



**Australian Government**

---

**Department of Defence**

Intelligence, Security and International Policy

# **INVITATION TO REGISTER INTEREST**

in

## **Multi Use List**

for

Various Security Compliance and Performance Review Services

# INVITATION TO REGISTER INTEREST (ITR)

## TABLE OF CONTENTS

<b>1.</b>	<b>SUMMARY OF REQUIREMENT AND ITR OBJECTIVES .....</b>	<b>1</b>
1.1	Background and Scope.....	1
1.2	ITR Objectives .....	1
1.3	Commonwealth Disclaimer .....	2
1.4	Multi Use List .....	2
<b>2.</b>	<b>GENERAL INFORMATION AND RESPONSE LODGEMENT.....</b>	<b>2</b>
2.1	Interpretation of Terms.....	2
2.2	Definitions .....	3
2.3	Variation of ITR.....	4
2.4	AusTender, the Australian Government Tender System.....	4
2.5	Registered Respondents and Notices.....	5
2.6	Contact Officer for ITR Enquiries.....	5
2.7	AusTender Help Desk.....	5
2.8	RESERVED.....	6
2.9	Part and Joint Responses.....	6
2.10	Response Guidance .....	6
2.11	Lodgement of Responses.....	6
2.12	Commonwealth Procurement Policy Requirements .....	7
<b>3.</b>	<b>MATTERS CONCERNING RESPONSE.....</b>	<b>8</b>
3.1	Language of Responses .....	8
3.2	Response Preparation and Format .....	8
3.3	Respondents to Inform Themselves.....	8
3.4	Use of Response Documents.....	9
3.5	RESERVED.....	9
<b>4.</b>	<b>EVALUATION OF RESPONSE.....</b>	<b>9</b>
4.1	Response Evaluation .....	9

4.2	Conditions of Participation .....	10
4.3	RESERVED.....	10
4.4	RESERVED.....	10
4.5	Debriefing of Respondents .....	10
	Introduction.....	4
	<b>ACCEPTANCE OF SERVICES.....</b>	<b>4</b>
	<b>REQUIREMENT A .....</b>	<b>5</b>
	Background to Requirement A .....	5
	Two Categories of Reviews.....	5
	<b>REQUIREMENT A – SCOPE OF SERVICES .....</b>	<b>6</b>
	<b>CONTRACTOR REQUIREMENTS.....</b>	<b>7</b>
	Clearance Level .....	7
	Travel	
	Information and Communication Technology (ICT).....	7
	<b>REQUIREMENT B .....</b>	<b>9</b>
	Background to Requirement B .....	9
	Protective Security Compliance.....	9
	<b>REQUIREMENT B – SCOPE OF SERVICES .....</b>	<b>9</b>
	Security Compliance Activities .....	9
	Security Compliance Activities Methodologies .....	10
	Compliance Reports .....	13
	Review, Approval or Non-Approval, and Acceptance of Reports .....	14
	<b>DOCUMENTATION .....</b>	<b>14</b>
	GOVERNMENT FURNISHED MATERIAL (GFM).....	15
	Provision and Management of GFM .....	15
	Care of GFM .....	15
	Shared GFM.....	16
	Provision and Management of Government Furnished Facilities .....	16

<b>TRAINING IN DEFENCE INFORMATION SYSTEMS .....</b>	<b>16</b>
Training Cost .....	16
Training Reporting .....	17
<b>CONTRACTOR REQUIREMENTS .....</b>	<b>17</b>
Security Clearance Levels .....	17
DISP Entry Requirements.....	17
State Licences.....	17
Travel Requirements.....	18
Contractor Training Competency Levels.....	18
Ad Hoc Meetings.....	18
Contractor Operating Performance Reviews .....	19
<b>CONTRACTOR QUALITY RESPONSIBILITIES .....</b>	<b>19</b>
Quality Management System .....	19
Audit and Surveillance activities .....	19
Subcontractors .....	19
<b>ANNEXES TO THE ITR</b>	
A.	Declaration by Respondents
B.	Information to be Supplied by Respondents
C.	Example Description of Requirement

## 1. SUMMARY OF REQUIREMENT AND ITR OBJECTIVES

### 1.1 Background and Scope

---

1.1.1 This ITR invites responses for a requirement to register for a Multi Use List to provide the following security compliance and performance review services for one, a combination or all of the following categories at Annex B:

- (a) **Security reviews** will primarily fall into four security categories:
- (i) information, and communications technology security (ICT);
  - (ii) physical, personnel and information security,
  - (iii) handling and management of weapons, munitions and explosives (WME) throughout their lifecycle; and
  - (iv) Other tasks that may be required include the development of:
    - review methodology;
    - performance review methodology;
    - templates;
    - review tracking;
    - reporting mechanisms; and
    - research of best practice security review.
- (b) **Security performance and Compliance** will primarily fall into three security categories:
- (i) Physical security;
  - (ii) Information, communications and technology (ICT) security; and
  - (iii) Personnel and information security

### 1.2 ITR Objectives

---

1.2.1 The purpose of this ITR is to allow the Commonwealth to:

- (a) develop a Multi Use List of prequalified suppliers who have satisfied the conditions for participation for inclusion on the Multi Use List for one, a combination or all categories;
- (b) develop a list of prequalified suppliers to be listed on the Multi Use List to receive any subsequent Request for Tender (RFT);
- (c) develop a shortlist of respondents from the Multi Use List who will receive any subsequent RFT.

## ISIP ITR No: 2009/04

- (d) at the sole discretion of the Commonwealth, issue an RFT to members of the Multi Use List to establish a standing offer.

### 1.3 Commonwealth Disclaimer

---

- 1.3.1 The terms of this ITR are expressly not a contract between the Commonwealth and any respondent. Nothing in this ITR, or in any response, is to be construed, interpreted or relied upon as to give rise to common law or equitable rights or obligations, either express or implied. Respondents acknowledge that the issue of this ITR does not oblige the Commonwealth to proceed with:
- (a) the ITR process or any resultant Multi Use List or any resultant Request For Tender (RFT) process or any resultant Contract or any resultant Standing Offer;
  - (b) the requirement the subject of this ITR nor any part of the requirement; or
  - (c) any particular purchasing methodology in relation to the requirement.
- 1.3.2 No contract is entered into by the Commonwealth until a formal written Contract is executed on behalf of the Commonwealth.
- 1.3.3 Participation in any stage of this ITR process, or in relation to any matter concerning this ITR process, shall be at the respondent's sole risk, cost and expense. Without limitation, the Commonwealth shall not have any liability to pay compensation to respondents for any reason including for termination, variation or suspension of this ITR. Planning dates advised in this ITR are indicative only and the Commonwealth is under no obligation to hold to these dates.
- 1.3.4 In the event that the Commonwealth proceeds with the procurement process, the Commonwealth reserves the right to amend its requirement.

### 1.4 Multi Use List

---

- 1.4.1 The Multi Use List will be open to new applicants annually.
- 1.4.2 Inclusion on the Multi Use List will not constitute a guarantee of work, nor can membership of the list be used to imply that a business is a supplier to the Commonwealth or has any preferred position.
- 1.4.3 Successful applicants will be progressively published as participants on the Multi Use List from March 2009.

## 2. GENERAL INFORMATION AND RESPONSE LODGEMENT

### 2.1 Interpretation of Terms

---

- 2.1.1 In this ITR, unless the contrary intention appears:
- (a) Headings are for the purpose of convenient reference only and do not form part of the ITR.
  - (b) The singular includes the plural and vice versa.

