Australian Government

Attorney-General's Department

EXECUTIVE MINUTE
on
JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT REPORT 485
Cyber Resilience

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

The Attorney-General's Department (the department) would like to thank the Joint Committee of Public Accounts and Audit for the opportunity to respond to Report 485: *Cyber Resilience.*

Supporting Commonwealth entities to effectively manage their cyber security risks and foster a positive security culture is a key priority for the department through the Protective Security Policy Framework (PSPF). The PSPF is a principles based framework that seeks to equip all non-corporate Commonwealth entities (NCCEs) to achieve the government's desired protective security outcomes.

Annual reporting on the implementation of the PSPF and the Australian Signals Directorate's (ASD) cyber posture reports demonstrate that entities have made positive progress in implementing cyber security requirements. The department will continue to work in partnership with other government agencies, including the Australian Cyber Security Centre (ACSC) in ASD, which leads the Australian Government's operational cyber security capability, and the Department of Home Affairs, which leads the development of cyber security policy for the Australian Government, to assist entities to enhance their cyber posture. This includes supporting them to cultivate a positive security culture underpinned by a collective awareness of risks and best practices. The department welcomes further opportunities to engage with the Committee on this matter.

Recommendation 1: The Committee recommends that the Attorney-General's Department provide an update on its implementation of external moderation models/benchmarking processes, to verify Commonwealth entities' reported compliance with cybersecurity requirements, including implementation timeframes.

Summary of response: Agreed.

The department is exploring options, including moderation, to further support entities to improve the accuracy of their self-assessments. We have advised the Australian National Audit Office (ANAO) of this work in response to recommendation 11 of their recent Report No. 32 of 2021-22 Cyber Security Strategies of Non Corporate Commonwealth Entities. In addition, the department is also reviewing the existing maturity model to ensure it is fit for purpose.

To progress this work, the department has sought feedback from entities on the current model, including on any existing processes that entities have in place to ensure the accuracy of their self-assessments. Entities have also been asked to detail any further supports that would assist them to accurately self-assess the maturity of their security capability and risk culture. This feedback will complement the comparative analysis that the department has completed on the approaches across different jurisdictions to improve the accuracy of assessments against security policy frameworks. The department expects to settle on a preferred approach to this work in the second half of 2021.

Recommendation 2: The committee recommends that the Attorney-General's Department:

- Provide an update on the levels of cyber security maturity within Commonwealth entities and the feasibility of mandating the Essential Eight across Commonwealth entities, including the threshold of cyber security maturity required by the Government to impose this mandate, and expected timeframes; and
- Report back on any impediments to mandating the Top Four mitigation strategies for government business enterprises and corporate commonwealth entities.

Summary of response: Agreed.

Cyber security maturity of non-corporate Commonwealth entities (NCCEs)

The department has published 2 PSPF assessment reports on the department's protective security website since the revised PSPF was introduced in 2018. These reports provide information on the overall security maturity of NCCEs and show meaningful improvement in cyber security maturity. In the 2019-20 reporting period, 89% of NCCEs reported they had substantially implemented the cyber security requirements in the PSPF. The department expects that this pattern of improvement will continue, although fluctuations may occur in accordance with changes in the threat environment.

Mandating the Essential Eight

The department remains committed to maintaining robust protective security standards to ensure the PSPF supports entities to manage their security risks. The PSPF currently requires entities to implement 4 specific mitigation strategies from the *Strategies to Mitigate Cyber Security Incidents* (known as the Top Four, which are a subset of the Essential Eight), and strongly recommends that entities implement the Essential Eight. As the PSPF is administered by the Attorney-General, any amendments to the PSPF require the Attorney-General's approval.

The department has carefully considered Recommendation 2 and has held detailed discussions with the ACSC on the cyber security settings in the PSPF. On this basis, the department will recommend an amendment to the PSPF to mandate the Essential Eight. This reflects the ACSC's advice that entities should progress maturity across all 8 strategies that form part of the Essential Eight, rather than focusing efforts on a smaller subset like the Top Four, as this provides a greater level of protection. This approach has also been endorsed by the Government Security Committee, an interdepartmental committee that provides strategic oversight of protective security policy.

