1 Role of accountable authority

A. Purpose

1. This policy outlines the role and responsibilities of an accountable authority.[1]

Applicable sections of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act):

Section 21 Non-corporate Commonwealth entities (application of government policy)
The accountable authority of a Commonwealth entity **must** govern their entity in accordance with paragraph 15(1)(a) in a way that is not inconsistent with the policies of the Australian Government.

Section 15 Duty to govern the Commonwealth entity
(1) The accountable authority of a commonwealth entity **must** govern the entity in a way that:
(a) promotes the proper use and management of public resources for which the authority is responsible.

2. This policy establishes consistent, efficient and effective protective security measures across government. It forms the basis for protecting people, information and assets from security threats and supports continuous delivery of Australian Government business.

B. Requirements

B.1 Core requirement

The accountable authority is answerable to their minister and the government for the security of their entity.

The accountable authority of each entity must:

- ***a. determine their entity's tolerance for security risks***
- ***b. manage the security risks of their entity, and***
- ***c. consider the implications their risk management decisions have for other entities, and share information on risks where appropriate.***

The accountable authority of a lead security entity must:

- ***a. provide other entities with advice, guidance and services related to government security***
- ***b. ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security, and***
- ***c. establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities.***

B.2 Supporting requirement

Supporting requirement for role of accountable authority

#	Supporting requirement
Requirement 1. Exceptional	Where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement, the accountable authority:

[1] The accountable authority of a Commonwealth entity is the person or group of persons responsible for, and with control over, the entity's operations.

#	Supporting requirement
circumstances	a. **may** vary application, for a limited period of time, consistent with the entity's risk tolerance b. **must** record the decision to vary in the annual report on security to the Attorney-General's Department and advise remedial action taken to reduce the risk to the entity.

C. Guidance

C.1 Accountable authority role and responsibilities

3. The accountable authority is answerable to their portfolio minister for the protective security of the entity's people, information and assets. In meeting obligations to their portfolio minister, the accountable authority is supported by a Chief Security Officer and, where appropriate, a security governance committee.
4. The accountable authority's role is to have effective protective security arrangements in place that achieve:
   a. capacity to function including during security incidents, disruptions or emergencies
   b. safety of those employed by the entity to carry out the functions of government (including contractors) and those who have dealings with the entity (including visitors)
   c. protection of resources and information held within the entity.
5. The accountable authority is responsible for:
   a. implementing the PSPF core and supporting requirements
   b. appointing an SES Chief Security Officer who is responsible for oversight of protective security and authorised to make security decisions (see PSPF policy: Management structures and responsibilities)
   c. providing security awareness training for personnel (including contractors) about their security responsibilities (see PSPF policy: Management structures and responsibilities)
   d. approving an appropriate security plan to manage security risks and ensure personnel understand how to manage those risks (see PSPF policy: Security planning and risk management)
   e. ensuring appropriate accreditation processes are in place for ICT systems, including accepting any residual security risks to the system or the information the system processes, stores or communicates (see PSPF policy: Robust ICT systems)
   f. fostering a positive security culture with clearly defined expectations and priorities (see PSPF policy: Security planning and risk management)
   g. monitoring the entity's security maturity (see PSPF policy: Security maturity monitoring)
   h. accurately recording in the annual report the entity's security maturity (see PSPF policy: Reporting on security)
   i. approving citizenship waivers and uncheckable background waivers (see PSPF policy: Eligibility and suitability of personnel)
   j. embedding effective security risk management (see section C.2)
   k. ensuring variances to PSPF implementation (as a result of exceptional circumstances) are defendable, considered in light of the entity's risk tolerances and are for a limited time period (see section C.4).
6. The accountable authority of a lead security entity has additional responsibilities, as outlined in the core requirement and section C.3.

C.2 Security risk management

7. Overall responsibility for security risk management in the entity rests with the accountable authority, with support from the Chief Security Officer.
8. Security risk management includes identifying, assessing and prioritising risks to people, information and assets. It involves the efficient and coordinated application of protections that minimise, monitor and control the probability and effects of risks.

9. The Department of Finance Commonwealth Risk Management Policy sets out the requirements and guidance for managing government risks, including security and shared risks.

10. The PSPF policy: Security planning and risk management outlines how to identify and manage an entity's security risks through security planning and embedding security into risk management practices.

