Australian Government

Australian Security Intelligence Organisation

Clearance holder obligations







Clearance maintenance obligations

The **Commonwealth Government Protective Security Policy Framework (PSPF)** contains the controls used by the Australian Government to protect its people, information and assets and clearance holders have obligations in order to maintain their clearance.

Clearance holders must maintain a standard of behaviour the public would expect from someone in a position of trust. This includes:

- acting with **honesty and integrity**
- acting in accordance with Australian laws, regulations and determinations
- avoiding excessive alcohol consumption
- not taking illegal recreational or non-prescribed prescription drugs.

In order to retain an Australian Government clearance, holders must meet other obligations including (but not limited to):

- reporting changes in personal circumstances
- reporting suspicious or unusual contact by an individual or group – **regardless of nationality**
- reporting suspicious or unusual occurrences around the workplace, including colleagues' behaviours
- disclosing and **avoiding real or apparent conflicts of interest**, financial or otherwise
- disclosing personal information when required.



Reporting changes of circumstances

The granting of your security clearance is based on a snapshot of you as a person at a point in time, but your personal circumstances, behaviours and attitudes will continue to evolve.

Employers need to be made aware of such changes so they can provide the necessary support to their staff and prevent small issues from becoming large problems.

The consequences of not reporting

As a clearance holder, your access to privileged information and other security clearance holders makes you a potential target of foreign governments, criminal organisations, issue-motivated groups, commercial organisations and others. They can take advantage of life changes that are unknown to your employer, which may then lead you to be increasingly vulnerable to blackmail, deliberate breaches of security, acts of fraud or corruption.

Examples of what to report

- changes of name/identity, including gender
- changes in citizenship or nationality
- changes in personal relationships, such as marital status or family structure (birth/adoption of children)
- changes of address or living arrangements
- changes in financial circumstances (mortgage, debt, change to income or financial windfall)
- changes in health or medical circumstances
- new social media accounts
- involvement or association with any group, society or organisation that may be of security concern
- changes in criminal history, involvement with police or association with criminal activity
- disciplinary procedures, including professional misconduct and deregistration from a professional body
- alcohol, drug or gambling problems
- personal overseas travel (in accordance with your agency's security plan)
- identity document replacement following a cyber hack (drivers licence, passport and Medicare card)
- any other changes having a significant impact on your personal circumstances.

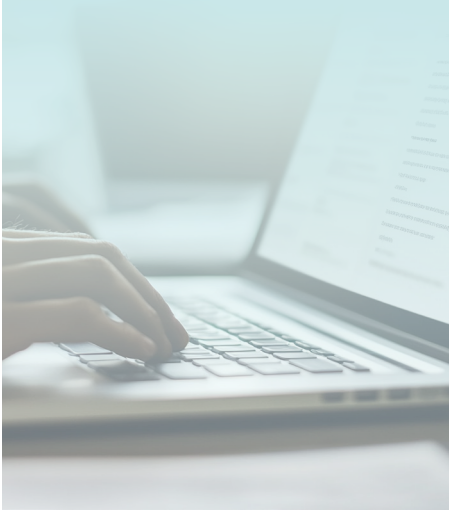
The full list of what to report is listed on the PSPF website: **www.protectivesecurity.gov.au**



How to report

Contact your **Agency Security Adviser (ASA)** or equivalent security personnel.

They will assist in determining if a particular change of circumstance or a particular contact needs to be reported to your employer and ASIO. **Reports will be treated in the strictest confidence**.



Reporting foreign contacts

The Australian Government Contact Reporting Scheme is a whole-of-government counter-espionage strategy managed by ASIO as part of the PSPF. As a clearance holder, you are required to complete a contact report when you experience questioning or contact from a foreign national that seems **suspicious, ongoing, unusual or persistent (SOUP)** in any way.

The contact of concern may be official, as part of your work role, or via social or electronic media. It is not necessary to report official contact that resulted in a corporate record detailing the topics discussed and who attended. **A contact report is required when a foreign national seeks to establish ongoing social or electronic contact outside official channels.**

For example:

- requests via social networking sites, VoIP apps (WhatsApp, Skype, Signal etc.) and dating apps
- phone calls, including unsolicited phone calls where the caller has obtained the employee's details from the internet
- invitations to attend functions
- written correspondence and email requests
- through sporting or recreational activities
- offers of overseas travel
- visits to embassies or consulates, or involvement with trade missions or other international events
- via membership of international clubs, institutes, professional associations or friendship societies
- through training or study (for example, language classes)

How to report

Government workers and security clearance holders:

- contact your Agency Security Adviser and fill out a contact report

Other workers:

- use ASIO's Notifiable incidents, Threats or Reportable Observations (NITRO) portal at nitro.asio.gov.au





Minimising your online profile and risk of being exploited

Seemingly innocuous information shared online can be used by Australia's adversaries to target you for cultivation or recruitment.

How to protect yourself online:

- Consider the type and amount of information you post on **professional networking sites** (such as LinkedIn) or share in resumes about your work duties or whether you hold a clearance. Do not post information from your current or previous roles that is **not for public release**, such as projects and specialised systems.
- **Restrict personal information on social media**. This can include posting identifying details (like addresses and phone numbers) and sharing financial struggles, relationship issues or work dissatisfaction. Avoid location-based posts – including those with photos – which can reveal your routines and whereabouts.
- Avoid disclosing your full name if possible.
- Monitor the information friends and colleagues post about you on social media websites to prevent the unauthorised disclosure of your personal information.
- Consider limiting access on social media websites to 'friends only'.
- Always use a personal email address rather than a work email address when creating personal profiles.
- Apply any available **security and privacy options** to your accounts and use a 'private' profile where available.



- Where possible, 'opt out' of social media websites that allow search engines to search and display your personal information.
- Review social media sites' **security and privacy policies** regularly, as these can change with minimal communication to users.
- Exercise caution when accessing online accounts, social media or otherwise, from public computers or networks (for example, internet cafes or public wi-fi).
- Be wary of unsolicited contact through social media or email which may be a scam or an approach.
- Report to your ASA (or equivalent security personnel) any incidents where you **identify or suspect sensitive or classified information on social media or websites** about other personnel.
- Report any suspicious contact made to you or colleagues through social media websites or applications.

Further advice on protecting yourself online can be found via the Australian Government resource webpage:
cyber.gov.au/protect-yourself



Complying with your obligations

Compliance with your obligations is assessed not just during revalidation but at other times to ensure you remain eligible to hold a clearance. If you meet your obligations, it demonstrates your trustworthiness and responsibility, which supports your suitability to continue holding the clearance. Failing to meet your obligations, such as not reporting foreign contacts or changes in your financial circumstances, can raise concerns about your judgement and reliability. This can potentially lead to clearance revocation or denial.

To update personal circumstances:

- contact your ASA or equivalent security personnel

How to Report

Government workers and security clearance holders:

- contact your Agency Security Adviser and fill out a contact report

Other workers:

- use ASIO's Notifiable incidents, Threats or Reportable Observations (NITRO) portal at nitro.asio.gov.au
- call the National Security Hotline on 1800 123 400





asio.gov.au

25-0244