT environment. DPS experienced significant turnover in ICT staff in the previous 18 months. Some technology platforms supporting key business functions require risk-managed operation due to lifecycle constraints, and inventories of key information, assets and risks were outdated. Recent self-assessment activities have been evidence-based and embedding these activities could support the department continuing to improve.

Supporting findings

Essential cyber security strategies

13. DPS established enterprise-wide governance arrangements for cyber security. Governance arrangements were weakened because DPS did not have an IT control environment that addressed key risks across all the user groups supported, and because DPS had not completed key cyber security policies. DPS had not completed identification and documentation of key systems and other ICT assets, and did not formally consider if the risk mitigation strategies were appropriate for the threats in their broader strategic environment. DPS accepted risks above tolerance when approving the operation of new technology systems, and systems in active use required re-assessment and approval. (See paragraphs 2.2 to 2.20)

14. The department was relying on risk-management approaches to address the gap between implemented and required controls. For the seven strategies using risk mitigations, these risk-management approaches fell short of the standard required to adequately address the risk. Accordingly, the department had not implemented all essential cyber security strategies to the requirements of Maturity Level Two. (See paragraphs 2.23 to 2.45)

15. DPS had undertaken a range of internal reviews, audits, and other exercises to assess and improve its cyber security posture. The department did not have a single source of truth for identified risks and issues, and available registers were not complete. Limited evidence was available to support previous PSPF self-assessment activities, although the most recent assessment in 2024–25 was supported by testing of controls. (See paragraphs 2.46 to 2.61)

Recommendations

Recommendation no. 1
Paragraph 2.21

The Department of Parliamentary Services should review its governance arrangements and risk assessment processes for cyber security to determine if they remain appropriate to the Department and the Parliament's risk environment and the requirements of the Information Security Manual.

Department of Parliamentary Services response: *Agreed*

Recommendation no. 2
Paragraph 2.62

The Department of Parliamentary Services:

(a) develop a prioritised, risk-based program of uplift activities to address known risks related to essential cyber security strategies, and issues identified through cyber security assurance activities; and

(b) implement the program of uplift activities to achieve compliance with requirements of the Protective Security Policy Framework.

Department of Parliamentary Services response: *Agreed*

Summary of entity response

16. The proposed audit report was provided to DPS. The summary response to the report is below and the full response is at Appendix 1.

Department of Parliamentary Services

The Department of Parliamentary Services (DPS) thanks the Australian National Audit Office (ANAO) for the proposed audit report on the Management of Cyber Security in the Department of Parliamentary Services. The department agrees with all recommendations in the proposed report and will undertake the following to support addressing the recommendations.

In December 2025, DPS commenced a comprehensive review of its cyber security governance and risk assessment processes, guided by the DPS Risk Management Policy and Framework and informed by the ANAO audit. The review will assess existing arrangements to ensure they are fit for purpose and scalable to meet the Parliament's evolving cyber security environment. The

review will include identifying governance and assurance activities to be uplifted that will support mitigating cyber security risks in the Parliamentary Computing Network (PCN).

DPS is committed to working collaboratively with partners to align with Australian Government cyber security standards, embedding Information Security Manual controls and improving maturity under the Essential Eight framework. Funding from the 2026–27 Budget will support delivery of a Parliamentary Information and Cyber Resilience project, which will address critical cyber, information security and operational resilience risks in the PCN, strengthening security and resilience of the network.

Key messages from this audit for all Australian Government entities

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

Governance and risk management

- Entities should ensure that the cyber security controls they rely on adequately address the scope of identified risks (or that other mitigating controls address gaps in coverage) and are regularly reassessed to determine their continued effectiveness against current and emerging threats.
- Entities should seek their own assurance over the effectiveness of key cyber security controls. This assurance should consider appropriate sources of evidence that can demonstrate a control is functioning as intended.
- Entities should ensure that policy and procedure documentation remains current and accurately reflects the operating environment and risks being mitigated. Such documentation is critical to maintaining business continuity and managing key personnel risks.

Audit findings

1. Background

Introduction

1.1 In November 2023 the Australian Government released the 2023–2030 Australian Cyber Security Strategy. The minister's foreword identifies cyber security as an 'urgent national problem' that 'touches the lives of every Australian', and declares the government's intention to 'hold itself to the same standard it expects of industry'. The strategy notes the government's appointment of a National Cyber Security Coordinator to lead whole-of-government cyber security uplift.

1.2 The Department of Parliamentary Services (DPS) is a non-corporate Commonwealth entity (NCE) that provides essential services to the Australian Parliament. The DPS Corporate Plan 2025–26 notes that it operates in a 'challenging' security environment and that cyber security is a 'top priority'.[2] In 2019 DPS was subject to a high-profile cyber security incident, and the department regularly monitors and responds to other potential cyber threats.

Protective Security Policy Framework

1.3 The Australian Government Protective Security Policy Framework (PSPF) 'prescribes what Australian Government entities must do to protect their people, information and resources'.[3] The Minister's Directive on the Security of Government Business establishes the PSPF as government policy and directs NCEs subject to the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) to comply with the PSPF.[4] Section 21 of the PGPA Act requires accountable authorities of NCEs to govern the entity in accordance with the PGPA Act in a way that is not inconsistent with the policies of the Australian Government.

1.4 The PSPF is updated annually, with each 'release' providing a list of requirements and a summary of changes made since the previous release. As at March 2026 the most recent release was issued on 24 July 2025.[5] PSPF Release 2025 sets out Australian Government policy across six connecting protective security 'domains' — governance, risk, information, technology, personnel and physical — and prescribes entity responsibilities to meet protection requirements. It also covers principles, policy, standards, and technical manuals and guidelines. Entity application of the PSPF is intended to assure government that protective security practices are sound and that entities can identify and mitigate risks. The technology domain covers technology lifecycle management, cyber security strategies and cyber security programs, with section 14 stipulating cyber security strategy requirements. This audit made assessments based on PSPF Release 2025.

2 Department of Parliamentary Services, *Corporate Plan 2025–2026*, DPS, Canberra, p. 12, 2025, available from https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Department_of_Parliamentary_Services/Publications/Corporate_Plans [accessed 23 February 2026].

3 Department of Home Affairs, *Protective Security Policy Framework*, DHA, Canberra, available from https://www.protectivesecurity.gov.au/about [accessed 5 March 2026].

4 The Directive was issued by the Minister for Home Affairs. The PSPF represents better practice for corporate Commonwealth entities and wholly-owned Commonwealth companies.

5 Department of Home Affairs, *Protective Security Policy Framework: PSPF annual release,* DHA, Canberra, 24 July 2025, available from https://www.protectivesecurity.gov.au/pspf-annual-release [accessed 5 March 2026].

