Protective security governance guidelines
Security of outsourced services and functions

Approved
13 September 2011

Version 1.0
© Commonwealth of Australia 2011

All material presented in this publication is provided under a Creative Commons Attribution 3.0 Australia (http://creativecommons.org/licenses/by/3.0/au/deed.en ) licence.

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the CC BY 3.0 AU licence (http://creativecommons.org/licenses/by/3.0/legalcode).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour (http://www.itsanhonour.gov.au/coat-arms/index.cfm) website.

Contact us

Inquiries regarding the licence and any use of this document are welcome at:

Business Law Branch
Attorney-General’s Department
3-5 National Cct
BARTON ACT 2600
Telephone: (02) 6141 6666
copyright@ag.gov.au

<table>
<thead>
<tr>
<th>Document details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security classification</td>
<td>Unclassified</td>
</tr>
<tr>
<td>Dissemination limiting marking</td>
<td>Publicly available</td>
</tr>
<tr>
<td>Date of security classification review</td>
<td>July 2013</td>
</tr>
<tr>
<td>Authority</td>
<td>Protective Security Policy Committee</td>
</tr>
</tbody>
</table>
| Author                                     | Protective Security Policy Section
                                           | Attorney-General’s Department |
| Document status                            | Approved by PSPC 13 September 2011 |
Table of Contents

1. Introduction .................................................................................................................. 1
   1.1. Purpose .................................................................................................................... 1
   1.2. Audience ................................................................................................................ 1
   1.3. Scope ..................................................................................................................... 1
       1.3.1. Use of specific terms in these guidelines .................................................... 1

2. Background .................................................................................................................. 2
   2.1. Why were these Guidelines developed? ............................................................... 2
   2.2. Relationship to other documents ........................................................................ 2
   2.3. How are these guidelines structured? ................................................................. 2

3. Including protective security terms and conditions in contracts ............................ 3
   3.1. Evaluating tender responses ................................................................................ 4

4. Security clearances for service providers’ staff ....................................................... 5
   4.1. Incidental or accidental contact with security classified material .................... 5
   4.2. Agency specific character checks ...................................................................... 6

5. Information security ................................................................................................... 7
   5.1. Offshore holdings ............................................................................................... 7

6. Physical security ......................................................................................................... 8

7. Contract management ................................................................................................. 9
   7.1. Reporting security breaches and incidents ......................................................... 9
   7.2. Periodic assessments of service providers’ premises ....................................... 9
   7.3. Completion of the contract ................................................................................. 10

Annex A—Example Non-disclosure Agreement ............................................................. 11
## Amendments

<table>
<thead>
<tr>
<th>No.</th>
<th>Location</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. Introduction

1.1. Purpose

The PSPF Protective security governance guidelines—Security of outsourced services and functions identify better practice and provide advice to agencies to assist them in developing security requirements in an agency’s outsourcing policies and contracts. When an agency adopts an outsourcing approach to service provision, accountability for the performance of the service or function and responsibility for outcomes remains with the agency. This agency responsibility includes the management of security risks where external service providers are being used.

1.2. Audience

These guidelines apply to:

- agency security, contract and procurement management personnel
- contracted service providers, and
- agency contract managers.

1.3. Scope

These guidelines amplify the Protective Security Policy Framework (PSPF) Governance – 4.12 Contracting relating to contracting agency functions and better practice that agencies should apply to meet the requirements of GOV 12.

1.3.1. Use of specific terms in these guidelines

In these guidelines the use of the terms:

- ‘need to’ refers to a legislative requirement that agencies must meet
- ‘are required to’ or ‘is required to’ refers to a control:
  - to which agencies cannot give a policy exception, or
  - used in other protective security documents that set controls.
- ‘are to’ or ‘is to’ are directions required to support compliance with the mandatory requirements of the physical security core policy, and
- ‘should’ refers to better practice; agencies are expected to apply better practice unless there is a reason based on their risk assessment to apply alternative controls.

For details on policy exceptions see the PSPF Australian Government Physical security management protocol.

The following terms are also used in these guidelines:

- **Service provider**—a contractor to a government agency and/or sub-contractors to the agency’s contractor.
- **Request Documents**—documents provided to a potential service provider when requesting pricing on services or functions, or used in a procurement process.
2. Background

2.1. Why were these Guidelines developed?

The PSPF Protective security governance guidelines—Security of outsourced services and functions were developed to provide a consistent and structured approach to determining:

- the protective security required at service provider’s premises
- personnel security clearance requirements of service provider’s staff, and
- protective security management arrangements within contracts.