## ISIP ITR No: 2009/04

- (c) A reference to an Act is a reference to an Act of the Commonwealth, State or Territory of Australia, as amended from time to time, and includes a reference to any subordinate legislation made under the Act.
  - (i) A reference to a clause includes a reference to a sub-clause of that clause.
- (d) A reference to a specification, publication or other document is a reference to that specification, publication or document, in effect on the date of release of this ITR or alternatively, a reference to a revised version of the document if agreed in writing between the parties.
- (e) The word “includes” in any form is not a word of limitation.

### 2.2 Definitions

---

2.2.1 In this ITR, unless the contrary intention appears, the term:

- (a) “Annex” means an Annex to this ITR.
- (b) "Commonwealth" means the Commonwealth of Australia.
- (c) “Commercial-in-Confidence Information” means information that:
  - (i) is by its nature confidential; or
  - (ii) the receiving party knows or ought to know is confidential;but does not include information which:
  - (iii) is in the possession of a party without restriction in relation to disclosure before the date of receipt; or
  - (iv) has been independently developed or acquired by the receiving party.
- (d) "Contract" means a contract which may be entered into between the Commonwealth and a person for the provision of the requirement of a type envisaged by this ITR.
- (e) “Contractor” means a person who enters into a Contract with the Commonwealth for the provision of the requirement of a type envisaged by this ITR.
- (f) “day” means a calendar day.
- (g) “document” includes:
  - (i) any paper or other materials on which there are writing, marks, figures, symbols or perforations having meaning for persons qualified to interpret them; and
  - (ii) any article or material from which sounds, images, or writings are capable of being reproduced with or without the aid of any other article or device.
- (h) “Intellectual Property” or "IP" means all copyright (including moral rights) and all rights in relation to inventions (including patent rights), registered and unregistered trade marks (including service marks), registered and unregistered designs, confidential

## ISIP ITR No: 2009/04

information (including trade secrets and know how), and circuit layouts, and any other rights resulting from intellectual activity in the industrial, scientific, literary and artistic fields recognised in domestic law anywhere in the world.

- (i) "month" means a calendar month.
- (j) "Multi Use List" means a list, intended for use in more than one procurement process. This list consists of pre-qualified suppliers who have satisfied the conditions for participation for inclusion on the list through an open tender process, intended for use in more than one procurement process.
- (k) "Organisational Suitability Assessment" or "OSA" means the assessment administered by a qualified practitioner, to determine whether or not a nominated person is suitable to work in a high security environment.
- (l) "Request for Tender" or "RFT" means a request issued by the Commonwealth to persons to submit an offer to provide the Supplies.
- (m) "Response Closing Time" is the time specified in clause 2.9 by which responses to this ITR must be lodged.
- (n) "Working Day" in relation to the doing of an action in a place means any day other than a Saturday, Sunday or public holiday in that place.

### 2.3 Variation of ITR

---

- 2.3.1 The Commonwealth may amend this ITR upon giving respondents timely written notice of an amendment.
- 2.3.2 If the Commonwealth amends this ITR under clause 2.4. after responses have been submitted it may seek amended responses.
- 2.3.3 The Commonwealth may, in its absolute discretion, terminate the process at any time.

### 2.4 AusTender, the Australian Government Tender System

---

- 2.4.1 AusTender is the online tendering system for Australian Government Agencies. AusTender allows tenderers to download tender documentation. Respondents must first register with AusTender at <https://www.tenders.gov.au>.
- 2.4.2 Access to and use of AusTender is subject to terms and conditions. Respondents must agree to comply with those terms and conditions and any applicable instructions, processes, procedures and recommendations as advised on AusTender.
- 2.4.3 It is the responsibility of respondents to ensure their infrastructure including operating system and browser revision levels meet the minimum standards as defined on AusTender. The Commonwealth does not take any responsibility for any problems arising from respondents' infrastructure and/or Internet connectivity.
- 2.4.4 Respondents acknowledge that although the Commonwealth has implemented the security measures described on AusTender, the Commonwealth does not warrant that unauthorised access to information and data transmitted via the Internet will not occur.
- 2.4.5 Respondents must inform themselves concerning all security measures and other aspects of

## ISIP ITR No: 2009/04

the AusTender technical environment. Respondents must make their own assessment of the AusTender system prior to using it for any matter relating to this ITR and no responsibility will be accepted by the Commonwealth arising in respect of any use or attempted use by any party of AusTender.

### 2.5 Registered Respondents and Notices

---

- 2.5.1 In the event that the Commonwealth elects to vary or supplement this ITR, it will make reasonable efforts to inform respondents in accordance with this clause 2.6.
- 2.5.2 Respondents may be informed by notices and other information issued as addenda posted on this ITR page on AusTender.
- 2.5.3 Respondents who have registered and downloaded the ITR documentation will be notified by AusTender via email of any addenda issuance. It is in the interest of respondents to ensure they have correctly recorded their contact details prior to downloading ITR documentation. If respondents have not recorded their details correctly, they should amend their details and download the ITR documentation again.
- 2.5.4 Respondents are required to log in to AusTender and collect addenda as notified.
- 2.5.5 The Commonwealth will accept no responsibility if a respondent fails to become aware of any addendum notice which would have been apparent from a visit to the AusTender page for this ITR.
- 2.5.6 If a respondent has obtained ITR documentation other than from AusTender, they must visit AusTender, register as a user and download the documentation for this ITR.

### 2.6 Contact Officer for ITR Enquiries

---

- 2.6.1 The Contact Officers for this ITR are:

**Technical**

Ms Alice Gardiner  
Email: [alice.gardiner1@defence.gov.au](mailto:alice.gardiner1@defence.gov.au)

**Contractual**

Ms Sherrie Choikee  
Email: [sherrie.choikee1@defence.gov.au](mailto:sherrie.choikee1@defence.gov.au)

Respondents should direct any questions regarding this ITR to the relevant Contact Officer in writing.

- 2.6.2 The Commonwealth may circulate respondent's questions and Commonwealth answers to all other respondents without disclosing the source of the questions or revealing Commercial-in-Confidence Information or the substance of a proposed response.

### 2.7 AusTender Help Desk

---

- 2.7.1 All queries and requests for technical or operational support must be directed to:

AusTender Help Desk  
Telephone: 1300 651 698  
Email: [tenders@finance.gov.au](mailto:tenders@finance.gov.au)

The AusTender Help Desk is available between 9:00am and 5:00pm, Monday to Friday (excluding ACT and national public holidays).

2.8 **RESERVED**

---

2.9 **Part and Joint Responses**

---

- 2.9.1 The Commonwealth **SHALL** consider a response for part of the requirement.
- 2.9.2 The Commonwealth **SHALL NOT** consider a joint response for part of the requirement.

2.10 **Response Guidance**

---

- 2.10.1 Respondents should use the information contained in this ITR and all its enclosures as guidance when preparing responses.
- 2.10.2 Respondents should respond to each of the information requests detailed in Annex B, in addition to requests for information located elsewhere in this ITR.
- 2.10.3 The responses to Annex B and the requirements of this ITR are to be provided in the order that the requests appear, and are to include a clear cross-reference to the relevant ITR clause numbers they address.
- 2.10.4 Responses should be concise and in direct correspondence to each request for information.
- 2.10.5 Minimal use of promotional material and referenced documents in addressing requests is encouraged. Where additional information is supplied and referenced, the references should clearly identify the information that directly relates to the request.
- 2.10.6 An original and one copy of the ITR response (including supporting documentation) are to be provided in hard copy. The original is to be marked as the original and the copy marked with the copy number. In the event of any discrepancy between the copy and the original, the original will take precedence.
- 2.10.7 One read-only electronic copy, on either CD-ROM or 3.5-inch floppy disk(s), in Adobe Acrobat PDF or Microsoft Word format is also required. In the event of any discrepancy between the electronic copy and the original hard copy, the original hard copy will take precedence.

