6 Security governance for contracted goods and service providers

A. Purpose

1. This policy provides information about assessing and managing security risks that arise from procuring goods and services. While procurement offers benefits (eg scalability, elasticity, performance, resilience and cost efficiency), the security risks of procuring goods and services need effective management to reduce the likelihood of additional financial and non-financial costs to government.
2. This policy supports the Commonwealth Procurement Rules (the rules) that govern how entities procure goods and services. The rules seek to achieve value for money and consideration of the financial and non-financial costs and benefits.

Relevant Commonwealth Procurement Rules[1]

Relevant entities **must** establish processes for the identification, analysis, allocation and treatment of risk when conducting a procurement. The effort directed to risk assessment and management should be commensurate with the scale, scope and risk of the procurement. Relevant entities should consider risks and their potential impact when making decisions relating to value for money assessments, approvals of proposals to spend relevant money and the terms of the contract.

Relevant entities should consider and manage their procurement security risk in accordance with the Australian Government's Protective Security Policy Framework.

B. Requirements

B.1 Core requirement

Each entity is accountable for the security risks arising from procuring goods and services, and must ensure contracted providers comply with relevant PSPF requirements.

3. The Commonwealth Procurement Rules Appendix B: Definitions states that a contract is 'an arrangement, as defined by s23(2) of the PGPA Act, for the procurement of goods and services under which relevant money is payable or may become payable. Note: this includes standing offers and panels'.

B.2 Supporting requirements

4. Balancing the effort directed to risk assessment and management with the scale, scope and risk of the procurement is important (eg the procurement of tables or chairs will have a relatively minor protective security effort). This is significant because procurement of goods and services does not transfer the operational risk from the Commonwealth. The supporting requirements help entities consider security risks when undertaking procurement and applying relevant PSPF requirements.

[1] Commonwealth Procurement Rules paragraphs 8.2-8.3

Supporting requirements for security governance for contracted goods and service providers

#	Supporting requirement
Requirement 1. Assessing and managing security risks of procurement	When procuring goods or services, entities **must** put in place proportionate protective security measures by identifying and documenting: a. specific security risks to its people, information and assets, and b. mitigations for identified risks.
Requirement 2. Establishing protective security terms and conditions in contracts	Entities **must** ensure that contracts for goods and services include relevant security terms and conditions for the provider to: a. apply appropriate information, physical and personnel security requirements of the PSPF b. manage identified security risks relevant to the procurement, and c. implement governance arrangements to manage ongoing protective security requirements, including to notify the entity of any actual or suspected security incidents and follow reasonable direction from the entity arising from incident investigations.
Requirement 3. Ongoing management of protective security in contracts	When managing contracts, entities **must** put in place the following measures over the life of a contract: a. ensure that security controls included in the contract are implemented, operated and maintained by the contracted provider and associated subcontractor, and b. manage any changes to the provision of goods or services, and reassess security risks.
Requirement 4. Completion or termination of a contract	Entities **must** implement appropriate security arrangements at completion or termination of a contract.

C. Guidance

C.1 Assessing and managing security risks of procurement

5. A key determinant of value for money is achieving quality security outcomes. When an entity outsources the provision of goods or services, accountability for the goods or service and associated delivery outcomes (including managing security risks) remains with the entity.

6. An entity is accountable for the security risks arising from its procurement of goods and services. However, goods and service providers can also play an important part in identifying and addressing security risks. The Commonwealth Procurement Rules state that risks are most effectively borne by the party best placed to manage them. As such, if an entity is best placed to manage a particular risk, it would be inappropriate to transfer that risk to the supplier.

7. The Commonwealth Procurement Rules state that risk is required to be considered in all procurements. Entities are encouraged to specifically consider and manage any associated protective security risks. This includes:

   a. identifying mandatory and desirable security requirements in procurement request documents, including any specific provisions relating to subcontracting

   b. using relevant protective security terms and conditions in procurement contracts

   c. managing the ongoing delivery of security requirements for contracted goods and service providers

   d. implementing appropriate security arrangements at completion or termination of contracts.

