Role of the Chief Security Officer

The Protective Security Policy Framework (PSPF) sets clear lines of accountability for protective security in non-corporate Commonwealth entities, establishing defined roles and responsibilities including the new role of Chief Security Officer (CSO). This role is described in the PSPF Policy: Management structures and responsibilities.

PSPF Policy: Management structures and responsibilities—Core requirement

The accountable authority **must**:

a. appoint a Chief Security Officer (CSO) at the Senior Executive Service level to be responsible for security in the entity
b. empower the CSO to make decisions about:
    i. appointing security advisors within the entity
    ii. the entity's protective security planning
    iii. the entity's protective security practices and procedures
    iv. investigating, responding to, and reporting on security incidents, and
c. 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.

The CSO's overarching responsibility is to support their accountable authority to achieve the entity's security outcomes by providing strategic, entity-wide oversight of protective security across security governance, information security (including ICT), personnel security and physical security—either directly or through a security governance committee.

A. CSO's key responsibilities:

- Implement the requirements of the PSPF within the entity
- Set the strategic direction for the entity's protective security planning and risk management
- Effectively integrate security into the entity's risk and business processes and decisions
- Champion a positive security culture that is supported by effective security awareness training
- Embed efficient and effective security management, awareness and practices
- Prioritise appropriate staffing levels, resources and funding to support delivery of protective security outcomes
- Realise optimal security maturity through clear understanding of vulnerabilities, decisions and future plans
- Manage the entity's response to security-related crises, incidents and emergencies and establish monitoring mechanisms across the entity
- Determine when a security incident is serious or significant enough to commence an investigation
- Monitor security performance to achieve required protections, identify emerging risks, build security capability, mitigate unacceptable security risks, and improve security maturity.

B. CSO obligations across the PSPF policies

Summary of CSO obligations	PSPF policy
Security oversight Support the accountable authority by being responsible for entity-wide oversight of protective security and direct all areas of security to protect the entity's people, information (including ICT) and assets.	1 Role of the accountable authority
Security arrangements and appointments Tailor security arrangements to the scale and complexity of the entity and its risk environment, including by appointing sufficient security advisors to support the day-to-day delivery of protective security outputs and to perform specialist services.	2 Management structures and responsibilities
Security planning and procedures Establish effective procedures to achieve security outcomes that are consistent with the PSPF and other Australian Government policies and legal requirements–including for investigating, responding to, and reporting on security incidents.	
Positive security culture Foster a positive security culture that supports entity personnel to understand their role in managing security risk, reinforced by practices that embed security into entity operations.	
Security awareness training Ensure personnel (including contractors and those travelling or located overseas) complete annual security awareness training so they can understand and meet their security obligations.	
Implement the PSPF Direct the entity's implementation of PSPF requirements giving consideration to the entity's size, operations and risk environment.	3 Security planning and risk management
Risk management Develop a comprehensive security plan to articulate how the entity will manage its security risks, spanning all areas of protective security.	
Alternative mitigations Document any decisions to implement an alternative mitigation measure or control to a PSPF requirement, and adjust the maturity level for the related PSPF requirement.	
Managing intelligence and threat information Disseminate and manage intelligence and threat information to stakeholders across the entity.	4 Security maturity monitoring
Security performance measures Establish security performance measures to monitor the effectiveness of protective security activity to achieve required protections, address security risks and improve security maturity.	5 Reporting on security
Preparation of entity's annual PSPF security report Oversee preparation of the annual PSPF security report to accurately reflect the entity's security maturity level and detail how the entity is addressing areas of vulnerability.	
Certification and accreditation authority Ensure ICT systems are certified and the appropriate level of security is being applied, with residual risks accepted by the relevant accreditation authority.	11 Robust ICT systems
Security clearances: eligibility waivers for citizenship and checkable backgrounds Where the accountable authority has delegated responsibility, consider and approve requests to waive an uncheckable background or citizenship requirement on the basis of a risk assessment.	12 Eligibility and suitability of personnel
Information sharing Ensure effective information sharing within the entity and with authorised vetting agencies to facilitate the ongoing assessment and management of the suitability of personnel to access Australian Government resources, including meeting security clearance maintenance obligations.	13 Ongoing assessment of personnel
Access control Granting ongoing (or regular) access to entity facilities for people with a business need who are not directly engaged by the entity or covered by the terms of a contract or agreement, only if the person has the required level of security clearance for the facility's security zones and subject to a business case and risk assessment (reassessed on a regular basis at least every two years).	16 Entity facilities
Security zone certification and accreditation Before a facility is used operationally, ensure the facility's Zones are certified and accredited in accordance with the PSPF.	