2.11 **Lodgement of Responses**

---

- 2.11.1 Responses are to be emailed to Contact Officer (Technical) on or before 12:00pm local time on **Monday 9 March 2009** (“the Response Closing Time”) to the following address:  
  
Ms Alice Gardiner  
**Email:** [alice.gardiner1@defence.gov.au](mailto:alice.gardiner1@defence.gov.au)
- 2.11.2 Responses lodged after the ITR Closing Time may be deemed to be ‘Late Responses’. Late Responses will be opened and registered separately and may be excluded from the evaluation process at the discretion of the Commonwealth.
- 2.11.3 Late Responses shall be admitted to evaluation if there is proof that they were mishandled by the relevant departmental purchasing office or by an official postal or telecommunications service.
- 2.11.4 Following notification that its submission has failed to meet the ITR Closing Time and is deemed to be a ‘Late Response’, the relevant Respondent may be asked to provide explanatory evidence in an appropriate form for consideration by the Commonwealth.

- 2.11.5 The circumstances surrounding the submission and the receipt of the Late Response will form the basis of the judgement on its admission to, or exclusion from the evaluation process. The most important issue from the perspective of probity is whether the late Respondent is likely to have had an opportunity to obtain some unfair advantage from late submission.
- 2.11.6 A number of factors may be taken into account in deciding whether or not to accept Late Responses. The following list provides an indication of some relevant considerations:
- (a) how late the response is, the reasons given for lateness and evidence available;
  - (b) the length of time allowed for the preparation of responses; and
  - (c) evidence of unfair practices.
- 2.11.7 The Commonwealth's decision on whether to admit a Late Response to evaluation shall be final and the Commonwealth is not obliged to give reasons for its decision.

## 2.12 Commonwealth Procurement Policy Requirements

---

- 2.12.1 Tenderers should familiarise themselves with the following Commonwealth policies:
- (a) Contract Gazettal policy as detailed in Section 5, Chapter 5.8 of the *Defence Procurement Policy Manual*, Version 3.0: 2002;
  - (b) Defence Equity and Diversity policy as detailed in the *Defence plain-english guide to Managing and Eliminating Unacceptable Behaviour in the Workplace*, May 2000 and Departmental Personnel Instruction No 1/2001;
  - (c) Equal Opportunity for Women in the Workplace policy as detailed in the *Defence Procurement Policy Manual*;
  - (d) Freedom of Information policy as detailed in Section 5, Chapter 5.7 of the *Defence Procurement Policy Manual*;
  - (e) Hazardous Substances policy as detailed in Annex 3F of the *Defence Procurement Policy Manual*;
  - (f) Maximising Employment Opportunities for Aboriginal and Torres Strait Islanders policy as detailed in Annex 3D of the *Defence Procurement Policy Manual*;
  - (g) Ozone Depleting Substances Policy as detailed in Annex 3G of the *Defence Procurement Policy Manual*; and
  - (h) Getting Smarter about Knowledge Rights – Defence Intellectual Property Policy June 1999.

**Note to respondents: An electronic version of the Defence Procurement Policy Manual can be accessed at the Contracting section of the DMO web site at [www.defence.gov.au/dmo](http://www.defence.gov.au/dmo). An electronic version of the Defence Equity and Diversity policy can be accessed at the Publications section of the DPE web site at [www.defence.gov.au/equity](http://www.defence.gov.au/equity). An electronic version of the Company Scorecard policy can be accessed at the Policy section of the Industry Resources area of the DMO web site at [www.defence.gov.au/dmo](http://www.defence.gov.au/dmo).**

- 2.12.2 Respondents acknowledge that as a Commonwealth agency, the Department of Defence is subject to legislative and administrative accountability and transparency requirements of the Commonwealth, including disclosures to Parliament and its Committees. Any resultant RFT and/or Contract will be subject to these requirements, including that RFT and/or contractual provisions (and related matters) may be disclosed to Parliament and its Committees unless there is a sound basis for their confidentiality.

### **3. MATTERS CONCERNING RESPONSE**

#### **3.1 Language of Responses**

---

- 3.1.1 Responses to this ITR are to be in English, formatted for A4 paper. Measurement is to be expressed in Australian legal units of measurement unless otherwise specified.

#### **3.2 Response Preparation and Format**

---

- 3.2.1 Respondents are to complete and provide the information requested in the Annexes to this ITR.
- 3.2.2 Where clauses in this ITR require information to be provided by the Respondent, this information is to be included in the relevant Annex or incorporated in the relevant section of Annex B.
- 3.2.3 Supporting documentation may be provided to enhance the response. Supporting documentation relevant to a particular volume shall be indicated in that volume.
- 3.2.4 Responses which are incomplete, non-compliant with essential requirements or clearly non-competitive may be excluded from consideration at any time during the evaluation process at the Commonwealth's discretion but the Commonwealth may still consider such bids and seek clarification under clause 4.3.
- 3.2.5 Respondents shall not use the improper assistance of employees, or former employees of the Commonwealth, or information obtained unlawfully or in breach of an obligation of confidentiality to the Commonwealth in compiling their responses. Respondents should note the requirement in Annex A to provide a declaration to this effect. The Commonwealth may not further consider a response which has been compiled using such assistance or information.

#### **3.3 Respondents to Inform Themselves**

---

- 3.3.1 Respondents are considered to have:
- (a) examined this ITR, any documents referenced in the ITR and any other information made available in writing by the Commonwealth to respondents for the purpose of responding to this ITR;
  - (b) examined all further information which is obtainable by the making of reasonable enquires relevant to the risks, contingencies, and other circumstances having an effect on their responses; and
  - (c) satisfied themselves as to the correctness and sufficiency of their response.
- 3.3.2 Responses are made on the basis that respondents acknowledge that:

## ISIP ITR No: 2009/04

- (a) they do not rely on any representation, letter, document or arrangement, whether oral or in writing, or other conduct as adding to or amending these conditions other than amendments in accordance with clause 2.4 of this ITR;
- (b) they do not rely upon any warranty or representation made by or on behalf of the Commonwealth, except such as are expressly provided for in this ITR, but they have relied entirely upon their own enquires and inspection in respect of the subject of their responses;
- (c) the Commonwealth shall not be responsible for any costs or expenses incurred by respondents in complying with the requirements of this ITR; and
- (d) neither these conditions nor the response gives rise to contractual obligations between the Commonwealth and the respondent.

### 3.4 Use of Response Documents

---

- 3.4.1 Respondents are to submit documents in response to this ITR on the basis that the Commonwealth may use, retain and copy the information contained in those documents for the purposes of evaluation of proposals pursuant to this ITR, shortlisting respondents, preparation of any resultant Multi Use List or resultant RFT or resultant Contract or any review of the acquisition process. Notwithstanding this clause 3.4, ownership of the Intellectual Property in the proposal shall remain unchanged.
- 3.4.2 Respondents should note that the Commonwealth may provide the responses, either in whole or in part, to a third party for the purposes of assisting the Commonwealth in the purposes listed in 3.4.1. The Commonwealth shall obtain a deed of confidentiality between the Commonwealth and a third party prior to that third party being provided with documentation requiring protection.
- 3.4.3 Respondents should be aware that the Commonwealth may wish to include information which is provided in its response to this ITR in any subsequent RFT. Respondents are to indicate their acceptance of this in Annex B.
- 3.4.4 Respondents should also note the provisions of the *Freedom of Information Act 1982 (Cth)* and the commercial confidentiality aspect of this ITR.
- 3.4.5 Notwithstanding anything in this ITR, the Commonwealth reserves the right, in its absolute discretion and without the need to notify any respondent, to disclose or allow the disclosure of, at any time, any information contained in or relating to any response to any Commonwealth Department, agency, authority, Minister for the proper performance of their portfolio and statutory responsibilities, or to Parliament or Parliamentary Committees on request.