C.1.1 Identifying risks

8. **Requirement 1** mandates entities identify and document the mitigations for security risks associated with any procurement. If identified security risks cannot be mitigated to an acceptable level or the security risks to government are too great, entities are encouraged to seek alternative procurement arrangements and maintain a record of such decisions. This includes where the security risks:

   a. cannot be quantified

   b. are too complex to be calculated.

9. Understanding relevant threats and vulnerabilities associated with a procurement helps entities identify suitable security treatments. For example, procuring cloud technologies may appear a more affordable and faster alternative to other ICT solutions. However, it could require specific contract clauses and operational controls to mitigate risks associated with storing information in a foreign country.

Case Study – Potential data centre ownership changes

An entity outsources its data holdings to a service provider. While the provider's data facility is physically located in Australia, the entity identifies a potential risk of foreign interference and malicious insider threat.

To help mitigate the identified security risks, the entity includes conditions in the contract regarding changes in ownership and management. Mitigations of foreign interference risks include:

- requiring advice on any ownership changes (including of subsidiaries), or changes to ownership structure, operational management and day-to-day control, and contracting arrangements for companies with access to the data facility
- permission to cancel or amend the contract, remove servers and data or associated equipment, recover records (or maintain protective security measures if records cannot be returned) without penalty if there is a change in ownership or management
- requiring Australian citizenship for the service provider's operational managers
- co-locating services with the service provider having no technical access to the entity's data
- requiring no offshore control or access to infrastructure, systems and entity data.

During the life of the contract, the cloud facility is subsequently sold to a foreign investor. Security provisions in the contract allow the entity to discontinue use of the data centre when ownership changed.

10. **Table 1** provides examples of potential procurement risks an entity may consider when entering into contractual arrangements.

Table 1 Examples of potential risks associated with procuring goods or services

Risk type	Risk description
Foreign involvement	Outsourcing can be cost-effective for providing goods or services. However, it can also affect an entity's risk profile and control over its threat environment. Entering into an arrangement where resources are made or held offshore (either by the contracted provider or a subcontractor) can have additional risks. For example, services located offshore are subject to the laws of those countries and may be subject to lawful and covert collection. The nature of the legal powers to access, or restrict access, to government resources held in foreign countries may differ.
Differences in the business and legal cultures in other nations	The difference in the business and legal cultures in other countries may give rise to additional risks, affecting the confidentiality, availability and integrity of Australian Government resources. For example: a. the tolerance (legal and law enforcement effectiveness) and acceptance of corruption and crime differ across countries b. foreign enterprises owned, influenced or funded by foreign governments c. a lack of visibility into the suppliers' corporate structures, funding or use of non-reciprocating safe harbours. Similarly, the extrajudicial behaviour of foreign governments and the ability of citizens to refuse those demands may be limited, potentially giving rise to further risks that need consideration. A lack of effective rule of law may encourage attempts to misappropriate information or assets (including by organised crime).