1.5 Under the Administrative Arrangements Orders, of 13 May 2025, the Department of Home Affairs (Home Affairs) is responsible for administering the PSPF and protective security policy.[6] The Australian Signals Directorate (ASD) is responsible for the Information Security Manual (ISM). The ISM sets out the technical controls relevant to cyber security for agencies to implement in applying the PSPF as the overarching policy framework.[7] To help organisations mitigate cyber security incidents, ASD produces the Strategies to Mitigate Cyber Security Incidents. These are prioritised according to effectiveness and those ASD considers most effective are referred to as the Essential Eight (see Table 1.1).[8]

Table 1.1: Essential Eight cyber threat mitigation strategies for entities

Strategy	Summary	Rationale for implementation
Application control	Use application control tools to allow only the execution of explicitly permitted software on workstations and internet-facing servers.	Prevent execution of all non-approved applications (including malicious code).
Patch applications	Patch commonly used applications that may interact with content from the untrusted sources, such as web browsers, office suites, and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Remove outdated software and proactively scan for vulnerable versions.	Prevent malicious actors from using security vulnerabilities in applications to execute malicious code on systems.
Configure Microsoft Office macro settings	Disable macros for users without a business need. Configure Microsoft Office macro settings to block macros from the internet. Allow only those macros that can be confirmed to be trusted, either through digital signatures, or the use of tightly controlled 'trusted locations'. Block the ability of macros to execute other code.	Prevent malicious actors from using Microsoft Office macros to deliver and execute malicious code on systems.
User application hardening	Use a modern web browser and remove Internet Explorer. Disable features of applications such as web browsers and office suites that may pose a security risk. Block and filter potential sources of malicious content from the web.	Applications that interact with internet content are popular ways to deliver and execute malicious code on systems.

6 The Administrative Arrangements Orders are available from the Department of the Prime Minister and Cabinet, at https://www.pmc.gov.au/government/administration/administrative-arrangements-orders [accessed 15 April 2026].

7 The Information Security Manual is 'a cyber security framework that an organisation can apply … to protect their information technology and operational technology systems from cyber threats'.
Australian Signals Directorate, *Information security manual*, ASD, Canberra, March 2026, available from https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism [accessed 20 March 2026].

8 PSPF Release 2025 made minimal changes to Release 2024.
Department of Home Affairs, *PSPF Release 2025 — Summary of Changes*, DHA, Canberra, 24 July 2025, available from https://www.protectivesecurity.gov.au/publications-library/pspf-release-2025-summary-changes [accessed 20 March 2026].

Strategy	Summary	Rationale for implementation
Restrict administrative privileges	Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges, and log and monitor privilege use. Don't use privileged accounts for routine activities and prevent these accounts from accessing the internet, email and similar services.	Administration accounts are the 'keys to the kingdom'. Adversaries may use these accounts to gain full access to information and systems.
Patch operating systems	Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Do not use unsupported versions.	Security vulnerabilities in operating systems can be used to further the compromise of systems.
Multi-factor authentication	Require users to use multi-factor authentication (MFA) for online services (including third-party services), remote access, and system logons. Use phishing-resistant MFA, and log and analyse uses (and attempted uses) of MFA.	Stronger user authentication will make it harder for adversaries to access sensitive information and systems.
Daily backups	Regular backup data, applications and settings with a frequency that is in accordance with business criticality and continuity requirements. Test backups regularly. Control who can access, modify and delete backups.	Regular backups can help to ensure information can be accessed following a cyber security incident (such as a ransomware incident).

Source: ANAO analysis of ASD Essential Eight guidance.

1.6 For each Essential Eight strategy ASD defines implementation maturity levels from zero to three.[9] Since 1 July 2022 the PSPF has required that NCEs entities maintain Maturity Level Two for implementation of each strategy.[10] NCEs must undertake annual PSPF compliance self-assessments against the entire PSPF and report this to their minister and Home Affairs. For the Essential Eight, Home Affairs allows entities to report their implementation of Maturity Level Two requirements as 'fully implemented', 'risk managed' or 'not yet implemented' and to provide commentary (see Table 1.2).[11]

9 ASD provides maturity level comparisons in *Essential Eight maturity model*.
Australian Signals Directorate, *Essential Eight maturity model,* ASD, Canberra, 27 November 2023, Appendix D, available from https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model [accessed 4 March 2026].

10 The Department of Home Affairs has been responsible for the Protective Security Policy Framework since August 2023, when it transferred from the Attorney-General's Department.

11 This is set out in the PSPF guidelines.
Department of Home Affairs, *Australian Government Protective Security Policy Framework release 2025: guidelines*, DHA, Canberra, available from https://www.protectivesecurity.gov.au/pspf-annual-release/pspf-guidelines [accessed 4 March 2026].

Table 1.2: PSPF self-assessment categories

Category	Definition
Fully implemented	The entity has implemented the requirement to the PSPF standard.
Risk managed	The entity has put in place proportional mitigations until it can fully implement the requirement.[a] This category is not intended to be enduring.
Not yet implemented	The entity has not implemented the strategy or suitable mitigations.

Note a: The PSPF Guidelines allow for entities to report as 'risk managed' the implementation of Essential Eight strategies with alternative mitigations that they consider meet or exceed PSPF requirements.

Note: PSPF refers to the Protective Security Policy Framework.

Source: ANAO analysis of PSPF Guidelines. See Department of Home Affairs, *Australian Government Protective Security Policy Framework release 2025: guidelines*, available from https://www.protectivesecurity.gov.au/pspf-annual-release/pspf-guidelines [accessed 4 March 2026].

1.7 The PSPF self-assessment process results in an overall entity score. The scoring approach does not 'penalise' entities for employing a risk-managed approach. Additional information is required to justify the approach.

1.8 Home Affairs does not require entities to provide evidence of their self-assessment or the effectiveness of their PSPF requirement implementation but may seek further information for quality assurance. As at March 2026 DPS had not received a request to provide information for a Home Affairs quality assurance activity.

Department of Parliamentary Services

1.9 DPS is one of four departments that comprise the Australian Parliamentary Service.[12] The DPS Secretary reports to the President of the Senate and the Speaker of the House of Representatives (the Presiding Officers). The DPS Corporate Plan 2025–26 sets out its key activities as:

- support the functioning of the parliament;
- facilitate visitor and community access to Australian Parliament House and the parliamentary process; and
- stewardship of Australian Parliament House.[13]

1.10 DPS provides Information and Communications Technology (ICT) office equipment to its staff inside and outside the Parliament House building as well as to parliamentarians, their electorate office staff and personal staff, and former prime ministers. In addition, it has established memoranda of understanding for provision of ICT services with:

- the Office of the Official Secretary to the Governor-General;
- the Parliamentary Workplace Support Service; and

12 The other three parliamentary departments are the Department of the Senate, the Department of the House of Representatives and the Parliamentary Budget Office.

13 Department of Parliamentary Services, *Corporate Plan 2025–26*, DPS, Canberra, 2025, p. 4, available from https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Department_of_Parliamentary_Services/Publications/Corporate_Plans [accessed 6 May 2026].

- jointly the Department of the Senate, the Department of the House of Representatives and the Parliamentary Budget Office (the parliamentary departments).

1.11 DPS advised the ANAO on 20 April 2026 that its network, and networks it supports under shared services arrangements, support 4,817 users across 10,951 end-user devices. The largest cohort of users are parliamentarians and their staff using the network, with staff of other parliamentary departments also forming a significant user group.