### 3.5 RESERVED

---

## 4. EVALUATION OF RESPONSE

### 4.1 Response Evaluation

---

- 4.1.1 The purpose of this ITR is to allow the Commonwealth to develop a list of respondents to be registered on a Multi Use List, subject to clause 1.3. The responses will be assessed according to the following criteria, which are in order of importance and are exhaustive:

- (a) Compliance with Conditions of Participation specified
- (b) the financial viability and capability of the respondents to complete the requirement;
- (c) the technical and managerial capability of the respondents to complete the requirement;
- (d) the experience of the respondents in undertaking similar requirements;
- (e) the quality of the respondents response against the requirement; and
- (f) the respondent's compliance with Commonwealth and Defence procurement policies and procedures.

#### **4.2 Conditions of Participation**

---

4.2.1 The Commonwealth will exclude a tender from further consideration if the Commonwealth considers that the tenderer does not have the following:

- (a) I-RAP registered; and
- (b) DISP registered.

4.3 **RESERVED**

4.4 **RESERVED**

#### **4.5 Debriefing of Respondents**

---

4.5.1 Respondents may request a debriefing following the conclusion of the ITR process. Respondents requiring a debriefing should contact the Contact Officer specified in clause 2.6 of this ITR.

4.5.2 Respondents will be debriefed against any evaluation criteria contained in this ITR. In accordance with Commonwealth policy a respondent will not be provided with information concerning other responses, except for publicly available information or that provided as envisaged by clause 2.6. No comparisons with other responses will be made.

**ISIP ITR No: 2209/04  
ANNEX A**

**Declaration by Respondent**

*(Insert Name of Organisation and ACN/ABRN and ABN as applicable)* submits this ITR response to register its interest in the **Multi Use List for Various Security Compliance and Performance Review Services**, and to declare its willingness in principle to undertake and perform the work associated with the provision of the requirement.

*(Insert Name of Organisation)* acknowledges that this ITR response will become the property of the Commonwealth upon submission, and will not be returned.

This ITR response has been compiled without the improper assistance of employees or former employees of the Commonwealth, and without the use of information obtained unlawfully or in breach of an obligation of confidentiality to the Commonwealth.

Signature of Respondent, or person authorised to sign the response on behalf of the Respondent:

**SIGNATURE:**

**DATE OF SIGNATURE:**

.....

.....

**NAME (Block Letters):**

**POSITION HELD:**

.....

.....

**SIGNATURE OF WITNESS:**

**ADDRESS OF WITNESS:**

.....

.....

**NAME (Block Letters):**

.....

.....

**ISIP ITR No: 2009/04  
ANNEX B**

**INFORMATION TO BE SUPPLIED BY RESPONDENT**

<b>Full Company or Organisation Name</b>			
<b>Date and Place of Incorporation</b>			
<b>Company Number and/or Business Number (eg. ACN/ABN)</b>			
<b>Any Trading or Business Name</b>			
<b>Names of any Associated Companies that may be involved in the proposed contract (consortium and/or subcontractor details)</b>			
<b>Details of the Company (and those of consortium members and subcontractors where applicable)</b>	Registered Office(s)	Principal Place(s) of Business	
<b>Individual shareholders holding 20 percent or more of any issued share capital for the proposed prime contractor</b>			
<b>Particulars of any foreign national, foreign bodies, etc. in a position to exercise control or influence over the proposed prime contractor</b>			
<b>Postal Address for all correspondence</b>			
<b>Address(es) of the location(s) where management of the Contract and any other off-site work would be conducted</b>			
<b>Executive Member nominated to receive correspondence</b>	Name		Title
<b>Contact Details</b>	Phone	Fax	e-mail
<b>Nominated Company Point of Contact</b>	Name		Title
<b>Contact Details</b>	Phone	Fax	e-mail

**ISIP ITR No: 2009/04  
ANNEX B**

**INFORMATION FOR SHORT-LISTING**

***Note to respondents: The following information is required to allow the Commonwealth to short-list ITR respondents. Responses assessed as being non-competitive against the evaluation criteria may be excluded from the short-list. Responses to this ITR may be assessed on a comparative basis against both the short-listing criteria and other responses.***

**Management**

The respondent is to provide details that demonstrate its capacity to satisfy the Commonwealth's requirement from a managerial perspective. This response should ensure the areas of competency and managerial experience are addressed. Details should be provided of arrangements for Contract management and customer interface mechanisms.

Where the respondent proposes utilising sub-contractors for delivery of a part of the requirements, details should be provided of the company's demonstrated ability to manage sub-contractors.

**Overall Organisational Arrangements**

The respondent is to provide an overview of the proposed organisational structure in a chart, covering operational and managerial aspects and in narrative format. This should include any potential sub-contractor relationships.

The respondent is to provide an organisation chart indicating the context within which those responsible for the provision of the proposed services will operate. Respondents should indicate how reporting to upper management will take place.

**Finance**

The respondent is to identify, consistent with the business relationships described in the overall response, the proposed prime contracting entity.

***Note to respondents: The Commonwealth would normally expect the respondent to this ITR to be the contracting entity.***

The Respondent is to provide incorporation details, ownership, corporate relationships and principal functions of the proposed contracting entity.

The respondent is to provide details of its annual revenue and profit/loss statements for the past 3 years.

**Personnel**

The respondent is to provide a list of Specified Personnel for membership under the Multi Use List including, as a minimum, the following details in respect of each of the Specified Personnel proposed:

<b>Name and Position</b>	<b>Qualifications (Particularly Tertiary Level Qualifications as set out under Annex C)</b>	<b>The Level and Type of Security Clearances Currently Held</b>	<b>Relevant Experience in Tasks Similar to that to be Conducted under the Statement of Work</b>	<b>Referees</b>

**ISIP ITR No: 2009/04  
ANNEX B**

**Requirement**

The respondent is to indicate which category or subcategory they would like to register for and up to five (5) examples of no longer than one A4 page per example of similar activities they have undertaken in accordance with the Commonwealth's requirements identified at Annex C in the Table below:

Category	Subcategory	Please tick preferred sub/category
(a) <b>Security reviews</b> will primarily fall into four security categories:	(A tick in this box includes all the subcategories)	
	(i) information, and communications technology security (ICT)	
	(ii) physical, personnel and information security	
	(iii) handling and management of weapons, munitions and explosives (WME) throughout their lifecycle	
	(iv) Other tasks that may be required include the development of:	
	• review methodology;	
	• performance review methodology;	
	• templates;	
	• review tracking;	
	• reporting mechanisms;	
• research of best practice security review.		
(b) <b>Security performance and Compliance</b> will primarily fall into three security categories:	(A tick in this box includes all the subcategories)	
	(i) Physical security;	
	(ii) Information, communications and technology (ICT) security;	
	(iii) Personnel and information security	

**ISIP ITR No: 2009/04  
ANNEX C**

**EXAMPLE DESCRIPTION OF REQUIREMENT**

This Example Description of Services set out under this Annex C to the ITR is **for information only** and is not part of the evaluation process or response documents and is only to ensure Respondee have an example of the types of requirements that may be requested in accordance with 1.2.1 by the Commonwealth.