While the PSPF strongly recommends entities implement the Essential Eight, the proposal to mandate the Essential Eight would nevertheless have an impact on the entities required to implement it. As a result, the department has commenced consultation with the 98 NCCEs about the implications of this proposal. The department expects responses from NCCEs by the end of June 2021. The department is also preparing draft amendments to the PSPF and considering timeframes for implementing this proposal. The outcomes of these processes will inform the department's advice to the Attorney-General about mandating the Essential Eight and appropriate implementation timeframes.

Mandating the Top Four for government business enterprises and corporate commonwealth entities

The PSPF is a government policy that applies to NCCEs, which are subject to section 21 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). Consistent with the Government response to the Joint Committee of Public Accounts and Audit Report 467: *Cybersecurity*

Compliance, the department has explored, in consultation with the Department of Finance, the possibility of extending the cyber security obligations in the PSPF to all Commonwealth entities via two potential mechanisms: legislation, and a Government Policy Order (GPO).

Incorporating specific security obligations in the PGPA Act, and applying those obligations to both NCCEs and corporate Commonwealth entities (CCEs), was explored as part of the *Independent Review into the operation of the Public Governance, Performance and Accountability Act 2013 and Rule* and was not recommended. On that basis the department is not proposing to pursue a legislative amendment.

The department also considered options to extend the PSPF to CCEs via a GPO under section 22 of the PGPA Act. The department concluded the use of a GPO for this purpose is not appropriate as a GPO would apply government policy at the time the order is made and require that every CCE be consulted in advance of each update. A GPO would therefore not offer the necessary flexibility to respond to emerging security threats. In addition, it would not be possible to extend the requirements to all CCEs via a GPO, as some CCEs are exempted from the operation of section 22 of the PGPA Act by their enabling legislation.

The PSPF remains better practice for CCEs and wholly owned Commonwealth companies, and the department encourages those entities to apply the PSPF. The department notes that CCEs are required to have security cleared personnel and appropriately classified systems in order to access security classified information. In addition, the department notes that the ACSC recommends that all organisations (including CCEs) implement the Essential Eight mitigation strategies to prevent cyber security incidents.

Recommendation 3: The Committee recommends that the Australian Government (the Attorney-General's Department) ensure that the framework of 13 behaviours and practices developed by the Australian National Audit Office (ANAO) play a greater role in the implementation and improvement of a cyber resilient culture within Commonwealth entities, including that;

- The Protective Security Policy Framework (PSPF) be amended to reflect or incorporate the behaviours and practices framework, including for auditing purposes, to maximise alignment between the PSPF and the ANAO's audit frameworks; and
- A dedicated section be created within the annual PSPF self-assessment questionnaire addressing the ANAO's 13 behaviours and practices that facilitate a cyber resilience culture.

Summary of response: Agreed with qualification.

The department recognises the importance of strong security culture. The revised PSPF (which commenced in October 2018) requires accountable authorities to ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture.

The department has undertaken an assessment of the 13 behaviours and practices developed by the ANAO and has formed the view that they are already reflected in the PSPF (in particular Policy 2 and Policy 11). Policy 11: Robust ICT Systems requires entities to follow the cyber security principles specified in the Australian Government Information Security Manual, and Policy 2: Management Structures and Responsibilities requires entities to ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture. PSPF Policy 2 also provides guidance on the 10 characteristics of a positive security culture. A table which compares the 13 behaviours and practices against the PSPF is provided at **Attachment A**.

The annual PSPF self-assessment requires each entity to report on its implementation of the requirements in the PSPF. As the behaviours and practices are already reflected in the PSPF, the annual self-assessment already requires entities to address those behaviours and practices.