1.12 As discussed in paragraph 1.3, the requirement of NCEs to adhere to the PSPF is established by section 21 of the PGPA Act. The extent to which section 21 applies to parliamentary departments is subject to subsection 9(2) of the *Parliamentary Service Act 1999*, which provides that the Parliamentary Service serves the Parliament independently of the Executive Government of the Commonwealth. The Minister for Home Affairs' foreword to the PSPF directs accountable authorities of NCEs subject to the PGPA to comply with the PSPF, and the DPS Security Plan 2025–2027 states that the department's protective security must be applied in alignment with PSPF requirements. DPS does not have other mechanisms (such as memoranda of understanding or user agreements) for those using its network to agree to comply with PSPF requirements.

1.13 The *Parliamentary Precincts Act 1988* provides that the presiding officers control and manage the parliamentary precincts (all land, structures and works within the circular boundary formed by the retaining wall). The *Parliamentary Service Act 1999* established the Security Management Board to advise the Presiding Officers on Parliament House security, including cyber security. The Security Management Board terms of reference state that it 'provides a formal forum for advice to the Presiding Officers on strategic and operational security matters that affect the control and management of the Parliamentary precincts'. The DPS Secretary is the board chair (appointed by the presiding officers), and the remaining membership comprises Department of the Senate and Department of the House of Representatives SES representatives, and the Australian Federal Police Commissioner.[14]

1.14 In 2022 DPS finalised the Parliament of Australia Cyber Security Strategy 2022–2025.[15] The strategy notes its responsibility for providing a diverse range of services to high-profile stakeholders and that the 'Parliament's status as the operational and symbolic centre of Australian parliamentary democracy raises its profile among malicious cyber actors'.

Rationale for undertaking the audit

1.15 Auditor-General Report No. 39 2024–25 *Interim Report on Key Financial Controls of Major Entities* reviewed entity self-reported PSPF data.[16] Only five of 22 entities (23 per cent) reported all Essential Eight strategies as fully implemented. The Department of Home Affairs 2024–25 PSPF Assessment report summarises results from entities' PSPF self-assessments, with 47 per cent of reporting entities having self-reported fully implementing all requirements associated with essential cyber security strategies and a further 42 per cent self-reporting risk-managed

14 The Security Management Board terms of reference also authorise the attendance of SES employees from Department of the Prime Minister and Cabinet, Department of Finance, Australian Security Intelligence Organisation, Australian Signals Directorate and Department of Home Affairs.

15 In June 2025 the DPS Executive Committee agreed to extend the strategy to 2027.

16 Auditor-General Report No. 39 2024–25 *Interim Report on Key Financial Controls of Major Entities*, ANAO, Canberra, May 2025, available from https://www.anao.gov.au/work/financial-statement-audit/interim-report-key-financial-controls-of-major-entities-2024-25 [accessed 5 May 2026].

compliance.[17] This audit provides independent assurance to Parliament on whether DPS has an effective baseline of cyber security strategies to mitigate cyber security risks.

Audit approach

Audit objective, criteria and scope

1.16 The objective of the audit was to assess whether the Department of Parliamentary Services has an effective baseline of cyber security strategies.

1.17 To form a conclusion against the objective, the following criteria were adopted:

- Has DPS appropriately assessed essential cyber security risks?
- Has DPS implemented appropriate essential cyber security controls?
- Does DPS have appropriate assurance of the effectiveness of its essential cyber security controls?

Audit methodology

1.18 The audit methodology included:

- reviewing entity documentation such as internal policies and procedures, management reports, self-assessments and assurance activities, committee papers and minutes relevant to the scope of this audit;
- conducting meetings with relevant DPS senior officials and officers involved in the design, implementation and monitoring of cyber security controls; and
- testing the effectiveness of selected controls and technical configuration within the DPS network.

1.19 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately $330,000.

1.20 The team members for this audit were Ben Siddans, Edwin Apoderado, Jay Banpel, Kelvin Le, Adam Reddiex, Jane Wiles and Lesa Craswell.

1.21 The ANAO has co-operative evidence gathering arrangements in operation with entities. On 16 December 2025 the Auditor-General issued DPS with a notice to provide information and produce documents pursuant to section 32 of the *Auditor-General Act 1997*, in order to facilitate timely provision of data given the sensitivities associated with the audit subject matter, and the role of DPS in supporting the work of the Parliament. DPS provided the information and documents requested within the specified time, following receipt of the notice.

17 Department of Home Affairs, *Protective Security Policy Framework Assessment Report 2024–25*, DHA, Canberra, p. 8, available from https://www.protectivesecurity.gov.au/news/pspf-assessment-report-2024-25 [accessed 4 March 2026]

2. Essential Cyber Security Strategies

Areas examined

This chapter examines whether the Department of Parliamentary Services (DPS) has effectively implemented essential cyber security strategies through an appropriate risk-based process, in accordance with the requirements of the Protective Security Policy Framework (PSPF).

Conclusion

The Department of Parliamentary Services has a partly effective baseline of essential cyber security strategies.

DPS has established governance processes for cyber security. The department has previously accepted cyber security risks and relied on mitigating controls which has complicated ongoing risk management, particularly given recent ICT staff turnover. The Essential Eight cyber security strategies have not been fully implemented in accordance with the requirements of the Protective Security Policy Framework, primarily because the department is relying on compensating controls without adequate coverage of all systems and risk management of identified vulnerabilities. DPS' processes for assuring itself that its essential cyber security strategies are working as intended are partly effective due to an outdated policy framework and shortcomings in tracking and assessing areas for improvement. Recent self-assessment activities have been evidence-based and embedding these activities could support the department continuing to improve.

Areas for improvement

The ANAO made two recommendations to DPS: on reviewing governance arrangements and risk assessment processes for cyber security to determine if they remain appropriate, and developing a risk-based program of activities to address cyber security risks.

The ANAO also suggested that DPS could improve its PSPF self-assessment of essential cyber security strategies by strengthening its evidence base for such assessments and ensuring that resulting recommendations are effectively managed.

2.1 As discussed in paragraphs 1.2 and 1.3, non-corporate Commonwealth entities (NCEs) such as the Department of Parliamentary Services are required to apply the PSPF, which includes adhering to the Information Security Manual (ISM). The PSPF and ISM outline a risk-based approach to a cyber security framework that organisations can apply to protect key systems from cyber threats. The ANAO considered the extent to which DPS followed key elements of a risk-based approach to its essential cyber security controls.

Has the Department appropriately assessed essential cyber security risks?

DPS established enterprise-wide governance arrangements for cyber security. Governance arrangements were weakened because DPS did not have an IT control environment that addressed key risks across all the user groups supported, and because DPS had not completed key cyber security policies. DPS had not completed identification and documentation of key systems and other ICT assets, and did not formally consider if the risk mitigation strategies were appropriate for the threats in their broader strategic environment. DPS accepted risks

above tolerance when approving the operation of new technology systems, and systems in active use required re-assessment and approval.

2.2 The first steps in the ISM's risk-based lifecycle approach to cyber security include defining the system to be protected and selecting appropriate controls. While the PSPF requires that entities implement the Essential Eight cyber security strategies to Maturity Level Two[18], entities may decide to implement controls to a higher standard, vary the specifics of the control implementation, or to use other mitigation strategies to achieve the same objective. The Australian Signals Directorate (ASD) provides guidance to entities to inform their implementation of the Essential Eight using a risk-based approach. The ANAO considered whether DPS performed appropriate assessments of risks to inform its posture for essential cyber security controls.

