7 Security governance for international sharing

A. Purpose

1. This policy details protections for valuable information and assets under international sharing agreements or arrangements to which Australia is a party.
2. These international agreements or arrangements also help to safeguard Australian information and assets when shared with foreign partners.

Legislative provisions on international sharing

Communicating, or making available, classified information with another country or foreign organisation could be considered espionage under the Criminal Code.

However, specific legislative provisions[1] authorise entities to share information internationally under arrangements made or directions given by the relevant minister.

B. Requirements

B.1 Core requirement

Each entity must adhere to any provisions concerning the security of people, information and assets contained in international agreements and arrangements to which Australia is a party.

B.2 Supporting requirements

Supporting requirements for security governance for international sharing

#	Supporting requirement
Requirement 1. Sharing information with a foreign entity	a. When an entity shares sensitive or security classified Australian Government information or assets with a foreign entity there **must** be an explicit legislative provision, an international agreement or an international arrangement in place for its protection. b. The following limitations apply, even when an international agreement or international arrangement is in place: i. entities **must not** share Australian Government information bearing the Australian Eyes Only (AUSTEO) caveat with a person who is not an Australian citizen, and ii. entities, other than the Australian Signals Directorate (ASD), Australian Security Intelligence Organisation (ASIO), Australian Secret Intelligence Service (ASIS), Department of Defence and Office of National Assessments **must not** share Australian Government information bearing the Australian Government Access Only (AGAO) caveat with a person who is not an Australian citizen.
Requirement 2. Safeguarding foreign information	Where an international agreement or international arrangement is in place, entities **must** safeguard sensitive or security classified foreign entity information or assets in accordance with the provisions set out in the agreement or arrangement.

[1] For example, section 19 of the *Australian Security Intelligence Organisation Act 1979* allows for cooperation with authorities of other countries approved by the minister as being capable of assisting in the performance of ASIO's functions.

3. A foreign entity includes a foreign government and foreign contractors (meaning any individual or legal entity entering into or bound by a classified contract and includes subcontractors).

C. Guidance

C.1 International security agreements and arrangements

4. Australia has international treaty-level agreements, or less-than-treaty-status arrangements, that provide for equivalent international protection of Australian Government security classified information or assets (some also cover protection of sensitive unclassified information):
   a. An international agreement constitutes a treaty and is binding under international law.
   b. An international arrangement has less-than-treaty status, such as a Memorandum of Understanding, and does not create legal rights or obligations. Arrangements do, however, create commitments that are politically and morally binding.
5. The Australian Government takes, wherever possible, a whole-of-government approach to international information sharing agreements. This builds consistency across government and is preferable to entity-to-entity-level agreements and arrangements. Existing whole-of-government international agreements for the security of information and assets exist between Australia and the following:
   a. European Union (EU)
   b. Japan
   c. Republic of France
   d. United States of America (US).
6. Australia also has agreements or arrangements with each of Australia's Five Eyes partners (US, United Kingdom, New Zealand and Canada).[2] These partners share similar security cultures and structures and the agreements or arrangements are based on high levels of trust and longstanding relationships and practices.
7. Some Australian entities, such as the Department of Defence, have specific entity-to-entity-level treaties that enable classified information sharing and provide certain protections.[3] Other entities have arrangements that provide similar entity-to-entity-level assurances and protections (including for ad hoc or one-off sharing). These arrangements can vary in format and substance, for example letters of assurance.
   a. It is important that entities have appropriate written arrangements in place that adhere to whole-of-government requirements and established classification alignment.

C.1.1 Key provisions in international security agreements and arrangements

8. International agreements or arrangements covering protective security matters commonly include provisions relating to:
   a. marking of sensitive and security classified information and assets
   b. protection of sensitive and security classified information and assets, including how they are handled and transferred
   c. access to and disclosure of sensitive and security classified information and assets, including personnel security clearance requirements and recognition
   d. responding to breaches or security violations
   e. undertaking security inspections and visits.
9. Many international agreements and arrangements include provisions for classified contracts. Before an entity engages a foreign contractor on a classified contract, it is important that an international agreement or arrangement is in place if the contract involves sharing classified information or assets.