**EXAMPLE ONLY – DO NOT RESPOND TO THIS DOCUMENT**

**Introduction**

1. The Commonwealth represented by the Defence Security Authority (DSA) is tasked with establishing a security compliance and performance review capacity within Defence. The capacity will be established through the selection of a number of service providers for a panel arrangement under a Deed of Standing Offer (Standing Offer). This capacity will assist the Secretary, Chief of Defence Force (CDF) and Group Heads by providing assurance that security policy and practices are applied appropriately across Defence at the enterprise and systems levels.
2. The capacity will also assist Defence commanders and managers at all levels, by proposing improvements to Defence security policy and practice by assessing and reporting on:
  - 2.1 the effectiveness of Defence protective security policy;
  - 2.2 the effectiveness and efficiency of security programs and response plans across Defence;
  - 2.3 systemic vulnerabilities in Defence security; and
  - 2.4 compliance with security policy.
3. The Contractor is advised that the Commonwealth is seeking a response for either one of two requirements or both requirements being:
  - 3.1 **Requirement A** - Directorate of Security Performance Review (DSPR) security performance and compliance reviews;
  - 3.2 **Requirement B** – Defence Security Authority (DSA) Security Compliance Augmentation Program; or
  - 3.3 **Requirement C** – both Requirement A and Requirement B.
4. The Commonwealth expects Respondents to be able to provide the full range of services for either Requirement A or Requirement B or both as detailed in this **Annex C**.
5. The Contractor is to clearly mark their response with either “Requirement A”, “Requirement B” or “Requirements C”.

**ACCEPTANCE OF SERVICES**

1. Acceptance of the Services is required under this Deed.

**ISIP ITR No: 2009/04**  
**ANNEX C**

**REQUIREMENT A**

**Background to Requirement A**

1. The Directorate of Security Performance Review (DSPR) was set up within DSA to implement and promote a program of security reviews. The DSPR focus is on reviewing the performance of security within Defence. The resultant Standing Offer will augment DSA's internal capacity to undertake security reviews.
2. DSPR reviews are identified on the DSPR Annual Work Plan based on direction from the Defence Audit Committee and the Defence Security Advisory Group. Consequently, the scope of each review is broad, with high level direction and stakeholder involvement across multiple groups and services.
3. DSA expects that a panel member will be primarily tasked through an Official Order by DSPR with undertaking security performance reviews, however, there will be occasions when reviews will be a combination of both security performance and compliance.

**Two Categories of Reviews**

1. There are two categories of review for Requirement A which are **Security Performance Review (SPR)** and **Security Compliance Review (SCR)**.
2. **Security Performance Review (SPR)**
  - 2.1 a security performance review is:
    - (i) the process of measuring efficiency and effectiveness of security programs, facilities, practices and policies, and
    - (ii) these reviews answer questions such as "Are things being done in the right way? Are the right things being done?"
  - 2.2 an SPR may:
    - (i) focus on the Defence-wide and systemic application of security policy and practices;
    - (ii) analyse Defence policy, standards and practice to identify common or systemic vulnerabilities in Defence security;
    - (iii) assess the effectiveness of Defence's security policy, procedures and measures;
    - (iv) examine the adequacy of internal procedures (controls) for promoting and monitoring security.
  - 2.3 an SPR will:
    - (i) make recommendations to improve security practices.
3. **Security Compliance Review (SCR)**
  - 3.1 an SCR is the process of measuring the degree to which:

**ISIP ITR No: 2009/04**  
**ANNEX C**

- (i) a facility, system, process, plan or response meets the relevant security policy, standards and guidelines; or
  - (ii) previous security recommendations have been implemented.
- 3.2 an SCR will:
- (i) make recommendations to improve security practices.
- 3.3 SCRs will primarily fall into three security categories:
- (i) information, and communications technology security (ICT);
  - (ii) physical, personnel and information security, or
  - (iii) handling and management of weapons, munitions and explosives (WME) throughout their lifecycle.

**REQUIREMENT A – SCOPE OF SERVICES**

1. If required by an Official Order, the Contractor will be required to perform security performance or compliance reviews using standardised risk assessment and review (or audit) methodologies as described below:
  - 1.1 Defence Risk Analysis must meet AS/NZS 4360: *Risk Management* using a Defence process called DEFRIMS
  - 1.2 Defence Review or Audit must meet AS/NZS ISO 9001:2000: *Quality management systems - Requirements standard*.
2. If required by an Official Order, the Contractor will be required to perform security performance or compliance reviews with reference to and in accordance with:
  - 2.1 the Defence Security Manual (DSM), and
  - 2.2 other relevant government security policy and standards such as the *Protective Security Manual* (PSM) and the *Australian Communications Security Instruction 33* (ACSI 33).
3. If required by an Official Order, each task will require the successful Contractor to:
  - 3.1 hold meetings with Director DSPR and team leaders;
  - 3.2 hold meetings with the relevant Defence owner addressed in the security review task;
  - 3.3 undertake field work where appropriate;
  - 3.4 gather information;
  - 3.5 analyse relevant security policy, and
  - 3.6 make recommendations to improve the effectiveness, efficiency and adequacy of security.
4. If required by an Official Order, the Contractor will be expected to deliver progress reports on a fortnightly basis, or as requested in any attached tasking statement, and a final report on the security performance or compliance review including such details as:

**ISIP ITR No: 2009/04**  
**ANNEX C**

- 4.1 the checks undertaken on the system, facility or process;
  - 4.2 findings of any security compliance work undertaken;
  - 4.3 findings on any performance issues identified;
  - 4.4 discrepancies identified, if any, between the security policy and the particular system, process or facility being reviewed;
  - 4.5 recommendations for improvements to physical, information, personnel, process and/or systems security practices or policy; and
  - 4.6 other areas of interest as directed.
5. The final report will detail recommendations for improvements. Such improvements may be for changes to security policy, security procedure, operational capability, and business improvement and certification and accreditation documentation. A report template will be developed, in conjunction with the successful Contractor, early in the life of the Standing Offer through an Official Order. Contractors are advised that any template created during the course of an activity identified under an Official Order will become the property of the Commonwealth for use in relation to all security activities as appropriate.
6. DSA anticipates that between 10 and 20 reviews will be sought through an Official Order per year in the following security review categories (without limitation):
- 6.1 ICT – between 2 and 6 reviews; and
  - 6.2 Other reviews – between 3 and 6 reviews.
7. Other tasks that may be required include the development of (without limitation):
- 7.1 review methodology;
  - 7.2 performance review methodology;
  - 7.3 templates;
  - 7.4 review tracking;
  - 7.5 reporting mechanisms; and
  - 7.6 research of best practice security review.

## **CONTRACTOR REQUIREMENTS**

### **Clearance Level**

1. The Contractor and their personnel must hold a **SECRET** level security clearance or be eligible to obtain a security clearance at the SECRET level as a minimum, to be able to undertake the required work.

### **Travel**

1. Although a majority of the work will be undertaken in the Australian Capital Territory (ACT), Contractors must have the capacity to undertake work throughout Australia. DSA expects travel expenses to be paid in accordance with the resultant Standing Offer conditions.