2.3 During the audit, ASD updated the ISM and associated Essential Eight guidance.[19] The ANAO considered the extent to which DPS aligned with overarching principles relevant to ISM principles and the scope of the audit, the result of which are shown in Table 2.1.

Table 2.1: Assessment of DPS' risk assessment processes related to essential cyber security risks

Aspect of assessment	ANAO assessment
Enterprise-wide governance	◕
Identification, documentation and assessment of key systems and requirements	◔
Risk acceptance and communication	◔

Key: ● Effective ◕ Largely effective ◑ Partly effective ◔ Limited effectiveness

Source: ANAO assessment of DPS IT control environment.

Enterprise-wide governance arrangements

2.4 DPS has established a Security Plan, which clearly defines roles and responsibilities related to cyber security, with overall responsibility resting with the Secretary (DPS' Accountable Authority). As the Accountable Authority, the Secretary has responsibilities under the PSPF including (but not limited to) determining tolerance for security risks, managing the security risks of DPS, and adhering to the mandatory directions issued by the Secretary of the Department of Home Affairs to government entities.[20] The Secretary is supported by the Chief Security Officer, the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) — who reports to the CIO.

18 DHA, *Protective Security Policy Framework*, p. 74.

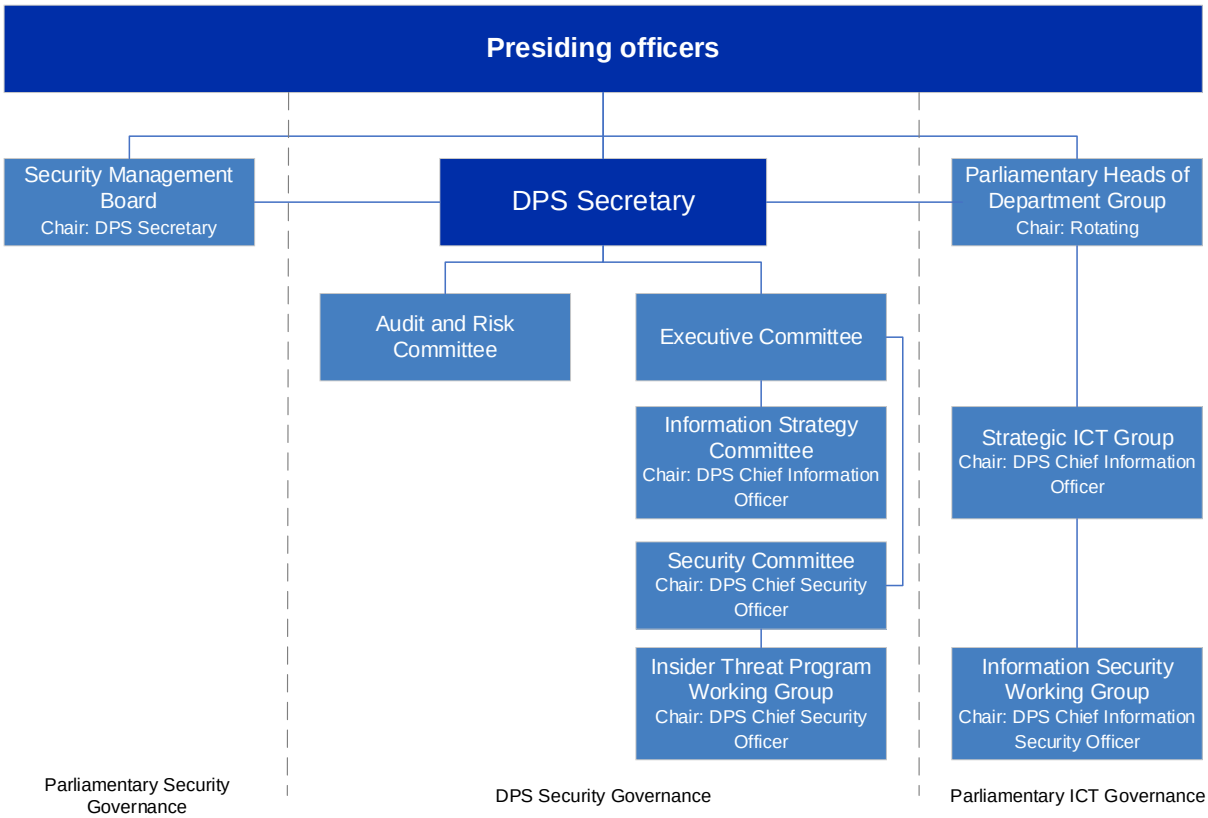
19 The ISM articulates six cyber security principles to provide strategic guidance to organisations on protecting themselves from cyber threats: govern, identify, protect, detect, respond, and recover. The ISM was updated in December 2025 and March 2026, and as part of the March 2026 updates, changes were made to the content and scope of these principles.

20 The PSPF provides that the Secretary of the Department of Home Affairs may issue a direction to accountable authorities to manage a protective security risk to the Australian Government.
Department of Home Affairs, *Protective Security Directions under the PSPF,* DHA, Canberra, available from: https://www.protectivesecurity.gov.au/protective-security-directions-under-pspf [accessed 15 April 2026]

2.5 The Security Plan defines a risk tolerance relating to cyber security and describes the circumstances in which DPS may adjust its tolerance in order to balance other imperatives. The Security Plan also assesses key security threats, and identifies strategic and business risks that are mapped to DPS' enterprise risks. DPS advised the ANAO on 3 March 2026 that it was unable to provide evidence of the process by which it had assessed the severity of these risks, or monitored them on an ongoing basis. While the PSPF requires entities achieve Maturity Level Two for the Essential Eight strategies as a minimum requirement, limited documentation was available to describe the process by which the department considered if other maturity levels may be required for its risk environment.

2.6 DPS has a Security Committee which is the body responsible for the oversight and management of protective security and security risk, including cyber security matters. The Security Committee meets quarterly and reports to the Executive Committee. As discussed in paragraph 1.13, the Security Management Board advises the Presiding Officers on Parliament House security, including cyber security. The Parliamentary Heads of Department Group is chaired on a rotating basis by the heads of each parliamentary department and receives advice on strategic ICT matters including those related to cyber security. The relationship between key cyber security governance committees is outlined in Figure 2.1.

Figure 2.1: Key DPS governance committees relevant to cyber security



Source: ANAO analysis of DPS governance arrangements.

2.7 Key policies relating to the management of cyber security risks are incomplete and/or not endorsed by the Security Committee and have not been implemented (security policies are discussed further in 2.48).

2.8 The ISM specifies requirements for reporting and coordination of cyber security. The ISM requires that the CISO report directly to the executive committee, and audit and risk committee on cyber security, a function performed by the DPS CIO.[21] ISM control 0725 requires that the CISO coordinate cyber security and business alignment through a cyber security steering committee or advisory board, which meets formally on a regular basis. While the Information Security Working Group serves this purpose, the group had not met within a 12-month period examined by the audit.