These guidelines provide agencies with a framework for incorporating protective security requirements into contracts when outsourcing agency functions.

2.2. Relationship to other documents

These guidelines explain mandatory requirement GOV 12 which requires agencies to ensure any service provider complies with Australian Government protective security policies and procedures where there is access to, or control over, Australian Government personnel, information, or assets.

In addition to GOV 12, these guidelines complement the Australian Government Personnel Security, Information Security, and Physical Security Core Policies. Some or possibly all of the PSPF Governance arrangements are also likely to apply to government services or functions outsourced to a service provider.

These guidelines should assist agencies in developing agency policies and procedures for managing protective security in outsourced services or functions.

2.3. How are these guidelines structured?

These guidelines are broadly divided into three parts:

- including protective security in contracts
- identifying specific requirements, and
- ongoing management of protective security in contracts.
3. Including protective security terms and conditions in contracts

The contract manager within the agency is responsible for ensuring the service provider complies with any protective security terms and conditions in the contract. Contract managers should consult with the Agency Security Adviser (ASA) and IT Security Advisers (ITSA) to identify essential security requirements when developing tender documents and throughout the life of the contract.

To meet their obligation to protect personnel, official information or agency assets from unacceptable risk when outsourcing services or functions, agencies are to:

- assess security issues associated with outsourcing or procurement during the planning phase of the procurement
- determine and publish in relevant Request Documents mandatory and desirable security requirements, including any specific provisions relating to sub-contracting, and
- use risk management as the basis of protective security terms and conditions in the contract, and ongoing contract management of the service provider and its employees.

Agencies should, where possible, explicitly refer to the highest level of security classified information the service provider will access in Request Documents and the final contract. If the level of access required changes, this is to be advised to the contractor as soon as possible through contract variation procedures.

SAI Global - ISO 31000: Risk Management—Principles and Guidelines provides guidance on identifying, assessing and treating risks that will assist agencies to develop strategies for managing security risks in procurement.

All relevant contracts are to include details of essential protective security requirements.

As agencies are required to develop their own protective security policies and procedures from the PSPF, a general condition that the service provider must comply with the PSPF is not likely to be appropriate or enforceable. Therefore the agency should identify the elements of their protective security policies and procedures that apply, and specifically include these obligations as terms and conditions in the contract.

The contract should provide for periodic updating of security requirements by the contracting agency to accommodate changes in the:

- risks to the agency or service provider
- National Alert Level, or
- protective security policies and protocols.

Agencies should consider using a separate schedule of security requirements to clearly identify the protective security conditions in the contract. This would simplify amendments to the protective security terms and conditions if needed.

In addition to any other statutory requirements, or specific security requirements, agencies need to ensure that contracts require service providers to comply with the Information Privacy Principles of the Privacy Act 1988 when entering into a contract on behalf of the Australian Government.
Agencies are to include a condition in contracts which allows agency representatives to access the service provider’s premises, records and equipment to monitor the service provider’s compliance with the protective security conditions in the contract.

Generally, contracts should specify that information provided by the agency or generated as a result of the contract belongs to the Government and should never be used for any purpose other than the service or function covered by the contract. By clearly identifying agency information the agency can impose protective security requirements on its information.

Some information generated as a result of the contract may be subject to Intellectual Property (IP) claims by the service provider. Where possible IP issues should be determined prior to entering into a contract.

Agencies should ensure any relevant contract with a service provider includes terms and conditions that permit the agency to terminate the contract if the service provider fails to comply with the protective security provisions in the contract, including the unwillingness, or inability of a service provider to remedy any security breaches.

### 3.1. Evaluating tender responses

Where Request Documents specify essential protective security requirements are part of an outsourced service or function, an agency is to ensure that tender responses adequately address the contract’s essential security requirements. If a proposed contract response does not address the essential security requirements the agency tender evaluation team should exclude the contract response from consideration.

If a contract is awarded subject to a service provider meeting security provisions, the contract is not to start before the agency verifies the compliance.

For further information on tender evaluations see the *Commonwealth Procurement Guidelines*. 
4. Security clearances for service providers’ staff

All service providers’ staff who will access security classified material to perform the contract are to be security cleared to the appropriate level before accessing any security classified material. See PSPF Australian Government personnel security core policy – PERSEC 1.

Not all services or functions outsourced to a service provider will require access to security classified material. Even though a service provider’s staff will not require security clearances to perform the services, agencies should assess if the access to official information justifies requiring the service provider’s staff signing a Non-Disclosure Agreement. Agencies should seek legal advice when developing their own agreements, see Annex A—Example Non-disclosure Agreement.