### **Information and Communication Technology (ICT)**

**ISIP ITR No: 2009/04**  
**ANNEX C**

1. Contractors tendering for ICT reviews should note that Defence has a preference for Contractors who meet the following standards:
  - 1.1 Security Construction and Equipment Committee (SCEC) membership or be willing to obtain this membership within the first month of entering into the Panel Arrangement, and/or
  - 1.2 Infosec Registered Assessor Program (IRAP) or be willing to obtain registration within the first month of entering into the Panel Arrangement;
  - 1.3 knowledge of and experience in industry-standard compliance and risk methodologies, such as Sarbanes-Oxley or a recognised equivalent;
  - 1.4 knowledge of and experience in government security policy such as PSM, ACS133 and the DSM;
  - 1.5 knowledge of ICT networks and platforms, access control, application security architecture and general ICT security principles; and
  - 1.6 an understanding of ICT Security compliance and review knowledge and experience, particularly international Information Security standards such as ISO 17799 & COBIT.
2. All Contractors must:
  - 2.1 be members of the Defence Industry Security Program (DISP) or be willing to seek membership within the first month of entering into the Panel Arrangement, and
  - 2.2 hold the relevant state security licences where applicable.
3. Contractors are to indicate their capacity to undertake the various reviews against Table 1-0 below:

**Table 1-0: Security Reviews**

<b>Type of service</b>	<b>Services can be provided</b>
ICT security	
Physical security	
Personnel Security	
Information Security	
Weapons, Munitions and Explosives Security	

**ISIP ITR No: 2009/04  
ANNEX C**

**REQUIREMENT B**

**Background to Requirement B**

1. DSA requires work to be carried out in support of the DSA security Compliance augmentation program. The Security Compliance Program is over sighted by the DSA Directorate of Security Operations.

**Protective Security Compliance**

1. To maintain effective protective security in Defence, periodic Compliance must occur. The aim of Compliance is to:
  - 1.1 ensure that security measures in place are sufficient to counter any perceived security threat and achieve an acceptable level of risk for an establishment;
  - 1.2 inform commanders and managers of the current state of security within units and facilities for which they are responsible; and
  - 1.3 ensure that existing security measures:
    - 1.4 are applied efficiently and effectively;
    - 1.5 are realistic and practical; and
    - 1.6 make the best use of available resources.
2. Protective security Compliance **only** covers processes that affect the security of assets within a Defence unit or a Defence Industry Security Program (DISP) organisation.

**REQUIREMENT B – SCOPE OF SERVICES**

**Security Compliance Activities**

1. If required by an Official Order, the Contractor will be required to conduct **security Compliance activities**, the processes involving security surveys, security inspections and visits as defined below, to:
  - 1.1 measure a Defence unit or DISP organisation’s compliance with protective security measures as detailed in the Defence Security Manual (DSM);
  - 1.2 report to the DSA on the findings of those **security Compliance activities**; and
  - 1.3 make recommendations to improve the effectiveness, efficiency and adequacy of security measures utilised within a Defence or DISP workgroup.
2. The Compliance methods are identified at Table 1-1 below:

**Table 1-1: Compliance Methods**

<b>Compliance Method</b>	<b>Purpose</b>
<b>Protective Security Survey (PSS)</b>	Provides a complete appraisal of all aspects of security within a Defence unit or DISP organisation.
<b>Protective Security</b>	Conducted to:

**ISIP ITR No: 2009/04  
ANNEX C**

Compliance Method	Purpose
<b>Inspection (PSI)</b>	<ul style="list-style-type: none"> <li>• cover a particular aspect of security;</li> <li>• update a survey; and/or</li> <li>• check that previous recommendations have been implemented</li> </ul> <p>within a Defence unit or DISP organisation.</p>
<b>Protective Security Advisory Visit (PSAV)</b>	<p>Provide advice on:</p> <ul style="list-style-type: none"> <li>• security issues,</li> <li>• implementing recommendations made in previous PSS or PSI;</li> <li>• conducting security education and training;</li> <li>• changes to unit security measures required to meet alterations in role, capabilities or accommodation; and</li> <li>• other matters at the request of the unit, workgroup head, manager or Unit/Facility Security Officer.</li> </ul> <p>Discuss major changes to security policy or procedures directly affecting the Defence unit or DISP organisation with the unit workgroup head, manager or Unit/Facility Security Officer.</p>

3. DSA expects that **security Compliance activities** will be undertaken by the Contractor. If required by an Official Order, all security Compliance activities will be conducted in accordance with the timetable, as provided in writing to the Contractor by the DSA and as amended from time to time.
4. The Contractor must have the capacity to undertake **security Compliance activities** throughout the regions of Australia identified at Table 1-2 below:

**Table 1-2: Estimated Compliance Numbers by Regions**

Ser	Region	Responsible DSA Office
1	Australian Capital Territory	<b>ACT SNSW (Canberra)</b>
2	Southern New South Wales	
3	Victoria	<b>VIC TAS (Melbourne)</b>
4	Tasmania	
5	New South Wales	<b>NSW (Sydney)</b>
6	Southern Queensland	<b>QLD (Brisbane)</b>
7	Northern Queensland	<b>QLD (Townsville)</b>
8	South Australia	<b>SA (Edinburgh)</b>
9	Northern Territory	<b>NT (Darwin)</b>
10	Western Australia	<b>WA (Rockingham)</b>

**Security Compliance Activities Methodologies**

1. If required by an Official Order, **security Compliance activities** undertaken by the Contractor will be conducted in accordance with the methodologies for each described activity identified at Tables 1-3 and 1-4 below:

**ISIP ITR No: 2009/04**  
**ANNEX C**

**Table 1-3: Security Compliance Methodology - PSS**

Activity	Methodology
<p><b>Protective Security Survey (PSS)</b></p>	<p><b>Purpose:</b> A detailed pre-planned examination carried out by security staff to examine, report and make recommendations concerning all aspects of security within a Defence unit or DISP organisation.</p> <p><b>STEP 1</b> - Requirement for conduct of PSS identified by DSA and notified in writing to the Contractor.</p> <p><b>STEP 2</b> – Contractor prepares for the conduct of the PSS:</p> <ul style="list-style-type: none"> <li>• Review workgroup and source data as provided by DSA.</li> <li>• Populate Security Electronic Aide Memoire (SEAM) with data provided by DSA.</li> <li>• Review workgroup history as supplied by DSA.</li> <li>• Commence liaison with affected workgroup: <ul style="list-style-type: none"> <li>❖ Contact workgroup Point of Contact (POC) as advised by DSA - usually Unit/Facility Security Officer (USO/FSO) or workgroup commander or manager.</li> <li>❖ Brief POC on PSS procedures and anticipated timelines.</li> </ul> </li> <li>• Prepare letter/minute (<b>templates will be provided by DSA</b>) to Defence unit or DISP organisation commander or manager outlining PSS procedures and anticipated timelines for release by nominated DSA regional office Manager Security Operations.</li> </ul> <p><b>STEP 3</b> - Contractor conducts the PSS using SEAM.</p> <ul style="list-style-type: none"> <li>• Brief commanders and managers, USO/FSO and other workgroup staff as required.</li> <li>• Review Procedural and Personnel Security issues through confirmation of and/or spot-checks of: <ul style="list-style-type: none"> <li>❖ DISP Accreditation (Industry) - is the accreditation type and level appropriate?</li> <li>❖ PSAMS (checklist provided by DSA) Designated Security Assessed Position check - are security clearances held by workgroup personnel at the appropriate level?</li> <li>❖ Unit/Facility Security Register - are all relevant sections contained within the register and is it being properly maintained?</li> <li>❖ Unit Security Standing Orders/ Facility Security Practices and Procedures - is content suitable for workgroup and are they circulated to relevant personnel on a regular basis?</li> <li>❖ Classified Document Register inspection (spot check).</li> <li>❖ Security Plan - result of DEFRIMS (as described in the DSM) Security Risk Assessment process.</li> <li>❖ Does the organisation have a current Threat Assessment?</li> <li>❖ Business continuity plan.</li> <li>❖ Protective Security (guarding) presence/procedures.</li> <li>❖ Access control – receptionist, sign in book, escorting, electronic.</li> </ul> </li> <li>• Review: <ul style="list-style-type: none"> <li>❖ Area ratings, eg Intruder Resistant, Secure (complete applicable area of SEAM).</li> <li>❖ Asset protection arrangements (complete applicable area of SEAM).</li> <li>❖ Are physical security containment measures adequate to contain asset types held by workgroup?</li> </ul> </li> <li>• Debrief USO/FSO and/or commanders and managers: <ul style="list-style-type: none"> <li>❖ Major issues identified.</li> <li>❖ The way forward.</li> <li>❖ DSA POC for follow up of queries regarding PSS outcomes.</li> </ul> </li> </ul>