Parliament and parliamentary departments

2.9 As discussed in paragraphs 1.9 to 1.14, DPS operates in an environment in which the majority of the users of its network are not its own staff, and are subject to varying legislative and policy requirements regarding cyber security. The DPS network does not provide separate governance arrangements or control environments that align with these differing business requirements and risks (discussed further in paragraph 2.39). DPS does not have other mechanisms (such as memoranda of understanding or user agreements) for those using its network to agree to comply with PSPF requirements. As a result, cyber security policy requirements not applied to Parliamentarians or parliamentary departments have also not been applied to DPS staff using the same network.[22] As the Secretary of DPS is responsible for ensuring that DPS staff adhere to the PSPF per the direction from the Minister (see paragraph 1.12), this may expose the department to risk.

2.10 DPS provides shared ICT services to other parliamentary departments, which are defined in a series of memoranda of understanding (MoUs). The MoUs describe a Parliamentary ICT Governance Framework that includes the following means by which shared cyber security risks are managed:

- the DPS CIO who represents the interests of parliamentary departments in the Executive Committee;
- the Strategic ICT Group which has members from the senior executive of the parliamentary departments including DPS CIO, the chair. The Group is described as 'the premier body for the escalation of and consideration of ICT issues that impact the parliamentary departments' and reports to the Parliamentary Heads of Department Group; and
- the Information Security Working Group which brings together representatives from all parliamentary departments at an operational level to discuss and review shared security risks, security incidents and escalate security issues to the Strategic ICT Group as necessary. The Working Group terms of reference set out that it will meet every two months from February to November, however as discussed in paragraph 2.8 this Working Group had not met within a 12-month period.

2.11 Regular review of governance arrangements, such as the role of committees and the frequency of their engagement, can assist entities in determining if they remain appropriate.

21 ISM controls 0718 and 1918 require that the CISO reports directly to the organisation's executive committee or board of directors, and audit and risk committee respectively.

22 For example, ISM control 1865 requires that personnel agree to abide by system usage policies before being granted access to systems and their resources. DPS does not currently enforce a requirement for personnel using their network to agree to such policies as they are not applicable to all users.

Resourcing of cyber security

2.12 As discussed in paragraph 2.4, DPS has appointed staff to key cyber security roles, including those required by the ISM. DPS' CIO is a senior executive reporting to the Deputy Secretary and leads Information Services Division (ISD). Within ISD, the CISO is a senior executive leading Cyber Security Branch.

2.13 The department has experienced considerable staff movement in recent years, with both the CIO and CISO commencing in their roles in 2025. As of February 2026, 55 per cent of staff in the Cyber Security Branch had been with the department for less than 12 months. Managing significant turnover in key personnel requires effective processes to preserve institutional knowledge (for example, documentation of key systems, and processes for regularly reviewing risks and treatments), and increases risks that key controls and risks may not be managed consistently.

Identification, documentation and assessment of key systems and requirements

2.14 Designing an effective control environment requires an understanding of the systems and risks requiring management. The PSPF requires that:

> A register of the entity's authorised technology systems is developed, implemented and maintained, and includes the name and position of the Authorising Officer, system owner, date of authorisation, and any decisions to accept residual security risks.[23]

2.15 DPS' registers relating to key systems and information assets are incomplete and not current. The business criticality of key systems is not consistently documented, and there is no central list of critical systems, with available lists having incomplete risk assessments for some systems. DPS did not have processes to assure itself that these registers were complete and accurate or regularly updated.

2.16 As discussed in paragraph 2.8, the ISM specifies controls for ensuring the coordination of cyber security and business objectives. An understanding of the business criticality of systems is important in designing a proportionate control environment, and in understanding the potential impact of an issue affecting the confidentiality, availability or integrity of a system. DPS' incomplete registers of systems, and associated risk assessments, limit its ability to demonstrate that it has appropriately considered and addressed the business criticality of the systems it maintains, and has designed risk treatments appropriate for these. DPS' registers and risk assessments also make limited mention of factors unique to its operating environment, such as the interaction with the other parliamentary departments and as a result, the potential presence of information that may be considered to be subject to parliamentary privilege.

2.17 The department's incomplete documented understanding of its operating environment limits its ability to effectively assess risks associated with key systems and information.

Security risk acceptance and communication

2.18 The PSPF requires that entities approve all technology systems prior to use in the entity.[24] The approval process provides an opportunity for entities to consider cyber security risks and design

23 DHA, *Protective Security Policy Framework: PSPF annual release*, p. 64, Requirement 0089.

24 ibid., Requirement 0086.

and implement essential cyber security strategies appropriate to address these risks, and ensure that these are communicated and understood.

2.19 DPS conducts risk assessments in relation to authorising new technology systems and for vulnerabilities that cannot be easily patched.[25] As discussed in paragraph 2.15 DPS has not completed risk assessments for all systems. The ANAO observed that some risk assessments were not completed in a timely manner and resulted in the department accepting risks above its tolerance. Case Study 1 provides an example of an instance in which earlier consideration of security risks could have provided DPS with opportunities to avoid accepting high levels of risk.

Case study 1. Security risk acceptance for a new DPS system

In May 2024 DPS initiated a project to replace a key business system. Due to the nature of the system timely replacement was critical and cyber security was also of considerable importance. The system was scheduled to enter operation in August 2024.

The original project proposal did not include a milestone for a security assessment. The project took longer than anticipated and a proposal to extend timeframes was provided to the Executive Committee in June 2025. DPS identified at this stage that key cyber security design and risk assessment work previously reported as completed had not been completed.

The Executive Committee was advised that further delaying the new system would itself create risk due to the need to replace the end-of-life predecessor system. In November 2025 an interim approval to operate was granted by the CIO, which a security assessment identifying a high level of residual risk, including risks to the system's compliance with elements of the Essential Eight.

The approval noted an intent to reduce the level of risk over the next 6 months. Earlier identification of potential security issues, through a timely security design and risk assessment, may have provided opportunities for the department to mitigate risks before the system was deployed.

2.20 Where the department has accepted risks above tolerance, it has relied on treatment plans to manage these risks and bring them into compliance. DPS' processes for managing risks and issues have shortcomings (discussed further in paragraph 2.57) and the treatment plans are not regularly reviewed for currency, with several DPS systems operating with expired approvals to operate. Re-approval of existing systems provides an opportunity to confirm that essential cyber security strategies are effective and remain appropriate. DPS advised the ANAO on 27 February 2026 that it is undertaking work to inventory existing system approvals to identify those systems requiring re-assessment.

25 Management of vulnerabilities is discussed further in paragraph 2.41.

Recommendation no. 1

2.21 The Department of Parliamentary Services should review its governance arrangements and risk assessment processes for cyber security to determine if they remain appropriate to the Department and the Parliament's risk environment and the requirements of the Information Security Manual.

Department of Parliamentary Services response: *Agreed*

2.22 *In December 2025 DPS commenced a comprehensive review of its cyber security governance and risk assessment processes, guided by the DPS Risk Management Policy and Framework and informed by the ANAO audit. The review will assess existing arrangements to ensure they are fit for purpose and scalable to meet the Parliament's evolving cyber security risk environment.*

Has the Department implemented appropriate essential cyber security strategies?

The department was relying on risk-management approaches to address the gap between implemented and required controls. For the seven strategies using risk mitigations, these risk-management approaches fell short of the standard required to adequately address the risk. Accordingly, the department had not implemented all essential cyber security strategies to the requirements of Maturity Level Two.