Risk type	Risk description
Complications arising from the simultaneous application of multiple legal jurisdictions	Complications may arise from information being subject to the laws of multiple jurisdictions. This may occur in circumstances where: a. foreign laws apply to a supplier because it is located offshore, sometimes in multiple locations b. foreign laws have an extra-territorial application to a supplier located in Australia c. the goods or services provided by the supplier pass through a foreign jurisdiction. Most foreign jurisdictions have legislative powers that allow access to assets, communications and stored information for the purposes of law enforcement and national security. In some cases, these laws allow international law enforcement and national security agencies to access information and assets held overseas or in Australia. Any qualified assurances and controls provided by the supplier will need to align with entity risk profiles to ensure that information and assets are managed securely.
Complications from multiple delivery entities/ contractors (supply chain)	In some cases, an entity may engage multiple providers to deliver goods or services, or a contracted provider may engage multiple subcontractors as part of a supply chain. Engagement of multiple partners inherently increases the complexity, and associated security risks, of a procurement. In addition, transparency of (and control over) operations is more challenging the further down a supply chain it is from government. The Attorney-General's Department recommends: a. considering security risks of each contracted provider independently and holistically across all contracted and subcontracted partners b. reducing vulnerabilities and ensuring security continuity to manage risks along the whole supply chain.
Insider threat	Australia is exposed to persistent and sophisticated exploitation. Allowing access to entity resources can diminish an entity's mitigation of threats. The incentives and capability to conduct malicious insider activity may be exacerbated by: a. increased motivation i. Australia is an attractive target for exploitation due to its prominent role in the Asia-Pacific region, its strong diplomatic, defence and intelligence relationship with the United States, its resource industries and expertise in research and development fields. ii. Entity resources (particularly exploited information or assets) could be used to gain economic, diplomatic or political advantage against Australia. For example, stolen intellectual property can be used to gain access to new technologies while circumventing costly and lengthy research and development programs. Personal information (such as financial or medical records) could be used for malicious activities through social engineering. iii. State-sponsored actors working on behalf of a foreign entity are sophisticated and active malicious adversaries. They seek national security information to identify vulnerabilities or gain advantage and often target Australia's commercial sectors (eg resources, banking and telecommunications). b. ease of acquiring capability i. Technical capability is increasingly sophisticated with malicious tools, information and supporting guidance readily available. The ease of acquiring capability, coupled with the potential high gains (e.g. financial, economic, diplomatic or political) may entice malicious activity by insiders (and others). c. new technologies generating new vulnerabilities i. Technological advancements (such as the growth in cloud computing and mobile devices like smartphones, laptops and tablets) generate platforms with distinct software, settings and applications. A greater number of trusted insiders using new technologies may increase vulnerability to exploitation.

11. When undertaking a risk assessment of procurement in line with **Requirement 1**, it is important that entities consider (at a minimum):

    a. national interest

    b. risks to critical infrastructure

    c. risks to those transacting with the entity through a contracted provider

d. the ability to manage and control resources in an outsourced, offshore or supply-chain arrangement with potentially changing legal frameworks

e. foreign involvement

f. the insider threat

g. informing associated entities of relevant risks, relevant treatments and the likely effects where there are multiple government stakeholders

h. security plans as a ready source of information on risks to entity information, see the PSPF policy: Security planning and risk management.

12. Refer to the Australian Security Intelligence Organisation for assistance managing national security risks, in particular the Business and Government Liaison Unit. Some threat assessment products are also available and may form part of an entity's assessment of protective security risks associated with the procurement. Refer to the Critical Infrastructure Centre for assistance managing critical infrastructure risks.

Case study – outsourced ICT service provider

An entity has a contract to purchase phones from a telecommunications provider. In delivering the services, key phone components are sourced from a foreign supplier.

A significant security risk is the potential compromise of the phone components as well as the entity's limited influence and control over the foreign supplier.

C.2 Protective security terms and conditions in contracts

13. **Requirement 2** mandates that contracts for goods and services include relevant security provisions and appropriate protections. To achieve this, entities are encouraged to include terms and conditions in their procurement documents (such as requests for tender and subsequent contracts) relating to:

a. imposing appropriate information, physical and personnel security requirements

b. identified security risks relevant to the procurement

c. ongoing management of security matters (refer to section C.3).

14. Written contracts between two or more parties outline each party's rights and obligations. The benefit of having a contract identifying relevant security terms and conditions is that they are legally enforceable.

15. The Attorney-General's Department recommends entities establish robust governance and assurance processes so that contracted providers implement applicable protective security requirements. These may include:

a. applying relevant personnel security provisions such as security clearance vetting requirements for people accessing classified Australian Government resources (applying the same security measures to contracted provider personnel as an entity would to its employees)

b. applying relevant information handling controls and storage arrangements to protect sensitive or classified information (requiring contracted goods and service providers to protect Australian Government information resources in the same manner as an entity would)

c. applying relevant physical security measures for protection at facilities where government resources are held and facilities where goods are prepared for government use, as well as addressing all hazards an entity may face in the protection of its people, information and assets (including requiring contracted goods and service providers to apply protection against national security threats).

d. establishing governance arrangements to manage ongoing protective security requirements (during the contract and at the completion or termination of the contract). This includes permissions for entities to:

i. amend (or terminate) a contract where issues of national interest arise (eg procedures to address actual or suspected security incidents or breaches, or a change of ownership of supplier that is not approved)

ii. monitor ongoing contracts (eg access to premises, records and equipment) through all levels of subcontracted supply chains

iii. manage changes to the provision of goods or services

iv. terminate the contract if the provider fails to comply with provisions in the contract, including where there is unwillingness or inability to remedy or mitigate security incidents.