**ISIP ITR No: 2009/04  
ANNEX C**

Activity	Methodology
	<p><b>STEP 4</b> - Contractor conducts the following post survey activity:</p> <ul style="list-style-type: none"> <li>• Collate and analyse information gathered.</li> <li>• Determine issues to be corrected.</li> <li>• Identify short and long term treatments with interim brief to USO/FSO and commanders and managers as required.</li> <li>• Produce PSS Report (<b>template provided by DSA</b>) and provide to DSA.</li> </ul>

**Table 1-4: Security Compliance Methodology - PSI**

Activity	Methodology
<p><b>Protective Security Inspection (PSI)</b></p>	<p><b>Purpose:</b> A routine inspection carried out by security staff, either to review a specific aspect of security within a Defence unit or DISP organisation, or as a follow-up to a Protective Security Survey to ensure that recommendations have been implemented.</p> <p><b>STEP 1</b> - Requirement for conduct of PSI identified by DSA and notified in writing to Contractor.</p> <p><b>STEP 2</b> - The DSA determines what security aspects within the workgroup are to be covered as part of the PSI and advises the Contractor.</p> <p><b>STEP 3</b> – Contractor conducts the PSI utilising SEAM.</p> <p><b>AS REQUIRED</b> to satisfy intent of conducting PSI:</p> <ul style="list-style-type: none"> <li>• Brief commanders and managers, USO/FSO and other workgroup staff as required.</li> <li>• Review Procedural and Personnel Security issues through confirmation of and/or spot-checks of: <ul style="list-style-type: none"> <li>❖ DISP Accreditation (Industry) - is the accreditation type and level appropriate?</li> <li>❖ PSAMS (checklist provided by DSA) Designated Security Assessed Position check - are security clearances held by workgroup personnel at the appropriate level?</li> <li>❖ Unit/Facility Security Register - are all relevant sections contained within the register and is it being properly maintained?</li> <li>❖ Unit Security Standing Orders/ Facility Security Practices and Procedures - is content suitable for workgroup and are they circulated to relevant personnel on a regular basis?</li> <li>❖ Classified Document Register inspection (spot check).</li> <li>❖ Security Plan - result of DEFRIMS (as described in the DSM) Security Risk Assessment process.</li> <li>❖ Does the organisation have a current Threat Assessment?</li> <li>❖ Business continuity plan.</li> <li>❖ Protective Security (guarding) presence/procedures.</li> <li>❖ Access control – receptionist, sign in book, escorting, electronic.</li> </ul> </li> <li>• Review: <ul style="list-style-type: none"> <li>❖ Area ratings, eg Intruder Resistant, Secure (complete applicable area of SEAM).</li> <li>❖ Asset protection arrangements (complete applicable area of SEAM).</li> <li>❖ Are physical security containment measures adequate to contain asset types held by workgroup?</li> </ul> </li> <li>• Debrief USO/FSO and/or commanders and managers:</li> </ul>

**ISIP ITR No: 2009/04  
ANNEX C**

Activity	Methodology
	<ul style="list-style-type: none"> <li>❖ Major issues identified.</li> <li>❖ The way forward.</li> <li>❖ DSA POC for follow up of queries regarding PSI outcomes.</li> </ul> <ul style="list-style-type: none"> <li>• Debrief USO/FSO and/or commanders and managers: <ul style="list-style-type: none"> <li>❖ Major issues identified.</li> <li>❖ The way forward.</li> <li>❖ DSA POC for follow up queries regarding PSI outcomes.</li> </ul> </li> </ul> <p><b>STEP 4</b> - Contractor conducts the following post inspection activity:</p> <ul style="list-style-type: none"> <li>• Collate and analyse information gathered.</li> <li>• Determine issues to be corrected.</li> <li>• Identify short and long term treatments with interim brief to USO/FSO and commanders and managers as required.</li> <li>• Produce PSI Report (<b>template provided by DSA</b>) and provide to DSA.</li> </ul>

**Compliance Reports**

1. If required by an Official Order, the Contractor will be expected to provide copies of reports resulting from the conduct of security Compliance activities to the relevant DSA Representative, by the date nominated by the DSA Representative.
2. All security Compliance reports produced and submitted by the Contractor to the DSA Representative are to conform to the template format as provided by the DSA. Templates will be provided at the commencement of an activity.
3. All security Compliance reports are to be produced and submitted by the Contractor to the DSA Representative in both printed form and electronically in Microsoft Word 2003 version format, or in updated Microsoft software suite versions used as the standard within Defence, as may be advised by the DSA Representative from time to time.
4. Information resulting from the conduct of security Compliance activities, including security Compliance reports, is only to be recorded and/or produced on electronic information technology (IT) systems that have been accredited by the appropriate Defence authority and that have been endorsed for such use by the DSA. Accreditation of IT systems will be provided as part of Contractor DISP entry requirements and processes which are described at clause 3.9.1 below.
5. Reports produced by the Contractor are to be transmitted to the DSA in accordance with the procedures mandated by the DSM, relative to the security classification level applied to the reports by the Contractor.
6. Compliance reports produced by the Contractor are to be submitted to the Principal Security Adviser, Protective Security Section in the relevant DSA regional office as detailed at Table 1-5 below:

**Table 1-5: Regional DSA Representatives**

Ser	Defence or DISP Workgroup Location
1	Australian Capital Territory
2	Southern New South Wales
3	Victoria
4	Tasmania
5	New South Wales
6	Southern Queensland
7	Northern Queensland
8	South Australia

**ISIP ITR No: 2009/04  
ANNEX C**

Ser	Defence or DISP Workgroup Location
9	Northern Territory
10	Western Australia

**Review, Approval or Non-Approval, and Acceptance of Reports**

1. If, the DSA Representative provides the Contractor with notice of non-approval of a report, the DSA Representative will advise the Contractor in writing of the reasons for non-approval and may provide details of any corrective action to be taken by the Contractor before the report will be reconsidered for approval.
2. The DSA Representative's reasons for non-approval of a report will be limited to the context of any or all of the following criteria:
  - 2.1 in the judgement of the DSA Representative, the report submitted by the Contractor is not clearly understandable;
  - 2.2 in the judgement of the DSA Representative, the report submitted by the Contractor does not provide adequate detail;
  - 2.3 in the judgement of the DSA Representative, the report submitted by the Contractor is inconsistent with the Contract; and
  - 2.4 in the judgement of the DSA Representative, the report submitted by the Contractor will not meet the objective of the security Compliance activity conducted by the Contractor.
3. If the DSA Representative provides the Contractor with notice of non-approval, the Contractor will, within a period of **one working week** deliver the rectified report to the DSA Representative for approval.