C.2.1 Determine tolerance for security risks

11. The accountable authority makes informed decisions on priorities and balances the entity's capacity to deliver business objectives while maintaining a secure environment. This is achieved by determining the level of risk the entity is willing or able to accept. The accountable authority takes a common-sense approach when setting security risk tolerance levels.

12. The Attorney-General's Department recommends that the accountable authority documents the entity's risk tolerances and protections to reduce, treat or mitigate risks. This would include the defined benchmarks against which the success of implemented risk mitigations can be measured.

13. For guidance on determining risk tolerances for security threats, see PSPF policy: Security planning and risk management and the Department of Finance Defining risk appetite and tolerance information sheet.

C.2.2 Implications of risk management decisions

14. The core requirement mandates that the accountable authority considers the implications of security risk management decisions on other entities or whole-of-government security. Particular consideration is required where a lead security entity's decision has adverse implications for a supported entity. The supported entity may have a different risk tolerance level or limited capacity to meet the resulting obligations.

15. The core requirement also mandates that the accountable authority must consider when to share information with other entities that may be affected by risk management decisions made within their entity. Entities are strongly encouraged to adopt a default position to seek and share information (unless security, secrecy or privacy limitations are in place). In the event these limitations are in place, entities are encouraged to look at options that allow partial sharing of information. Where there are legislative limitations, such as under the *Privacy Act 1988*, entities may consider using formal agreements with other entities to share information.

16. Sharing information between entities may help to mitigate threats across government. For example, parties that pose security threats, such as organised crime groups, may target multiple government entities.

17. For guidance on managing shared risks, refer to element seven of the Commonwealth Risk Management Policy and Understanding and managing shared risk information sheet.

18. For guidance on sharing information with other entities, see PSPF policy: Access to information.

C.3 Lead protective security entities

19. Lead protective security entities are those with additional responsibilities as a:

    a. lead entity in their portfolio

    b. provider of government protective security advice, policy, technical standards or intelligence services or

    c. provider of shared-services arrangements.

20. **Table 1** outlines Australia's lead entities that hold key protective security accountabilities to provide government advice, policy, technical standards or intelligence services.

Table 1 Key lead protective security entities

Entity	Protective security responsibility
Attorney-General's Department	Responsible for whole-of-government protective security policy development and governance oversight. The National Security Authority for the purpose of whole-of-government general security agreements, responsible for general oversight and administration of international agreements.

Entity	Protective security responsibility
Australian Federal Police (AFP)	Responsible for protection services for designated Commonwealth establishments and diplomatic and consular missions in Australia. Authorised vetting agency (for AFP clearances).
Australian Secret Intelligence Service	Australia's overseas secret intelligence collection agency. An authorised vetting agency.
Australian Security Intelligence Organisation	Australia's national security intelligence service with investigative and advisory responsibilities including provision of threat assessments, protective and physical security services, and personnel security advice. Responsible for security services through the T4 Protective Security Unit, including: risk assessments, technical surveillance counter measures and certification of TOP SECRET storage facilities. An authorised vetting agency.
Australian Signals Directorate	Responsible for Australian Government ICT security standards and advice, including the Information Security Manual and certifying outsourced cloud computing services.
Department of Defence	Responsible for security clearance vetting services to government and industry through the Australian Government Security Vetting Agency. An authorised vetting agency.
Department of Foreign Affairs and Trade	Responsible for whole-of-government security policy to protect Australian Government officials overseas. An authorised vetting agency.
Department of Home Affairs	Responsible for providing coordinated strategy and policy leadership for Australia's federal law enforcement, national and transport security, criminal justice, emergency management, multicultural affairs and immigration and border-related functions.
Department of the Prime Minister and Cabinet	Responsible for high-level leadership, direction and coordination of national security and intelligence entities.
Digital Transformation Agency	Responsible for facilitating greater transparency to government on ICT projects, costs, risks and opportunities, as well as a whole-of-government approach to investing in cloud technologies.
National Archives of Australia	Responsible for Commonwealth records and information standards and advice.
Office of the Australian Information Commissioner	Responsible for whole-of-government information management policy and practice, including freedom of information and privacy.
Office of National Intelligence	Responsible for strategic development and intelligence enterprise management of the Australian Intelligence Community as the principal adviser to the Prime Minister on matters relating to the national intelligence community. An authorised vetting agency.

C.3.1 Providing advice and support to another entity

21. Some entities have additional specific lead security responsibilities (as outlined in section C.3). Timely security support and advice provided by lead security entities is critical to helping supported entities achieve and maintain an acceptable level of security (appropriate to their risks) and remain aligned with government-wide security policies, priorities and plans.