e. assurances that the 'primary' contracted provider:

i. immediately notify the entity of actual or suspected security incidents and follow direction from the entity in relation to incident investigations, including providing assistance to rectify the situation. Where entities jointly hold personal information (such as an entity and contracted provider), both entities have obligations to notify the Office of the Australian Information Commissioner and affected individuals in the event of an eligible data breach. For guidance on managing these obligations, see Data breaches involving more than one organisation

ii. take reasonable steps to prevent, detect and respond to fraud and corruption

iii. implement security arrangements to manage risks corresponding to the material and/or property provided by the entity (including personnel, information and physical security measures required to protect the material and property at all times from unauthorised access, misuse, loss, interference, unauthorised modification and unauthorised disclosure)

iv. periodically review its security arrangements under the contract to ensure the arrangements are current and address the risks and security environments

v. is responsible for managing and monitoring protective security of its subcontractors, including supply-chain arrangements.

Case study – contractor personnel security

An entity considers using cleaning services from a cleaning company as opposed to directly employing cleaners. The cleaning company employs Australian and non-Australian citizens.

Cleaners will have access to secure physical zones and may have contact with sensitive and classified information up to and including the PROTECTED classification level.

The entity includes contract conditions requiring the provider to adhere to requirements for appropriate access to classified resources under the PSPF policy: Access to information. This includes taking steps to obtain the required security clearance for ongoing access to security classified information such as where contact exceeds the maximum allowable limit of three months temporary access over a 12 month period. Contract conditions also require the provider to report instances where uncleared contracted cleaners have contact with security classified material, this assists the entity to monitor security incidents.

Case study – contractors handling sensitive information

A non-corporate Commonwealth entity, in its role as a regulatory authority, outsources services to an external consultancy to assess and confirm the financial income, assets and expenditure of a third-party entity as part of the annual compliance process.

This process involves transmission and sharing of sensitive information between the non-corporate Commonwealth entity and the outsourced service provider. The non-corporate Commonwealth entity ensures tender documentation and contracts include clauses stating what and how the information is to be shared, transferred, stored and disposed of.

16. **Annex A** includes examples of considerations when developing contract clauses.

17. For guidance material and templates to assist in developing legally binding agreements (such as contracts or deeds), an entity may wish to:

a. seek legal advice

b. contact the Department of Finance for policy advice in relation to general procurement in government via procurementagencyadvice@finance.gov.au and refer to www.finance.gov.au/procurement and the Commonwealth-contracting-suite for further information

c. contact the Digital Transformation Agency at ictprocurement@dta.gov.au for information about ICT procurement in government and for access to the ICT Procurement Portal in DTA.

C.3 Ongoing management of protective security in contracts

18. Security environments and risks constantly change. Sound contract management provides ongoing oversight and management and helps adherence to essential security requirements of contracts.

19. Entities are encouraged to evaluate compliance with contract conditions by performing ongoing assessments (such as regular inspection of premises used to store Australian Government information or assets, or an ongoing accreditation program). Identifying a contract manager who is responsible for monitoring and reviewing risk for each contract can assist in this process.

C.3.1 Monitoring and reviewing risk

20. Changes in the entity's risks, as well as its internal and external security environment, may necessitate a flexible approach to contracts and their management.

21. When implementing **Requirement 3**, key questions for entities to ask when monitoring and reviewing risk may include:

    a. Have positive working relationships been established with the contracted provider to promote open communication? Are issues being identified and resolved in a prompt manner?

    b. Is the contracted provider advising employees (including subcontracted providers and their personnel) of the protective security conditions that apply under the contract?

    c. Have the premises been inspected prior to the commencement of the contract to verify that protective security measures specified in the contract comply with the PSPF? Has there been periodic reinspecting of contracted providers' and subcontractors' premises during the life of the contract, specifically:

        i. prior to re-negotiation or extension of a contract

        ii. following a security incident at the provider's or subcontractor's premises?