Agencies are responsible for arranging the security clearance for any of the service providers’ employees or sub-contractors who require a security clearance. Agencies should check with the Australian Government Security Vetting Agency (AGSVA) to determine if a service provider’s employee currently holds a valid security clearance. If the person holds a clearance at the appropriate level, the contracting agency does not have to take further action until revalidation is required. AGSVA should initiate the revalidation prior to the clearance expiry. However, if the clearance was initially sponsored by another agency AGSVA may not have the correct agency contact details.

PSPF Australian Government personnel security core policy – PERSEC 4 requires agencies to sponsor any service providers’ staff who need a security clearance. AGSVA will only invoice the sponsoring agency for the costs of security clearances for service providers’ staff processed by AGSVA.

Agencies should consider the costs of providing security clearances for service providers’ staff for the life of the contract, and any cost-shifting arrangements when negotiating the contract.

The contracting agency is responsible for managing personnel security aftercare of service providers’ security clearances throughout the life of the contract.

Agencies are to include conditions in the relevant contracts that require the service provider to prevent all access to security classified material by personnel whose security clearances are revoked, lapse, or who no longer require access.

4.1. Incidental or accidental contact with security classified material

Agencies should include conditions in the relevant contracts that require the service provider to report to the agency when any of the service providers’ employees have any incidental or accidental contact with security classified material. This condition is particularly important in security guarding and cleaning contracts.

Agencies may share limited amounts of PROTECTED level information with non-government agencies that screen employees to the level of Australian Standard AS: 4811-2006: Employment screening. An agency may decide to accept the risk of irregular incidental or accidental contact with PROTECTED level material by service providers’ staff who are screened to AS: 4811-2006: Employment screening.

Service providers’ staff who may reasonably be expected to have incidental or accidental contact with security material classified above PROTECTED are to be cleared to Negative Vetting Level 1.

Service providers’ staff who may reasonably be expected to have incidental or accidental contact with TOP SECRET material are to be cleared to Negative Vetting Level 2.
Service providers’ staff who do not hold a security clearance at the appropriate level are not permitted unescorted access to any areas where classified information is handled.

4.2. Agency specific character checks

Agencies that conduct agency specific character checks for their own staff should determine whether or not they require the same agency specific character checks to be conducted for the service providers’ staff. See the PSPF Australian Government personnel security protocol.
5. **Information security**

Agencies are to ensure that the requirements of the PSPF *Australian Government information security core policy* for the protection of agency information are addressed when deciding to outsource a service or function.

Agencies should ensure relevant information security requirements to meet their information security policies and procedures are included as protective security terms and conditions in a contract. In addition agencies are to ensure all contracts requiring a service provider to access and handle official information contain terms and conditions that satisfy the following requirements:

- a direction that no service or function that may require access to official information can be subsequently sub-contracted, or sub-contracted to a different agreed provider, without written approval by the contracting agency
- a direction to disclose any potential conflicts of interest that would impact on security in the performance of functions or services on behalf of the Australian Government
- that service provider employees requiring access to security classified information are cleared to the appropriate level
- that service provider premises and facilities used to handle or store security classified information meet the minimum standards for the storage and handling of official information up to and including the nominated security classification level
- the service providers are to have systems able to meet designated information security standards for the electronic processing, storage, transmission and disposal of official information, see the *Australian Government Information Security Manual* (ISM), and
- a direction on any ongoing confidentiality requirements relating to official information provided as part of the contract.

Agencies should consider the potential for legal rights that may be held by a third party over the service provider that could allow access to agency information. Where agencies consider this is a risk the contract should include terms and conditions, to the extent possible, which protects against third party access.

Agencies should consider the impact on the agency of any loss or compromise of official information held by a service provider, especially aggregated information, and include conditions in the contract to mitigate any assessed risks.

Agencies remain responsible for the management of their official records under the *Archives Act 1983* whether held by the agency or by a service provider at an offsite facility.

5.1. **Offshore holdings**

Any official information held offshore is to meet the requirements of the Protective Security Policy Framework, in particular the Australian Government Information Security Protocol. The ISM also prescribes limits on holding electronic security classified information offshore.
6. Physical security

Agencies are to ensure that the requirements of the PSPF *Australian Government physical security core policy* for the protection of agency personnel, information and assets are addressed when deciding to outsource a service or function.

