# Joint Committee of Public Accounts and Audit

## Attorney-General's Department

**Question date:** 31 May 2023

**Julian Hill asked the following question:**

1. What is the role of the Attorney-General's Department in ensuring the implementation of cybersecurity measures?
2. What are the key requirements outlined in the updated PSPF Policy 10 regarding the safeguarding of data from cyber threats?
3. What guidance is available for entities to implement their obligations under the Protective Security Policy Framework and other requirements?
4. The AGD collects information on entities' self-assessed level of maturity for the of PSPF. Can the AGD provide an overview of the latest self-assessed maturity data for entities?
5. Does AGD undertake any assurance over self-assessed data?
6. What reporting does AGD provide to government on entities' PSPF maturity or compliance?
7. Is this reporting public?

**The response to the question is as follows:**

1. Under the Administrative Arrangements Order, the Attorney-General's Department (AGD) is responsible for protective security policy, which is implemented through the Protective Security Policy Framework (PSPF).

   The *Directive on the Security of Government Business*, issued by the Attorney-General, establishes the PSPF as a government policy. The Directive provides that AGD's role is to 'assess emerging security risks and develop and refine protective security policy', with oversight from the Government Security Committee. This includes cyber security policy settings.

   Section 21 of the *Public Governance, Performance and Accountability Act 2013* requires the accountable authority of a non-corporate Commonwealth entity to govern the entity in a way that is not inconsistent with Australian Government policies. PSPF policy 1: *Role of accountable authority* provides that accountable authorities are responsible for implementing the PSPF requirements, including those relating to cyber security. It also provides that the accountable authority is answerable to their minister and the government for the security of their entity.

   PSPF policy 5: *Reporting on security* requires entities to report annually to AGD and their portfolio minister on whether they achieved security outcomes through effectively implementing and managing requirements under the PSPF. The policy also requires each entity to complete the Australian Signals Directorate's annual cyber security survey.

   AGD supports non-corporate Commonwealth entities to implement the PSPF, including its cybersecurity requirements. This includes:

   - providing guidance to entities on implementation of PSPF requirements in

collaboration with lead security agencies
- ensuring entities complete and submit their annual security maturity self-assessments and analysing those assessments
- providing a range of guidance materials to support PSPF reporting, including a best practice evidence guide and reporting guides
- developing a peer review process, which was piloted in the 2021-2022 reporting period, to provide entities with a mechanism to obtain external review of their self-assessments
- preparing benchmarking reports on implementation of the PSPF, and
- providing advice to government on protective security maturity across entities, based on the reporting data received from entities.

2. PSPF Policy 10: *Safeguarding data from cyber threats*, mandates that each non-corporate Commonwealth entity must mitigate common cyber threats by:
    - implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents:
        - application control
        - patch applications
        - configure Microsoft Office macro settings
        - user application hardening
        - restrict administrative privileges
        - patch operating systems
        - multi-factor authentication
        - regular backups
    - considering which of the remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents need to be implemented to achieve an acceptable level of residual risk for their entity.

3. Each PSPF policy provides detailed guidance for entities on implementing each PSPF core and supporting requirement. This is supplemented by guidance provided by technical experts. The department also provides advice to agencies as required, as well as facilitating advice from relevant security agencies.

    For example, PSPF policy 10 provides guidance on each of the eight mandatory strategies (known as the Essential Eight) and points to additional guidance provided by the Australian Signals Directorate (ASD), including in the Information Security Manual (ISM). ASD provide a range of guidance materials to support implementation of the Essential Eight, including the *Essential Eight Assessment Process Guide*, *Essential Eight Assessment Toolkit*, *Essential Eight Maturity Model*, *Essential Eight Maturity Model and ISM Mapping*. This guidance is further supplemented by technical uplift support from ASD.

4. Each year the department publishes a consolidated annual assessment report which details entities' reported maturity against the PSPF. The report is publicly available on the PSPF website. The most recent report is available at *PSPF Assessment Report 2021–22*.

5. The department has arrangements in place to ensure that it receives the required data from entities on an annual basis, that the calculation model and tools are tested and are operating correctly and that the data is appropriately analysed.

The department makes considered efforts to support entities to improve the accuracy of their security maturity self-assessment reports. The department initiated a peer review process pilot for the 2021-2022 reporting period to provide entities with a mechanism to obtain external review of their self-assessment report prior to submission. The peer review process supports entities to improve the accuracy of their reports and provides a forum for information sharing, including sharing best-practice approaches to implementation of PSPF requirements and reporting.

A total of 12 entities participated in the pilot (approximately 10%) and were matched according to function, size and security profile. Participating entities advised the review assisted their self-assessment process and that their peer review partner provided useful feedback. Some entities modified their reports in response to the peer feedback received prior to submission. AGD intends to extend the peer review pilot for the 2022-23 reporting period with a broader cohort to determine whether the process should be established as an ongoing approach.

The department has made modifications to the reporting portal and the reporting questions to improve the clarity and accuracy of reporting. It also hosts an annual reporting information session ahead of the opening of the reporting period to support entities to understand their obligations and assist them in accurately completing the survey. The department continues to explore further options to strengthen assurance and evaluation.

6. At the conclusion of each annual reporting period, the department analyses the data and prepares advice for the Attorney-General on security maturity across non-corporate Commowealth entities, including details about individual entities with low maturity. The department also prepares a consolidated PSPF assessment report on the security maturity of entities with respect to the requirements of each of the 16 PSPF policies – this report is published on the PSPF website.

7. The consolidated annual PSPF assessment report is publicly available on the PSPF website.