2.23 As discussed in paragraph 1.6, entities are required to annually self-assess the extent to which they have implemented each of the Essential Eight mitigation strategies. In 2024–25, DPS self-assessed that it had implemented all strategies to the standard required by Maturity Level Two, with risk-managed elements for seven of eight strategies. Where an entity is relying on risk-managed elements to achieve a maturity level, it is assessing that deficiencies in selected controls for a given strategy require mitigation through the implementation of additional controls (for example, additional logging and monitoring controls to detect exploitation of control deficiencies).[26]

2.24 The ANAO assessed the extent to which DPS had implemented each Essential Eight mitigation strategy (as described in Table 1.1) and where applicable, associated risk-management approaches.[27] The DPS' self-assessment and the ANAO's assessment are shown below in Table 2.2. DPS was assessed as not meeting Maturity Level Two for seven of eight strategies. The department is relying on risk-management approaches to address the gap between implemented and required controls. For five of eight strategies, these risk-management approaches fell short of the standard required to adequately address risks. The remaining two strategies were assessed as meeting Maturity Level One requirements only.

26 Department of Home Affairs, *Australian Government Protective Security Policy Framework release 2025: guidelines*, DHA, Canberra, available from https://www.protectivesecurity.gov.au/pspf-annual-release/pspf-guidelines [accessed 4 March 2026].

27 The assessment leveraged guidance and technical tools provided by the Australian Signals Directorate. The technical tools are available to NCEs and other entities via the Australian Signals Directorate partner portal.

Table 2.2: DPS and ANAO Essential Eight assessments

Strategy	Department assessment	ANAO assessment
Patch applications	Maturity Level Two (risk managed)	Risk management insufficient for full Maturity Level Two compliance
Patch operating systems	Maturity Level Two (risk managed)	Risk management insufficient for full Maturity Level Two compliance
Multi-factor authentication	Maturity Level Two (risk managed)	Maturity Level One
Restrict administrative privileges	Maturity Level Two (risk managed)	Risk management insufficient for full Maturity Level Two compliance
Application control	Maturity Level Two (risk managed)	Risk management insufficient for full Maturity Level Two compliance
Restrict Microsoft Office macros	Maturity Level Two (fully implemented)	Maturity Level Two
User application hardening	Maturity Level Two (risk managed)	Risk management insufficient for full Maturity Level Two compliance
Regular backups	Maturity Level Two (risk managed)	Maturity Level One

Source: DPS PSPF self-assessment 2024–25 and ANAO assessment of DPS cyber strategies.

2.25 Specific considerations behind the ANAO's assessment for each strategy are discussed further below.

Patch applications and patch operating systems

2.26 DPS self-assessed as risk-managing patching of both applications and operating systems due to the presence of IT systems for which patches are not necessarily available in a timely manner, and for which other controls are required. DPS relies on its vulnerability management process as mitigating control for some systems (see paragraph 2.41).

2.27 DPS' patch management of its modern environment was more robust but could be improved by strengthening compliance monitoring and processes to remediate identified issues.

Multi-factor authentication

2.28 DPS does not have sufficient assurance that its multi-factor authentication arrangements are appropriate for all systems. For some systems, the technical implementation of multi-factor authentication required improvement. Where systems are not adequately covered by multi-factor authentication, systems may be more vulnerable to unauthorised access.

Restrict administrative privileges

2.29 Selected technical controls regarding management of privileged credentials were identified as not being configured. Additionally, as a result of a management-initiated review, and as part of its PSPF self-assessment, DPS identified that:

- selected controls to prevent privileged accounts from undertaking certain non-privileged activities were not in place;
- removal of privileges after a period of inactivity was subject to a manual process; and

- lack of revalidation of privileged access in components of DPS' environment.

2.30 These deficiencies in the privileged user management regime increase the risk that privileged accounts may be used inappropriately.

Application control

2.31 DPS self-assessed its use of application control as 'risk managing' due to limitations on the scope of controls and the Department's work to adopt a new application control solution, the implementation of which was in progress.

2.32 DPS had restricted some required functionality relating to application control, however, some controls required by Maturity Level Two had not been fully addressed. These issues may allow certain applications to bypass application control restrictions, increasing the risk that malicious software may be allowed to execute.

Restrict Microsoft Office macros

2.33 DPS has implemented the relevant controls for Maturity Level Two.

User application hardening

2.34 DPS operates some software with known vulnerabilities, and the ANAO identified that some software was misconfigured. According to DPS' self-assessment, compensating controls were in the process of being finalised and implemented.

Regular backups

2.35 DPS does not maintain a comprehensive, prioritised system inventory. Consequently, it cannot reliably ensure that backup activities are prioritised in accordance with business criticality and business continuity requirements.

2.36 The ANAO identified that DPS had no formal program of disaster recovery testing in place. The department was able to demonstrate restoration of data in a test environment, but had not recently tested disaster recovery arrangements in a production capacity. Regular testing of backup and recovery arrangements is critical to providing assurance that such arrangements will work in a disaster scenario and is a requirement of Maturity Level Two.

Factors affecting implementation

2.37 DPS' 2024–25 self-assessment identified a number of factors for incomplete implementation of Essential Eight strategies. Key themes included:

- a lack of resources for full implementation of the strategy (seven of eight strategies); and
- the presence of 'legacy factors' (such as systems approaching the end of their useful life).[28]

2.38 Where the ANAO assessed implementation of Essential Eight strategies below Maturity Level Two requirements, the assessment primarily related to deficiencies with the intended compensating controls that DPS relied upon for risk-managed elements of the strategy.

28 Legacy IT is defined in section 13.7 of the PSPF as an IT product that is, among other criteria, end-of-life or out of support from the vendor.

2.39 In January 2026 DPS reported publicly that the parliamentary network may no longer be fit for purpose and does not provide for appropriate segmentation between users.[29] The lack of segmentation in the DPS environment increases the potential impact of identified issues, noting the different business, risk and security requirements of the stakeholders DPS supports (see paragraph 2.9).[30] In March 2026 DPS sought additional funding to progress a project to segment its network and address associated risks. In the 2026–27 Budget the department received additional resourcing to deliver necessary enhancements for critical information technology systems.

Compensating controls

2.40 For several Essential Eight strategies DPS has placed reliance on two compensating controls; vulnerability management, and logging and monitoring.

Vulnerability management

2.41 DPS makes use of a vulnerability management (VM) platform to conduct regular scans of its environment. The VM platform automatically scans the network and identifies known vulnerabilities. For supported platforms, the VM platform can propose and deploy security patches to address the identified issues. Vulnerability scanning of this nature is a requirement of the ISM and several Essential Eight strategies (specifically patch operating systems and patch applications).

2.42 DPS' VM measures address the ISM requirements for supported platforms. The DPS environment features systems that are not supported by the VM platform, and systems with identified vulnerabilities. Accordingly, vulnerability management as a compensating control is less effective for these portions of DPS' environment.

2.43 DPS has technology platforms supporting key business functions that require risk-managed operation due to lifecycle constraints. The department is working to risk assess this infrastructure and renew authorities to operate, however this work is not yet complete. In some instances, risk assessments have been completed but not yet reviewed and accepted by relevant decision-makers, resulting in a default acceptance of risk in the interim. While the department works to address these issues, it is exposed to an increased level of risk and its vulnerability management controls are less effective.