Agencies should ensure relevant physical security requirements to meet their physical security policies and procedures are included as protective security terms and conditions in a service contract.
7. **Contract management**

Contract management involves monitoring both the performance of contracted functions or services, and adherence to the essential security requirements of the contract. Agencies should:

- seek to develop a positive working relationship with their service providers to promote open communication, and add value to the security environment through the prompt identification and resolution of issues, and
- monitor the service provider’s security procedures by undertaking regular site visits and audits.

Agencies should ensure that the service providers advise relevant employees and any sub-contracted service providers of the protective security terms and conditions that apply under the contract.

Agencies should include conditions in the relevant contracts that require the service provider to remind any separating personnel who have accessed official or classified information that their responsibility to maintain confidentiality is ongoing.

For further guidance see the Department of Finance and Deregulation publication *Confidentiality throughout the Procurement Cycle*.

7.1. **Reporting security breaches and incidents**

A security incident might have wide-ranging and critical consequences for the agency and for the Australian Government.

Agencies should include conditions in the relevant contracts that require the service provider to notify the agency of any actual or suspected security incidents or breaches that may impact on:

- their ability to deliver the services they have been contracted to provide, or
- the agency’s information which is held by, or in transit to/from the service provider.

Agencies should investigate any actual or suspected security breaches reported by a service provider, as well as any other breaches that may involve a service provider of which the agency is aware. Incidents provide valuable information for future risk reviews and assessments, and will help agencies to evaluate current security plans and procedures. The agency may have to adjust security procedures to deal with any security risk disclosed by the investigation.

Agencies are advised to include conditions in the relevant contracts that require the service provider to report any breaches of ICT security, not involving agency information, to CERT Australia. CERT Australia can help mitigate ICT threats. Agencies may also consider requiring service providers to report ICT security issues to the contracting agency even when not immediately relevant to the contract.

7.2. **Periodic assessments of service providers’ premises**

Agencies should inspect any premises used to store Australian Government information or assets prior to the start of a relevant contract to verify that the protective security measures and procedures specified by the contract comply with the PSPF.
Agencies should periodically re-inspect contractors’ and sub-contractors’ premises during the life of the contract to ensure continued compliance with the PSPF. These inspections should be undertaken, but not limited to the following occasions:

- prior to any re-negotiation or extension of a contract, where the contract term exceeds two years
- following a security incident at the service provider’s (or sub-contractor’s) premises and/or
- as part of the agency’s security risk review.

Agencies can reassure concerned service providers that the purpose of the access is to monitor the contract, and not to discover information or details unconnected with the contract.

7.3. Completion of the contract

Agencies should apply appropriate strategies for transition security arrangements at the completion or termination of the contract. Agencies are to ensure that they recover records (both electronic and hard copy) and assets under the control of the service provider. However, a legal requirement may arise that causes the service provider to temporarily retain certain records.

Agencies should include conditions in the relevant contracts that require the service provider to maintain protective security measures if for legal reasons the service provider cannot return records or assets at the end of a contract.

Agencies should include conditions in the relevant contracts that require the service provider to delete all of the agency’s information from the service provider’s ICT systems. For information classified at PROTECTED or above, the service provider is to sanitise their ICT system in accordance with the provisions of the *Australian Government Information Security Manual*.

Agencies should include conditions in the relevant contracts that require the service provider to remind any personnel who have accessed official or classified information that the confidentiality requirements are ongoing.
Annex A—Example Non-disclosure Agreement

<table>
<thead>
<tr>
<th>Full Name in Block Letters</th>
</tr>
</thead>
<tbody>
<tr>
<td>I,</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date of Birth</th>
<th>Place of Birth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Born on:</td>
<td>At:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Full Residential Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Of:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of organisation/company/agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employed by:</td>
</tr>
</tbody>
</table>

Being a person who has agreed to receive official or security classified information from:

<table>
<thead>
<tr>
<th>Name of agency providing security classified information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

1. undertake to:
   (a) preserve the confidentiality/ secrecy of the information entrusted to me;
   (b) not disclose, publish or communicate such information to any person, inside or outside my organisation/ company/agency, except to senior managers who have a need to know such information and, for security classified information, have the appropriate security clearance;
   (c) ensure that anybody to whom I provide the information is made aware of the conditions under which this information is communicated, and of the fact that the confidentiality/ secrecy of the information must be maintained; and
   (d) undergo the security clearance vetting process where I have, or will be given access to security classified information for more than three months.

2. Further, I acknowledge that I have received a security briefing on my responsibility to protect the information, including the correct methods for storage, handling and dissemination.

<table>
<thead>
<tr>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Witness Signature</th>
<th>Witness Name and Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>