22. The Attorney-General's Department recommends that the lead security entity:

    a. implements appropriate oversight arrangements, including appointing an executive to coordinate security services to supported entities

    b. sustains capability to provide timely and accurate security advice and services

    c. maintains regular contact with the entities they support to increase awareness of the lead security entity's role and capabilities.

C.3.2 Partnerships and service arrangements

23. The accountable authority of a lead entity establishes and agrees on clearly defined accountabilities, responsibilities and procedures when entering into partnerships or security service provision arrangements with other entities.

24. The Attorney-General's Department recommends:

    a. supported entities report to their lead security entity in the event of significant changes in their protective security arrangements or threat environment

    b. lead and supported entities maintaining clearly defined and agreed processes for significant or reoccurring security incidents or events, such as:

        i. clear responsibilities (agreed by all parties) including who will take lead control and when

        ii. responsibilities of specialised areas the entities intend to include in decision-making

        iii. escalation responsibilities (to whom and when), particularly if there are multiple ministers or governing bodies involved

        iv. communication responsibilities to control and maintain the flow of information during an event and keep relevant parties informed (e.g. leadership, staff, contractors, building owners, in-house service providers)

        v. consistent approaches, particularly for co-located entities

    c. scheduling periodic reviews to consider the effectiveness of these arrangements and make procedural adjustments where necessary.

25. The accountable authority of a supported entity is responsible for the overall security of their entity. If the accountable authority of the lead security entity agrees, a supported entity may outsource responsibility for specific functions under shared-services or partnership arrangements.

26. The Attorney-General's Department recommends that lead security entities consider periodically reviewing existing partnership and shared-service arrangements to ensure accountabilities and responsibilities are clearly identified.

27. For cross-portfolio arrangements, entities are encouraged to review reporting arrangements to their relevant ministers at regular intervals.

28. For information on managing security incidents, see the PSPF policy: Management structure and responsibilities.

C.4 Exceptional circumstances

29. **Requirement 1** states that, where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement, the accountable authority may vary application (for a limited period of time) consistent with the entity's risk tolerance. Examples of exceptional circumstances include natural disasters and emergency situations; exceptional circumstances are not routine in nature or enduring.

30. Entities are required to apply a risk-based approach to managing security. However, this does not apply to deciding whether or not to implement PSPF core and supporting requirements. The exceptional circumstances provision allows accountable authorities to adapt to arising circumstances that affect the entity's implementation or maintenance of a particular requirement. Entities may consider alternative mitigation strategies during such periods to maintain appropriate protection.

31. The intention of the exceptional circumstances provision is to maintain the entity's PSPF maturity rating. Where the accountable authority demonstrates the exception decision was necessary (eg during an emergency) or justified within the entity's risk tolerance, the entity may maintain their maturity level for the affected core requirement.

32. Section 19 of the PGPA Act requires that accountable authorities notify the responsible minister of significant issues that affect, or may affect, the entity. This obligation includes advising the responsible minister, through the annual report on security, of any significant issues with implementing the PSPF requirements or decisions to vary implementation.

C.4.1 Alternative mitigations

33. It is not a reportable significant issue where the entity adopts alternative protective security measures that provide the same (or exceed the level of) protection as the PSPF requirement.

34. The security plan review obligation imposed by **Requirement 1a** of PSPF policy: Security planning and risk management is to consider the adequacy of existing measures and mitigation controls at least every two years (or if the entity's environment significantly changes). This also applies to any alternative mitigation implemented by the entity.

35. Deliberately disregarding implementation of a PSPF requirement is a security incident. For information on managing security incidents, see the PSPF policy: Management structures and responsibilities.

D. Find out more

36. Other legislation and policies include:

    a. *Public Governance, Performance and Accountability Act 2013* – Accountable authorities (Section 12) and Duty to keep responsible Minister and Finance Minister informed (section 19)

    b. Commonwealth Risk Management Policy.

37. Further guidance is available in Department of Finance Risk Management information sheets:

    a. Overview of the risk management process

    b. Defining risk appetite and tolerance

    c. Understanding and managing shared risk.

D.1 Change log

Table 2 Amendments in this policy

Version	Date	Section	Amendment
v2018.1	Sep 2018	Throughout	Not applicable. This is the first issue of this policy