29 Department of Parliamentary Services, *Submission to the Senate Standing Committee of Privileges*, DPS, Canberra, 23 January 2026, available from: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Privileges/DPS/Submissions (accessed 13 March 2026)

30 According to guidance from the Australian Signals Directorate, network segmentation 'involves partitioning a network into smaller networks', which when combined with network segregation (controlling communication between networks) 'are highly effective strategies an organisation can implement to limit the impact of a network intrusion.'

Australian Signals Directorate, *Implementing network segmentation and segregation*, ASD, Canberra, 6 October 2021, available from: https://www.cyber.gov.au/business-government/protecting-devices-systems/hardening-systems-applications/network-hardening/implementing-network-segmentation-and-segregation [accessed 15 April 2026]

Logging and monitoring

2.44 A Security and Event Management (SIEM) platform collects, centralises and analyses log data from sources within a network or system.[31] DPS has a SIEM platform in place to support staff in monitoring this data for indicators and trends that may suggest a security incident. Multiple Essential Eight strategies refer to the need to log and monitor events, as this may assist in the detection of both successful and failed attempts to bypass relevant controls. Evidence supporting the effectiveness of the department's logging and monitoring controls is mixed:

- in simulated threat activities, DPS' logging and monitoring capability successfully detected the test activities, allowing the department to respond;
- the ANAO has previously identified that some systems have inadequate monitoring, exposing the department to risks regarding unauthorised access; and
- as discussed in relation to vulnerability management, the department has deficiencies in the process for managing vulnerabilities (refer to paragraph 2.43).

2.45 The ability of the department to detect simulated threat activities provides management with some assurance that significant cyber incidents will be identified and mitigated when they occur. However, the absence of a consistent approach to managing identified issues (ensuring that identified problems can be triaged and risk managed), and potential limitations on the scope of systems monitored, increases the likelihood of such an incident occurring.

Does the Department have appropriate assurance as to the effectiveness of their essential cyber security strategies?

DPS had undertaken a range of internal reviews, audits, and other exercises to assess and improve its cyber security posture. The department did not have a single source of truth for identified risks and issues, and available registers were not complete. Limited evidence was available to support previous PSPF self-assessment activities, although the most recent assessment in 2024–25 was supported by testing of controls.

2.46 As discussed in paragraph 2.23, entities are required to assess the effectiveness of their essential cyber security strategies as part of their annual PSPF self-assessment. Beginning with the 2024–25 reporting cycle, Home Affairs moved to a compliance-based self-assessment model that 'emphasises evidence-based compliance, risk outcomes and measurable assurance'.[32]

2.47 The PSPF does not provide specific guidance as to the means by which entities might obtain appropriate evidence to support their self-assessment or assure their controls. The ANAO considered the extent to which DPS had established core elements of an assurance regime, as shown in Table 2.3.

31 Australian Signals Directorate, *Implementing SIEM and SOAR platforms*, ASD, Canberra, 27 May 2025, available from: https://www.cyber.gov.au/business-government/detecting-responding-to-threats/event-logging/implementing-siem-and-soar-platforms [accessed 30 March 2026]

32 Department of Home Affairs, *Protective Security Policy Framework (PSPF) 2024–25 Self-Assessment Report*, DHA, Canberra, 11 February 2026, available from: https://www.protectivesecurity.gov.au/publications-library/protective-security-policy-framework-pspf-assessment-report-2024-25 (accessed 5 March 2026)

Table 2.3: ANAO assessment of DPS' assurance processes for essential cyber security strategies

Aspect of assessment	ANAO assessment
Policy and procedure framework for essential cyber security strategies	◑
Risk assessment and assurance activities	◑
Tracking and remediation of identified risks and issues through a risk-based approach	◑

Key: ● Effective ◕ Largely effective ◑ Partly effective ◔ Limited effectiveness

Source: ANAO assessment of DPS assurance processes for essential cyber security strategies.

Policy and procedure framework for essential cyber security strategies

2.48 Policies and procedures help provide assurance that activities are performed consistently, and in accordance with management intent, by specifying standards for the performance of controls. Effective security controls are dependent on a sound policy framework approved by management, communicated to staff, and regularly reviewed to ensure currency against emerging threats and changes in the operating environment. Policies also help mitigate risks associated with staff turnover by documenting key information and reducing dependence on assumed knowledge. The PSPF requires that entities develop, implement, and maintain procedures to ensure all elements of the entity's security plan are achieved.

2.49 Several of DPS' key cyber security policies and procedures are in draft. In 2025 DPS commenced work to consolidate and finalise all cyber-related policies, this work is ongoing. DPS' Audit and Risk Committee has requested increased visibility of policy approval status.

2.50 The absence of a current policy and procedure framework, noting the significant staff turnover in DPS' ICT functions, creates risk that essential cyber security strategies may not be managed consistently and effectively.

Risk assessment and assurance activities

2.51 DPS has undertaken a range of internal reviews, audits, and other exercises to assess and improve its cyber security posture. These include:

- internal audits, with two relevant audits examining the department's Essential Eight strategies, and cyber security incident management processes, and identifying areas for improvement;
- advisory activities undertaken by the Australian Cyber Security Centre;
- assurance activities performed by contracted cyber security firms; and
- other assurance activities such as the departments' annual PSPF self-assessment process.

2.52 Many of these activities identified risks, issues and potential improvements. The department's processes for tracking and implementing these outcomes which are discussed further in paragraph 2.57, could be improved.

PSPF self-assessment

2.53 As discussed in paragraph 2.23, as a non-corporate Commonwealth entity DPS conducts an annual self-assessment of its essential cyber security strategies. The annual self-assessment provides an opportunity for the department to seek its own assurance as to the effectiveness of these strategies and identify potential improvements.

2.54 The ANAO examined the evidence by which DPS self-assessed its essential cyber security controls since 2020–21, and identified inconsistencies in the approach by which these assessments were conducted. For its 2024–25 assessment DPS improved its processes by undertaking testing to verify control effectiveness, as illustrated in Case Study 2.

Case study 2. DPS self-assessment of essential cyber security controls

DPS' self-assessments of essential cyber security controls since 2020–21 have consistently reported achievement of at least Maturity Level Two (or equivalent, noting changes in maturity requirements since this time) for the Essential Eight, with areas in which the department has been managing risks. These areas have included, but are not limited to, systems requiring risk-managed operation and resourcing constraints.

In the 2022–23 self-assessment approval minute, the Secretary noted an imperative to achieve Maturity Level Three for the Essential Eight strategies (that is, to exceed minimum PSPF requirements) for the 2023–24 self-assessment.

The 2023–24 self-assessment reported achievement of Maturity Level Three for the Essential Eight strategies. The self-assessment narrative noted the presence of issues and risks being managed, of a broadly similar nature to those identified in previous self-assessments. While requirements for achieving each maturity level change over time, the rationale by which these risks were considered to have reduced or changed since prior years was unclear and there was no evidence that DPS conducted testing of controls to assure itself of their effectiveness.

In November 2024 the Information Security Working Group noted that previous self-reporting was 'limited to lower quality levels, e.g. based on a verbal statement of intent', and that the department had set an intention to improve the quality of its assessments. In March 2025 the acting CISO completed an assurance activity to test the effectiveness of the implementation of Essential Eight strategies. The activity confirmed the effectiveness of some controls and identified areas for improvement.