[2] In some cases, these are at an entity-to-entity level and are less formal arrangements, such as letters of assurance.
[3] The Department of Defence has agreements with Canada, Denmark, New Zealand, Singapore, South Africa and Sweden for reciprocal protection of classified information.

10. Where Australia engages foreign industry on a classified contract, under General Security Agreements the foreign government is generally responsible for administering security requirements (such as providing facility and personnel security clearances) and for ensuring the security conduct of contractors within its territory.

C.1.2 Key governance roles in international sharing

11. The Attorney-General's Department establishes whole-of-government priorities for international agreements and arrangements. As the National Security Authority for the Australian Government, it is responsible for general oversight and administration of international General Security Agreements. This includes determining the policy for protecting and sharing sensitive or classified information and assets.

12. Some agreements give particular Australian Government entities (referred to as Competent Security Authorities) responsibility for administering international agreements or arrangements in specific fields. For example, the Department of Defence is a Competent Security Authority for defence matters.

13. Entities wanting to negotiate a treaty, or an instrument of less than treaty status, including treaties or instruments that involve national security issue, must be aware of their obligations under the *Legal Services Directions 2017*. The Directions tie certain categories of legal work to specified providers unless approval to use a non-tied provider is obtained. This includes that legal advice preparatory to, or in the course of, treaty negotiations (which includes negotiation of instruments of less than treaty status) must be sought from the Office of International Law in the Attorney General's Department, the Australian Government Solicitor or the Department of Foreign Affairs and Trade (as required under the Directions), unless approval is otherwise obtained

14. Entities establishing new agreements and arrangements are encouraged to contact the Attorney-General's Department (PSPF@ag.gov.au) to discuss their information sharing requirements. This consultation process establishes consistent protections for security classified information (such as equivalent classifications) and identifies whole-of-government policy issues.[4]

C.1.3 Sharing information and assets without an agreement or arrangement

C.1.3.1 Sharing information internationally under an explicit legislative provision

15. The security and protection of information is crucial, even where explicit legislative provisions authorise certain entities to share information internationally.

16. The Attorney-General's Department recommends that entities sharing information internationally under a legislative provision take appropriate measures to protect that information. If it is not viable to establish an international agreement or arrangement, it is recommended entities include appropriate handling instructions on all information to be shared or, alternatively use ad hoc sharing arrangements (see C.1.3.2).

C.1.3.2 Other sharing

17. **Requirement 1** prevents sharing of security classified Australian Government resources with a foreign entity unless explicit legislative provisions, international agreements or arrangements for protection of classified information and assets are in place.

    a. This requirement ensures appropriate mutual arrangements for the protection of information have been considered and agreed. Risk-based approaches to ad hoc or one-off sharing of classified information can be through arrangements such as a letter of assurance or using temporary access provisions under the PSPF policy: Access to information. The Attorney-General's Department recommends that ad hoc arrangements are:

        i. documented

        ii. for a limited time period

        iii. for a specific purpose, project or activity.

[4] For example, when negotiating an international agreement on information sharing with a foreign government that has the death penalty.

b. In all other circumstances, sharing classified information with a foreign national or international entity may be in breach of **Requirement 1**. For guidance on investigating, responding to and reporting on security breaches, see section C.5 and the PSPF policy: Management structures and responsibilities.

18. Where foreign entity information or assets are received, but are not covered by an international agreement or arrangement, the Attorney-General's Department recommends applying an Australian Government security classification. Application of an Australian security classification is based on an assessment of the value and sensitivity of the information asset in accordance with the PSPF policy: Sensitive and classified information. The Attorney-General's Department also recommends applying the following protections:

a. ensuring individuals who access foreign entity information hold a security clearance at the appropriate level

b. limiting access to the foreign entity information or assets to individuals with a need to know

c. protecting the foreign entity information or assets from unauthorised access

d. transmitting the information by secure means

e. seeking approval from the originating government before releasing their information to any other foreign government or foreign entity.

C.2 Identifying sensitive and classified information and assets from foreign entities

19. Classifications reflect each government's assessment of the possible harm to the national interest, organisations or individuals that could be caused by the unauthorised disclosure or compromise of classified information or assets and indicate the level of protection required. Where equivalent classifications between foreign and Australian Government information or assets are established, international agreements or arrangements require entities to stamp, mark or otherwise designate the foreign information with the corresponding Australian security classification.