    d. Have the ongoing clearance maintenance requirements been managed for a provider's staff holding security clearances?

    e. Where the contracted provider processes or stores entity information (and requires access to that information), have the provider's information security procedures been tested and monitored through regular site visits and audits? (ie use of third-party audits, including certifications)[2]

    f. Has the contracted provider monitored the security of information in systems that store, process or communicate entity information through, for example:

        i. conducting vulnerability assessments

        ii. maintaining change and release management processes

        iii. testing their business continuity plan

        iv. identifying, reporting and containing any cyber security incidents that could affect entity information?[3]

    g. To reduce information being lost, destroyed, damaged, compromised or misused, has the contracted provider maintained authorisations for access to information only when the following conditions are met:

        i. the person has the required level of security clearance

        ii. there is a genuine need-to-know the information

        iii. access will comply with legislative and policy requirements

        iv. there is no conflict of interest regarding the information

        v. the person has completed a declaration of secrecy?

22. For guidance on access to information, see the PSPF policy: Access to information.

[2] For information on certification, see www.asd.gov.au/infosec/irap.htm

[3] For information on ICT system security, see the Information Security Manual

C.3.2 Security incidents

23. A security incident may have wide-ranging and critical consequences for the entity and the Australian Government. Investigation of security incidents (actual or suspected) provides valuable information for future risk reviews and assessments. This helps entities evaluate current security plans and procedures.

24. Oversight of incidents through timely and thorough reporting is important during the life of the contract. This allows entities to adjust security procedures and contract conditions if necessary, to mitigate any security risks exposed by an investigation and to implement any additional safeguards to avoid further security incidents from occurring. For example, in service contracts there may be downtime experienced during a cyber-incident response. This may affect performance measures associated with the contract. To address this, contract terms may be structured to encourage appropriate responses to security incidents.

25. **Requirement 2** mandates that entities include conditions in relevant contracts that require the provider to notify the entity, in a timely manner, of any actual or suspected security incidents. This relates to any security incidents that may affect:

    a. the provider's ability to deliver the goods or services they have been contracted to provide

    b. the ability of the contracted provider's personnel to hold a security clearance

    c. any entity resources that are held by, or are in transit to and from the contracted provider.

26. Entities may require contracted providers to report security issues even when not immediately relevant to the contract. Where an entity suffers an eligible data breach (including where it jointly holds personal information with a third party such as a contracted provider), notification obligations arise under the OAIC Notifiable Data Breaches scheme. A data breach incident may also trigger reporting obligations outside of the Privacy Act.

27. Contract managers may refer to the PSPF policy: Management structures and responsibilities that provides guidance on incident reporting requirements.

C.4 Completion or termination of the contract

28. **Requirement 4** mandates that entities apply appropriate security arrangements at the completion or termination of a contract. This helps to safeguard government resources and limit the potential of sensitive or classified information being compromised.

29. The Attorney-General's Department recommends that, at the completion or termination of a contract, entities:

    a. recover records (both electronic and hard copy) and assets under the control of the provider (or require the contracted provider to maintain protective security measures if for legal reasons the provider cannot return records or assets at the end of the contract)

    b. require the provider to delete all entity information from the provider's ICT systems (additionally, for information classified at PROTECTED or above, the Information Security Manual details controls for sanitising ICT systems)[4]

    c. complete obligations under the PSPF policy: Separating personnel as a sponsoring entity, for example:

        i. for personnel with security clearances, inform the authorised security vetting agency of the separation of contracted provider's personnel[5]

        ii. obtain formal acknowledgement from contracted providers and their personnel of their continuing obligations to maintain confidentiality.

[4] For OFFICIAL or OFFICIAL: Sensitive information stored on cloud-based services, a similarly stringent approach to sanitisation may be warranted. For example, in a multi-national cloud-based company there may not be a practical way to erase physical media. In such cases a suitable solution may be stronger encryption of hosted content.

[5] This will cease the entities' sponsorship of security clearances for the contracted provider's personnel. Where entities advise the vetting agency that a contractor no longer requires a security clearance, the vetting agency will inform other known entities using the contractor. This gives interested parties the opportunity to assume sponsorship, including the responsibilities for clearance maintenance of the contractor.