In 2024–25 DPS self-assessed as meeting Maturity Level Two with risk-managed elements.

2.55 Risk assessment and assurance activities are a key tool for management to obtain assurance that cyber security risks are being managed in accordance with an organisation's risk tolerance.

Opportunity for improvement

2.56 DPS could improve its processes by strengthening its evidence base for such assessments and ensuring that resulting recommendations are effectively managed.

Tracking and remediation of identified risks and issues through a risk-based approach

2.57 DPS does not have an effective, risk-based approach for tracking and remediating risks and issues relating to essential cyber security strategies. The department does not have a single source of truth for identified risks and issues, and available registers are not complete. The ANAO identified instances in which cyber security risks were assigned to system owners for management of the risk, where those staff had subsequently left the department.

2.58 As discussed in paragraph 2.45, DPS' processes for managing identified vulnerabilities expose the department to risk. The ANAO examined two risk assessments performed by DPS during 2024–25 and neither assessment demonstrated formal acceptance by a system owner, the CISO, or CIO. While DPS staff responded appropriately in identifying potential vulnerabilities requiring treatment, the absence of a formal process to track and accept identified risks limits management assurance that these processes are occurring effectively.

2.59 As shown in Table 2.2, in 2024–25 DPS self-assessed that it was achieving Maturity Level Two for essential cyber security strategies through risk management. The extent to which risk management processes are embedded and monitored is unclear. DPS' self-assessment for 2024–25 noted that mitigation treatment plans for several requirements 'involves finalising and implementing a compensating control process for the entity', and that a formal guideline would be developed to 'outline the steps for identifying, applying, and maintaining compensating controls'.

2.60 Each of the department's PSPF self-assessments since 2020–21 have identified consistent themes as contributing to the need to risk-manage Essential Eight strategies, such as the presence of risk-managed software and other components in the environment. These self-assessments have also referred to plans being in place to address these issues, however resolution of these issues remains in progress.

2.61 DPS advised the ANAO on 27 February 2026 that work is in progress to develop registers of risk treatments and improve monitoring processes and strengthening assurance arrangements to demonstrate risk treatments are effective.

Recommendation no. 2

2.62 The Department of Parliamentary Services:

(a) develop a prioritised, risk-based program of uplift activities to address known risks related to essential cyber security strategies, and issues identified through cyber security assurance activities; and

(b) implement the program of uplift activities to achieve compliance with requirements of the Protective Security Policy Framework.

Department of Parliamentary Services response: *Agreed*

2.63 *An outcome of the department's review of its cyber security governance and risk assessment processes will include identifying governance and assurance activities to be uplifted that will support the department mitigating cyber security risks in the Parliamentary Computing Network.*

2.64 *DPS is committed to embedding Australian Government cyber security standards, including the Protective Security Policy Framework and embedding Information Security Manual controls to improve maturity under the Essential Eight framework.*

Dr Caralee McLiesh PSM
Auditor-General

Canberra ACT
27 May 2026

Appendices

Appendix 1 Entity response

PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

DPS ref: EC26-000260

Dr Caralee McLiesh PSM
Auditor-General for Australia
Australian National Audit Office
38 Sydney Avenue
Forrest ACT 2603

By email: OfficeoftheAuditorGeneralPerformanceAudit@anao.gov.au

Dear Dr McLiesh

Proposed Audit Report on Management of Cyber Security in the Department of Parliamentary Services

Thank you for your correspondence of 30 April 2026 providing the Australian National Audit Office (ANAO) proposed audit report for the *Management of Cyber Security in the Department of Parliamentary Services*. The Department of Parliamentary Services (DPS) thanks the ANAO for the opportunity to provide a response to the proposed audit report.

I appreciate the recognition by the ANAO in the report of the improvements DPS has been undertaking in cyber security and highlighting areas for improvement in consideration of DPS' complex cyber security and operating environment. DPS agrees with all of the ANAO's recommendations in response to the findings in the proposed audit report.

In December 2025, DPS commenced a comprehensive review of its cyber security governance and risk assessment processes, guided by the DPS Risk Management Policy and Framework and informed by this ANAO audit. The review supports Recommendation 1 and will support DPS' cyber security governance and risk processes, ensuring they are fit for purpose and scalable to support the Parliament's evolving and increasingly complex cyber security governance and risk environment. The review is expected to be completed in July 2026.

An outcome of the review will include identifying governance and assurance activities to be uplifted that will support the department mitigating cyber security risks in the Parliamentary Computing Network (PCN). The completion of this uplift work will address Recommendation 2.

DPS is committed to working collaboratively with partners across the Parliament and government to strengthen cyber security practices through a program of continuous improvement. This will further support strengthening of systems and processes in alignment with Australian Government standards through embedding Information Security Manual (ISM) controls and progressing actions to increase our maturity level within the Australian Signal Directorate's Essential Eight Maturity Model.

DPS is receiving funding, commencing from the 2026-27 Budget, to deliver a Parliamentary Information and Cyber Resilience (PICR) project. The PICR project reflects our view that the historic system design is no longer fit for purpose and will address the underpinning system design to improve critical cyber, information security, and operational resilience risks to ensure effective

Parliament House ● PO Box 6000 ● Canberra ACT 2600 Australia ● T: 02 6277 7111 ● aph.gov.au/dps

functioning of the PCN. The current PCN is outdated, unsegmented, and increasingly vulnerable to interference and disruptive cyber events.

The expected benefits of the PICR project are:

- increased resilience of parliamentary information, communications and technology operations
- materially reduced cyber blast radius, and
- improved compliance with Protective Security Policy Framework and ISM controls.

The PICR project will be the most significant uplift in the PCN since its establishment and will strengthen cyber security, information protection and operational resilience across the network. It will materially reduce exposure to cyber threats and implement system segmentation to enhance resilience across the network.

I would like to take this opportunity to thank the ANAO, and its officers, for the professional, constructive and cooperative conduct during the course of this audit and for the valuable insights that the ANAO has provided to the department that will inform the strengthening of cyber security arrangements for the PCN.

Our summary response to the proposed audit report is provided at **Attachment A** and our response to the recommendations is provided at **Attachment B**.

Should you or your staff require further information, please contact me or the DPS Chief Audit Executive, Mr Alex Philp, on (02) 6277 2676 or alex.philp@aph.gov.au.

Yours sincerely

Jaala Hinchcliffe
Secretary

7 May 2026

Attachments:

A. Summary response to the proposed audit report
B. Response to recommendations

Parliament House ● PO Box 6000 ● Canberra ACT 2600 Australia ● T: 02 6277 7111 ● aph.gov.au/dps

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 (JCPAA) has encouraged the ANAO to consider ways in which the ANAO could capture and describe some of these impacts. The ANAO's 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. During the audit, DPS undertook a new risk assessment of systems to identify vulnerabilities and inform future actions. DPS provided the ANAO with documentation demonstrating it had been developing designs and business cases for options to improve its ICT architecture and control environment, including segmenting users into separate environments. The department also advised the ANAO it was continuing to roll out an education program for its staff to improve cyber security awareness.