PSPF Direction 003-2025

Online Disclosure of Security Clearance and National Security Information

The Protective Security Policy Framework (PSPF) applies to non-corporate Commonwealth entities subject to the *Public Governance, Performance and Accountability Act 2013*. The PSPF provides that, having considered advice from technical authority entities, the Secretary of the Department of Home Affairs may issue a Direction to accountable authorities to manage a protective security risk to the Commonwealth.

The Accountable Authority of each entity must adhere to any Direction issued.

PSPF Direction 003-2025 requires Australian Government entities to manage the risks arising from personnel[1] disclosing information that identifies or alludes to their access to security classified material, including the fact that they hold a security clearance, on online platforms[2], by expanding established personnel security risk management and monitoring activities and including a specific policy prohibiting publication of this information.

After considering threat and risk analysis, I have determined that there is a pressing need for entities to manage the security risks arising from personnel disclosing information that identifies or alludes to their access to security classified material, including the fact that they hold a security clearance, on online platforms, due to threats of foreign interference, espionage, and sabotage. I have also considered the importance of a public policy statement to demonstrate best practice for those non-government holders of security clearances.

Security clearances afford personnel privileged access to Australian Government security classified information and resources. Public disclosure of security clearance information and indicating or alluding to access to security classified information makes personnel, and the entities they work for, vulnerable to targeting, including cultivation and exploitation, or cyber and physical security compromise, by foreign powers.

Immediate actions from technical authorities will include:

- The Department of Home Affairs will extend these requirements to key private sector providers through the Hosting Certification Framework,
- The Department of Home Affairs will work with social media providers to access publicly available data to identify non compliance,
- The Australian Security Intelligence Organisation will add a requirement for TOP SECRET-Privileged Access security clearance holders, and
- Australian Government Security Vetting Agency will add a requirement for other security clearance holders[3].

[1] *'Personnel' includes any employee and contractor, including secondees, and any service providers that an entity engages. It also includes any person who is provided access to Australian Government resources held by the entity as part of entity sharing initiatives.*

[2] *'Online Platforms' constitutes all publicly accessible online websites, including social media platforms and employment-focused platforms such as LinkedIn, however, excludes any official public transparency or accountability mechanism such as Hansard.*

[3] *'Other security clearance holders' constitutes all security clearances issued by the Australian Government Security Vetting Agency.*

By 1 December 2025, all non-corporate Commonwealth entities **must**:

1. Establish a specific policy relating to the publication of security clearance information[4] and other information indicating or alluding to access to security classified information for all entity personnel. This must:
    - Apply to all security clearance levels
    - Prohibit the publication of security clearance level
    - Clearly define limitations on the employment-related information that can be publicised
    - Prioritise personnel occupying a designated high-risk position[5]
    - Be integrated into the entity's annual Security Checks, including specifically requiring personnel to confirm compliance with this policy, and
    - To undertake regular auditing to ensure compliance with this policy.
2. Provide specific training on foreign interference, espionage, cultivation and exploitation by foreign powers, as part of the entity's annual security awareness training. This must:
    - Include targeted security awareness training for personnel occupying a designated high-risk position, and
    - Encourage proactive and comprehensive contact reporting, including how personnel can do that within their entity.
3. Report completion of above requirements to the Department of Home Affairs' Commonwealth Security Policy Branch at PSPF@homeaffairs.gov.au.

During the 2025-26 annual PSPF reporting period, all non-corporate Commonwealth entities **must** provide a summary of any reported disclosures of information that identifies or alludes to personnel access to security classified material (including the fact that they hold a security clearance) on online platforms and mitigations that have been implemented to:

1. The Department of Home Affairs' Commonwealth Security Policy Branch at PSPF@homeaffairs.gov.au, and
2. The relevant Authorised Vetting Agency.

Further information about foreign interference and espionage risks arising from personnel disclosing information that identifies or alludes to their access to security classified material on online platforms, is detailed in:

- Policy Explanatory Note 004-2025 - Managing Online Disclosure of Security Clearance and National Security Information, and
- PSPF Policy Advisory 002-2025 - Online Disclosure of Security Clearance and National Security Information.

For further information, contact PSPF@homeaffairs.gov.au.

Stephanie Foster

Stephanie Foster PSM
Secretary
Department of Home Affairs
7 October 2025

[4] *'Security Clearance Information' constitutes any information confirming or suggesting security clearance level, security vetting agency, or any other information that could identify a person as holding a security clearance.*

[5] *'Designated high-risk position' constitutes personnel who are identifiable as having access to, or transferable knowledge of, highly-secure entity and industry facilities, platforms and personnel, such as Department of Defence-related programs or industries, intelligence functions, or undeclared locations.*