30. For information regarding setting contract end dates and termination options, refer to the Department of Finance Commonwealth Procurement Rules.

D. Find out more

31. Other legislation, policies or contacts include:

    a. Department of Finance Commonwealth Procurement Rules

    b. Commonwealth contracting suite

    c. Foreign Investment Review Board information

    d. OAIC Notifiable Data Breaches scheme

    e. ASIO Business and Government Liaison Unit

    f. *Crimes Act 1914*.

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

Annex A. Developing contract clauses on security matters

Personnel security

1. It is recommended that the same personnel security measures are applied to contracted provider personnel as an entity would with its directly employed staff.

Annex A Table 1 Examples of personnel security contract terms and conditions

Context	Security matters to consider when developing contracts
The PSPF policy: **Eligibility and suitability of personnel** identifies requirements for employment screening and, for those accessing security classified Australian Government resources, vetting.	Personnel security matters to consider when developing contracts may relate to: a. contractor personnel who do not require security clearances – in some cases an entity may consider a signed Non-Disclosure Agreement is warranted to support access to official information.[6] b. a requirement for the contracted providers to seek written consent from the entity, for their personnel who may access the entity's resources and share entity information c. any standards of behaviour which it also expects employees to observe relating to code of conduct and the application of protective security measures d. confidentiality and for non-disclosure of official information (including security classified information) to a third party e. the requirement for contracted provider's personnel to protect the entity's information and assets. As contracted providers' personnel may work concurrently for a number of entities, it can be challenging to identify the relevant entity to sponsor the contractor personnel's security clearances for access to security classified material. In such cases, sponsorship is provided by the entity that: a. first engaged the contractor where a security clearance is required b. requires the highest level of security clearance or c. is the lead entity for a contract, where a single contract covers a number of entities, ie as the result of a panel arrangement.
The PSPF policy: **Ongoing assessment of personnel** identifies requirements to manage ongoing suitability, including sharing relevant information of security concern (where appropriate).	Personnel security matters to consider when developing contracts may relate to: a. provisions requiring the contracted provider to prevent all access to security classified material by personnel whose security clearances are revoked, lapsed or who no longer require access b. a requirement for the contracted provider to report to the entity when any of the provider's personnel have had any incidental or accidental contact with security classified material. For further information see the PSPF policy: Access to information c. arrangements for dealing with any reportable changes in circumstances and the reporting and investigation of security incidents or breaches. For example if a contractor's personnel: i. is employed on other concurrent contracts with other entities or governments ii. has been expelled from an accrediting body iii. has been arrested or is undergoing disciplinary proceedings iv. has been dismissed, has resigned or is on long-term leave d. ongoing security awareness training that includes the contracting company's responsibility that require personnel to: i. protect the entity's assets and information ii. report changes in personal circumstances iii. report suspicious, ongoing, unusual or persistent contact.

[6] Signing a non-disclosure agreement is not suitable in certain circumstances, for example, when sharing information with foreign nationals, or when Australia is not the originator. See PSPF policy: Security governance for international sharing for further information.

Context	Security matters to consider when developing contracts
The PSPF policy: Separating personnel details effective separation measures to ensure departing personnel fulfil their obligations to maintain confidentiality and protect Australian Government resources. See also the Department of Finance publication Confidentiality throughout the procurement cycle.	Personnel security matters to consider when developing contracts may relate to: a. provisions for revoking physical and ICT access upon a contracted provider's personnel's exit from the company b. an obligation on the contracted provider to advise the entity when the provider's personnel (or subcontractors) with sponsored clearances have ceased to work on the entity's contract c. requiring the contracted provider to remind personnel who have accessed official or classified information that the confidentiality requirements are ongoing.

Information security

2. It is recommended that contracted goods and service providers be required to protect Australian Government information resources in the same manner as an entity would themselves.

3. When outsourcing, the business goals of the entity may not align with those of the contractor. System design will always need to be an amalgamation of the entity business process and the system technical design that may be developed by the contractor. Selection and implementation of controls will need to draw from both the entity and the provider's perspectives.