Signed by

Iain Anderson

A/g Secretary, Attorney-General's Department

Comparison of ANAO's 13 behaviours and practices and the PSPF

13 behaviours and practices identified by the ANAO	Which PSPF Policy reflects this behaviour and practice?	How is the behaviour and practice already embedded in the PSPF Policy?
1. Establish a business model and ICT governance that incorporates ICT security into strategy, planning and delivery of services.	PSPF Policy 3: Security planning and risk management	Policy 3 requires entities to have in place a security plan that sets out 'how security risk management intersects with and supports broader business objectives and priorities'.
2. Manage cyber risks systematically, including through assessments of the effectiveness of controls and security awareness training.	Policy 3: Security planning and risk management Policy 4: Security maturity monitoring Policy 5: Reporting on security Policy 10: Safeguarding information from cyber threats	Policy 3 requires entities to review security plans every 2 years, and the review process must include 'how the entity will determine the adequacy of existing measures and mitigation controls'. Policy 4 requires each entity to 'assess the maturity of its security capability and risk culture'. Policy 5 requires entities to report annually on 'the maturity of the entity's security capability' and 'measures taken to mitigate or otherwise manage identified security risks.' Policy 10 requires an entity to 'mitigate common and emerging cyber threats' by implementing four specific strategies to mitigate cyber security incidents (known as the Top Four) and to consider which of the remaining strategies the entity needs to implement.
3. Task enterprise-wide governance arrangements to have awareness of cyber vulnerabilities and threats.	Policy 2: Management structures and responsibilities Policy 3: Security planning and risk management	Policy 2 requires entities to 'appoint a Chief Security Officer (CSO) at the Senior Executive Service level to be responsible for security in the entity', and provides that the CSO 'must be responsible for directing all areas of security to protect the entity's people, information (including ICT) and assets.' Policy 3 requires entities to 'have in place a security plan, approved by the accountable authority, to manage the entity's security risks'. The security plan must detail the entity's 'threats, risks and vulnerabilities that impact the protection of [its] people, information and assets', and set out the entity's 'strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.'
4. Adopt a risk-based approach to prioritise improvements to cyber security and to ensure	Policy 3: Security planning and risk management	Policy 3 requires entities to 'have in place a security plan, approved by the accountable authority, to manage the entity's security risks'. The security plan must detail the entity's 'threats,

higher vulnerabilities are addressed.		risks and vulnerabilities that impact the protection of [its] people, information and assets', and set out the entity's 'strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.' The analysis of security risks should 'prioritise risks for subsequent evaluation of tolerance or the need for further treatment'.
5. Assign information security roles to relevant staff and communicate the responsibilities.	Policy 1: Role of accountable authority Policy 2: Management structures and responsibilities	Policy 1 provides that accountable authorities must 'manage the security risks of their entity'. Policy 2 requires accountable authorities to 'appoint a Chief Security Officer (CSO) at the Senior Executive Service level to be responsible for security in the entity', and provides that the CSO 'must be responsible for directing all areas of security to protect the entity's people, information (including ICT) and assets.' The accountable authority must 'empower the CSO to make decisions about appointing security advisors within the entity, the entity's protective security planning, the entity's protective security practices and procedures and investigating, responding to, and reporting on security incidents'. The CSO is responsible for 'appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.' Policy 2 also requires accountable authorities to 'ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this'.
6. Develop the capabilities of ICT (information and communication technology) operational staff to ensure they understand the vulnerabilities and cyber threats to the system.	Policy 2: Management structures and responsibilities Policy 3: Security planning and risk management	Policy 2 requires accountable authorities to 'appoint a Chief Security Officer (CSO) at the Senior Executive Service level to be responsible for security in the entity'. The CSO is responsible for 'appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.' The department recommends 'the CSO ensure sufficient security advisors positions are in place to perform security management functions (particularly for specialist ICT security services) and ensure continuous delivery of government business'. Policy 2 also requires accountable authorities to 'ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this'. Entities need to provide 'personnel in specialist and high-risk positions (including contractors and security