20. For guidance on marking sensitive and classified information, see the PSPF policy: Sensitive and classified information.

Table 1 Australian Government information and asset classification equivalencies [Note i]

Australian classification	French equivalent [Note ii]	US equivalent	EU equivalent	Japanese equivalent
TOP SECRET	TRÈS SECRET DÉFENSE	TOP SECRET	TRÈS SECRET UE / EU TOP SECRET	Kimitsu 機密 Bouei Himitsu (Kimitsu) 防衛秘密(機密)
SECRET	SECRET DÉFENSE	SECRET	SECRET UE	Gokuhi 極秘 Bouei Himitsu 防衛秘密
CONFIDENTIAL [Note iii]	CONFIDENTIEL DÉFENSE	CONFIDENTIAL	CONFIDENTIEL UE	Hi 秘
PROTECTED	Handled as CONFIDENTIEL DÉFENSE			
No equivalence established	No equivalence established	No equivalence established	RESTREINT UE [Note iv]	No equivalence established

Table 1 notes:

[i] This table identifies established equivalencies to Australian classifications only. The equivalencies do not apply between the other foreign entities listed.
[ii] The agreement with France also establishes equivalent protections for sensitive but not classified information.
[iii] The Australian CONFIDENTIAL classification will be discontinued over the period from October 2018 to October 2020.
[iv] Implementation arrangements available from DFAT specify the handling requirements for RESTREINT UE.

21. In addition to the security classification, the Attorney-General's Department recommends marking foreign entity information and assets with the caveat RELEASABLE TO. This identifies the source of information or asset and restricts release to certain nationalities.

22. For guidance on how to mark information with a caveat, see the PSPF policy: Sensitive and classified information.

C.3 Handling protections for sensitive and classified information and assets from foreign entities

23. International agreements or arrangements require entities to handle foreign entity information and assets using the safeguards protecting equivalent Australian Government information or assets.

24. The Attorney-General's Department recommends entities review the relevant international agreement or arrangement to identify additional obligations or protections that may differ from the PSPF core requirements.

25. It may be an offence under the *Crimes Act 1914* or Criminal Code to share information with a foreign person or entity inappropriately. Sound record keeping that demonstrates the appropriateness of information sharing is recommended. The Attorney-General's Department suggests entities implement processes for sharing Australian Government security classified information with a foreign entity or person that includes:

    a. obtaining appropriate authorisation prior to sharing information (approval at the Senior Executive Service level is recommended)

    b. making the purpose of the information sharing clear

    c. keeping a record of the information transfer

    d. maintaining a register, where appropriate, of all security classified Australian Government information shared, even if a register is not prescribed in the agreement or arrangement (including the date of sharing, recipient of the information, description and classification of the information shared and reason for sharing is recommended).

26. For guidance on handling and operational requirements for sensitive and classified information, see the PSPF policy: Sensitive and classified information.

C.4 Security clearances for access to, release and disclosure of foreign entity information and assets

27. The PSPF policy: Access to information requires that access to sensitive or classified information is restricted to those who have appropriate security clearances and need to know that information. This security clearance requirement applies to foreign entity information. Access is based on the security clearance required for the corresponding Australian Government security classification:

    a. The General Security Agreement with France expressly provides for mutual recognition of each country's security clearances for access to classified information. This enables flexibility when engaging outside formalised processes with French Government personnel and contractors who deal with sensitive or classified information. This also opens up industry engagement between France and Australia across government sectors. An official government visit is not required for clearance recognition to be arranged. Authorised vetting agencies, such as the Australian Government Security Vetting Agency, provide specific advice on arrangements for verifying a clearance with the foreign authority.

    b. Entities may recognise clearances issued by Five Eyes country governments (US, United Kingdom, New Zealand and Canada) and consequently issue corresponding Australian clearances for specific operational purposes.

    c. Other international agreements and arrangements do not expressly provide for mutual recognition of clearances. Instead, the international agreements and arrangements include provisions outlining personnel security clearance vetting provisions each party is required to apply. Recognising a foreign clearance is only possible as part of an official government visit by the other party. Authorised vetting agencies, such as the Australian Government Security Vetting Agency, can provide specific advice on vetting foreign nationals or on verifying a clearance with the foreign authority.