Annex A Table 2 Examples of information security contract terms and conditions

Context	Security matters to consider when developing contracts
The Australian Signals Directorate's Information Security Manual (ISM) provides guidance to help entities ensure a contracted provider has systems able to meet designated information security standards for the electronic processing, storage, transmission and disposal of official and security classified information (particularly where this information is held off shore).	Information security matters to consider when developing contracts may relate to: a. specifying that resources provided by the entity, or generated as a result of the contract, belong to the government and are not used for any purpose other than the goods or services covered by the contract b. a direction to disclose any potential conflict of interest that would impact on security in the performance of services on behalf of the Australian Government c. conditions addressing any potential for legal rights which may be held by a third party over the contracted provider, that could allow access to entity information d. a direction that no service that requires access to official information (including security classified information) be subsequently subcontracted to a different agreed provider, without written approval by the contracting entity e. a direction that where the contracted provider knows or suspects that any sensitive or security classified information relating to the contract has been, or is likely to be, transferred overseas without approval in writing, it must promptly provide details to the contracting entity and follow reasonable directions from the entity in relation to the matter.

Physical security

4. Requiring contracted providers to apply protection against national security threats is recommended, as well as addressing all hazards an entity may face in the protection of its people, information and assets.

Annex A Table 3 Examples of physical security terms and conditions

Context	Security matters to consider when developing contracts
Inspection of any premises used to store Australian Government information or assets (prior to the start of, and during the life of) a relevant contract can help verify that the contracted provider's physical security measures meet relevant minimum PSPF protections.	Physical security matters to consider when developing contracts may relate to: a. ensuring the contracted provider's premises and facilities used to handle or store security classified information meet the PSPF's physical security standards to protect information and assets up to, and including, the nominated security classification level b. allowing entity representatives to access the contracted provider's premises, records and equipment to monitor the contracted provider's compliance with protective security conditions.

Security governance

5. This policy recommends that entities establish robust governance and assurance processes to ensure contracted providers comply with protective security requirements.

Annex A Table 4 Examples of security governance terms and conditions

Context	Security matters to consider when developing contracts
The PSPF policy: Management structures and responsibilities details incident reporting requirements. Incidents provide valuable information for future risk reviews and assessments, and help entities to evaluate current security plans and procedures. The entity may have to adjust security provisions within the contract to address any security risk disclosed by the investigation.	Security governance matters to consider when developing contracts clauses may relate to: a. providing for periodic updating of security requirements to accommodate changes in the: i. risks to the entity or contracted provider ii. National Terrorism Threat Level iii. Australian Government's protective security policies b. taking into account national security provisions (for example, removing information from a data centre if ownership is transferred to a foreign owner) c. conditions that the contracted provider immediately notify the contracting entity where they become aware of i. a proposal to acquire ii. an actual change in the provider's ownership iii. where a substantial overseas investor (including foreign government investors) acquires a substantial interest (eg equal to or greater than 20 per cent) of the contracted provider. d. require the contracted provider to notify the entity of any actual or suspected security incidents that may impact on the entity's information which is held by or in transit to/from the provider, or their ability to deliver the goods or services they have been contracted to provide. Also require the contracted provider to: i. report any breaches of ICT security to the Australian Cyber Security Centre[7] ii. report ICT security issues to the contracting entity even when not immediately relevant to the contract. e. permitting the entity to terminate the contract if the contracted provider fails to comply with the protective security provisions in the contract, including unwillingness or inability to remedy any security breaches f. including strategies for transition security arrangements at the completion or termination of the contract: i. requiring that information (both electronic and hard copy) and assets be returned, and deletion of all entity's information from the contracted provider's ICT systems (for information classified at PROTECTED or above, sanitising their ICT system in accordance with the ISM). See the PSPF policy: Sensitive and classified information for guidance on destruction of information ii. requiring the contracted provider to maintain protective security measures if for legal reasons they cannot return records or assets at the end of a contract.

[7] To report an ICT security incident, the Australian Cyber Security Centre can be contacted on:
a. for critical infrastructure and big business: 1300 172 499, or
b. for individuals and SMEs: 02 6141 6666