		incident investigators) with specific security awareness training targeted to the scope and nature of the position'. Policy 3 requires entity security plans to detail the 'maturity of the entity's capability to manage security risks'.
7. Ensure management understand their roles and responsibilities to enhance security initiatives for the services for which they are accountable. This includes senior management understanding the need to oversight and challenge strategies and activities aimed at ensuring the entity complies with mandatory security requirements.	Policy 1: Role of the Accountable Authority Policy 2: Management structures and responsibilities Policy 3: Security planning and risk management	Policy 1 requires the accountable authority to 'determine their entity's tolerance for security risks, manage the security risks of their entity and consider the implications their risk management decisions have for other entities.' Policy 2 requires accountable authorities to 'appoint a Chief Security Officer (CSO) at the Senior Executive Service level to be responsible for security in the entity'. The CSO is responsible for 'directing all areas of security to protect the entity's people, information (including ICT) and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.' Policy 2 also requires the accountable authority to 'ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this'. Policy 3 requires entities to have in place a security plan that sets out 'how security risk management intersects with and supports broader business objectives and priorities'.
8. Embed security awareness as part of the enterprise culture, including expected behaviours in the event of a cyber incident.	Policy 2: Management structures and responsibilities Policy 3: Security planning and risk management	Policy 2 requires the accountable authority to 'ensure personnel are aware of their collective responsibility to foster a positive security culture, and are provided with sufficient information and training to support this.' Entities need to 'provide all personnel, including contractors, with security awareness training at engagement and annually thereafter'. Policy 3 requires each entity to have in place a security plan that details 'entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF'.
9. Assign data ownership to key business areas, including the role to classify the data, and grant or revoke access to shared data by other entities.	Policy 8: Sensitive and classified information Policy 9:	Policy 8 requires entities to 'identify information holdings, assess the sensitivity and security classification of information holdings, [and] implement operational controls for these information holdings proportional to their value, importance and sensitivity'. This includes

	Access to information	requiring the originator to identify the appropriate classification and ensuring there is clear guidance on the appropriate operational controls. Policy 9 requires entities to ensure that 'those who access sensitive or security classified information have an appropriate security clearance'. In addition, 'entities must ensure access to sensitive and security classified information or resources is only provided to people with a need-to-know'. The requirement to ensure appropriate access to information includes 'controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.'
10. Develop and implement an integrated and documented architecture for data, systems and security controls.	Policy 3: Security planning and risk management Policy 9: Access to information	Policy 3 requires entities to 'have in place a security plan, approved by the accountable authority, to manage the entity's security risks'. Entities need to 'identify people, information and assets that are critical to the ongoing operation of the entity and the national interest and apply appropriate protections to these resources'. Policy 9 requires entities to 'enable appropriate access to official information', including by 'controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications'.
11. Identify and analyse security risks to their information and system, including documenting ICT assets requiring protection.	Policy 3: Security planning and risk management	Policy 3 requires entities to have in place a security plan that details 'threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets' and the 'entity's strategies to implement security risk management'. Entities need to 'identify people, information and assets that are critical to the ongoing operation of the entity and the national interest and apply appropriate protections to these resources'.
12. Establish a Cyber Incident Response Plan, informed by a comprehensive risk assessment and business continuity plan, including a priority list of services (not ICT systems) to be recovered.	Policy 2: Management structures and responsibilities Policy 3: Security planning and risk management	Policy 2 requires entities to 'develop and use procedures that ensure all elements of the entity's security plan are achieved, [and] security incidents are investigated, responded to, and reported'. Policy 3 requires entities to have in place a security plan 'to manage the entity's security risks'. The plan must detail the 'threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets' and the 'entity's strategies to implement security risk management'. In addition, entities are required to 'identify people, information and assets that are critical to the ongoing operation of the entity and the national interest and apply appropriate