28. Under the PSPF policy: Access to information, the Attorney-General's Department recommends obtaining originator agreement for third-party access to classified information. In line with this, international agreements or arrangements commonly require written approval from the originator (the foreign government) for release of classified information to any other third-party government or foreign entity. If these provisions are not included in an agreement, the Attorney-General's Department recommends written approval from the originating foreign government before releasing information to any other foreign government or foreign national.
29. The release of classified foreign government information under the *Freedom of Information Act 1983* (FOI Act) is not required. Under section 33(b) of the FOI Act, any information of a foreign government communicated in confidence to the Australian Government is an 'exempt document'. However, classified or sensitive foreign government information is not exempt from legal processes. The Attorney-General's Department recommends that entities involved in legal processes where foreign government information is, or is likely to be, relevant:
    a. seek legal advice on issues of relevance, disclosure and protection (including claims of public interest immunity)
    b. seek foreign government permission to disclose the information, noting that disclosure may still be required under Australia's domestic legal proceedings even if permission is not obtained.
30. For guidance on access to sensitive and security classified information, see the PSPF policy: Access to information.

C.5 Breaches or security violations involving foreign entity assets and information

31. Under the PSPF policy: Management structures and responsibilities, Chief Security Officers (or appropriate security advisor delegates) investigate, respond to and report on security incidents:
    a. Sharing classified Australian information and assets inappropriately with a foreign national or international entity without the protection of an agreement or arrangement may be in breach or violation of **Requirement 1** and may be an offence under the *Crimes Act 1914* or Criminal Code. Ensuring all instances of international information sharing without agreement or arrangement are reported to the entity Chief Security Officer (or appropriate security advisor delegate) will assist security incident investigations.
    b. Failing to safeguard sensitive or security classified foreign entity information or assets covered by an international agreement or arrangement may be in breach or violation of **Requirement 2**. Security breaches or violation incidents can involve the actual (or suspected) compromise of foreign entity classified information or assets. The Attorney-General's Department recommends entities report security incidents to the originating foreign government as soon as they are able.
32. International agreements or arrangements may impose additional reporting and security violation handling requirements beyond those detailed in the PSPF.

C.5.1 Foreign access to information caveated 'Australian Eyes Only' is a security incident

33. The Australian Eyes Only (AUSTEO) caveat denotes Australian Government information that is restricted to Australian citizens exclusively. This includes Australian citizens who also hold other nationalities, such as dual nationals. **Requirement 1** information sharing limitations are that information bearing the AUSTEO caveat cannot be shared with a person who is not an Australian citizen, even when an international agreement or arrangement is in place. As such, foreign access to AUSTEO caveated information is a security incident requiring Chief Security Officer (or appropriate security advisor delegate) investigation, response and reporting.
34. The Australian Government Access Only (AGAO) caveat denotes information that is restricted to Australian officers or representatives of foreign governments from Five Eyes countries who are on exchange, long-term posting or attachment to the Australian Government. For entities outside the Australian Signals Directorate, Australian Security Intelligence Organisation, Australian Secret Intelligence Service, Department of Defence and Office of National Assessments, information caveated AGAO is considered to be also caveated AUSTEO. As such, foreign access to caveated information is a security incident.

C.6 Foreign personnel conducting security assessment visits

35. Some international agreements or arrangements allow security assessment visits where foreign personnel access secure areas or facilities. The purpose of these visits is to assure foreign governments of the suitability and implementation of security procedures and the protection of areas or facilities where their information is stored and handled.

36. International agreements and arrangements commonly require that security assessment visits have prior written approval from the Attorney-General's Department or a Competent Security Authority. Visits will only be approved for foreign government personnel who have a valid level of Australian or foreign government security clearance for access to the foreign government information in the facility.

D. Find out more

The Australian Treaties Database provides further details of international agreements to which Australia is a party, including entity and subject-specific agreements. However, not all international arrangements are publicly available. In such cases, entity security advisors may be able to assist in determining if there is a relevant international arrangement in place.

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
V2018.2	Jan 2019	C.1.2	Revised to provide additional information on obligations in the *Legal Services Directions 2017*.