**DOCUMENTATION**

1. **Where considered necessary by the DSA**, the list of Security Manuals and other security policy documentation identified at Table 1-6, and as amended from time to time, will be made available by the DSA to the Contractor to assist in the conduct of the security Compliance activities:

**Table 1-6: Security Reference Material**

Title	Description
<b>PSM</b>	Australian Government Protective Security Manual
<b>DSM</b>	Defence Security Manual
<b>ACSI 33</b>	Australian Government Information and Communications Technology Security Manual
<b>ACSI 53</b>	Communications Security Handbook
<b>SEC Catalogue</b>	Security Equipment Catalogue
<b>DCSRM</b>	Defence Construction Security Reference Manual – including the RESTRICTED Construction Security Function matrix to support DCSRMs
	The Australian Code for the Transport of Explosives by Road and Rail
<b>DCM 10/98</b>	Defence Security Pass and Access Control System
<b>DI (G) ADMIN 23-5</b>	Overseas Visits
<b>DSI 3/2004</b>	Defence standards for commercial grade Information and Communications Technology equipment cabinets
<b>Title</b>	Description
<b>DSI 4/2003</b>	Policy on external connections to the Defence Information Environment

**ISIP ITR No: 2009/04  
ANNEX C**

<b>Title</b>	<b>Description</b>
<b>DSI 3/2003</b>	Classification of standard operating environment for the Defence Information Environment
<b>DSI 3/2002</b>	Use of cordless telephones within Defence environments
<b>DSI 2/2001</b>	Defence Information Environment Web Communities, Chat Forums, News and on-line discussion groups
<b>DSI 9/99</b>	Security Considerations for Unit Home Pages
<b>DSI 5/99</b>	Telephone security - classified and unclassified discussions RESTRICTED

2. If required by an Official Order, additional and future Australian Government and Defence security policy documentation, directly affecting the security Compliance activities being undertaken by the Contractor, will be made available to the Contractor by the DSA as and when required.

**GOVERNMENT FURNISHED MATERIAL (GFM)**

**Provision and Management of GFM**

1. If required by an Official Order, the DSA will deliver or provide access to GFM, to assist in the conduct of security Compliance activities, to the Contractor at the place and times as determined by the DSA Representative.
2. The Contractor will be required to acknowledge in writing receipt of the GFM to the DSA Representative upon delivery.
3. If the GFM is not accompanied by an issue voucher from the DSA, the Contractor will be required to report that omission in the acknowledgment of receipt for that GFM.
4. The Contractor will be required:
  - 4.1 upon receipt of the GFM, inspect GFM for defects or deficiencies and any physical damage which impact on, or are likely to impact on, the intended use of the GFM;
  - 4.2 at least five days prior to the date that the Contractor intends to utilise an item of GFM in connection with the provision of the Services, carry out appropriate functional testing to the extent feasible of that item to determine that it is serviceable for use as required by the Contract; and
  - 4.3 report in writing its satisfaction or dissatisfaction with the GFM to the DSA Representative within two days of inspection or functional testing.
  - 4.4 The Contractor will not use in connection with the services GFM that has been found on inspection to be materially damaged, defective or deficient.
  - 4.5 The Contractor will, in a skilful manner, utilise the GFM in the provision of the services in accordance with the Contract.

**Care of GFM**

1. The Contractor will be expected to take all reasonable care of GFM in its care, custody or control.
2. The Contractor will be expected to provide facilities, endorsed by DSA, to store and handle all GFM as it is received.

**ISIP ITR No: 2009/04**  
**ANNEX C**

3. The Contractor will be required to institute, maintain and apply a system for, and comply with the provisions of the Contract and any directions of the DSA Representative in respect of, the accounting for and control, handling, preservation, protection, maintenance and repair of GFM and any installation, setting to work, inspection, test or trial of GFM required under the Contract.
4. The Contractor will be expected to carry out such physical stock takes and certification of the GFM as the DSA Representative may by notice from time to time require.

**Shared GFM**

1. The Contractor will be required to acknowledge that certain GFM may also be utilised by the DSA and other DSA Contractors during the period of the Contract.
2. The parties will agree that:
  - 2.1 the DSA and the Contractor will act reasonably in sharing such GFM;
  - 2.2 any conflicts that arise regarding the use of the shared GFM can be referred by either party to the DSA Representative, who will decide on the operational priority of the tasks requiring the use of shared GFM;
  - 2.3 the DSA Representative will be guided by the relative operational priority of tasks in deciding which party has priority of use of the shared GFM; and
  - 2.4 the DSA Representative's decision on which party has priority of use of shared GFM will be final and binding.
3. The Contractor is advised that the DSA will be responsible for the operational level maintenance of shared GFM while in the DSA's care, custody and control.

**Provision and Management of Government Furnished Facilities**

1. The DSA will provide Contractor's personnel with office facilities and computer equipment necessary to facilitate background research activities and the production of reports resulting from security Compliance activities.

**TRAINING IN DEFENCE INFORMATION SYSTEMS**

1. The Contractor will be required to ensure that all relevant personnel, agents and sub-contractors, are trained in the operation of mandated Defence information systems. If required by an Official Order, a list of the relevant ICT systems will be provided to the Contractor on request.

**Training Cost**

1. During Phase-in, the DSA will provide, at no cost to the Contractor, the requisite training to allow the Contractor to conduct activities relating to mandated Defence information systems and to other Defence information systems nominated by the DSA.
2. After the Operative Date, the DSA will provide appropriate initial training for any new or upgraded mandated Defence information system provided to the Contractor by the DSA. The DSA will provide such appropriate training to the Contractor in advance of the introduction of the new or upgraded Defence information systems, at no cost to the Contractor.
3. Following the initial training for any new or upgraded mandated Defence information systems, the DSA will only provide 'train the trainer' training. It is expected that the

**ISIP ITR No: 2009/04**  
**ANNEX C**

Contractor will send one to two representative/s who will be tasked with training the Contractor's other personnel in the Defence information system.

4. The Contractor's personnel will be trained free of charge once only by the DSA after which the DSA will apply a cost recovery mechanism for continued training.

**Training Reporting**

1. For the training being provided by the DSA pursuant to this clause, the Contractor will be required to:
  - 1.1 identify personnel requiring initial system training or initial system upgrade training available from the DSA;
  - 1.2 ensure personnel presented for training have a suitable level of general competence in the use of electronic information systems; and
  - 1.3 ensure it, and its sub-contractors meet all the employer's responsibilities, including all salaries, travel, and accommodation allowances for their personnel during training.

**CONTRACTOR REQUIREMENTS**

**Security Clearance Levels**

1. All Contractor personnel undertaking security Compliance activities on behalf of the DSA must have, or be eligible to obtain, a security clearance at the SECRET level as a minimum. SECRET clearances **MUST** be in place prior to Contractors being eligible to conduct security Compliance activities.
2. Security Compliance activities requiring a higher level of security clearance will be advised to the Contractor by the DSA on a case-by-case basis.

**DISP Entry Requirements**

1. Contractors contracted to conduct security Compliance activities **MUST**:
  - 1.1 be, or be eligible to become, a member of the **Defence Industry Security Program** (DISP); and
  - 1.2 satisfy, or be eligible to satisfy, the requirements for a DISP facility accreditation at the **SECRET** level for document storage and information systems as a minimum.
2. DISP accreditation **MUST** be in place prior to Contractors being eligible to perform security Compliance activities.

**State Licences**

1. All Contractor personnel undertaking security Compliance activities on behalf of the DSA must have the required state or territory licences.
2. The Contractor will be required to have the appropriate state or territory licence identified at Table 1-7 to be eligible to undertake security Compliance activities in that state or territory.

**Table 1-7: State Security Licences**

Ser	Defence or DISP Workgroup Location	Responsible DSA Office	Licence Type
1	Australian Capital Territory	<b>ACT SNSW (Canberra)</b>	
2	Southern New South Wales		

**ISIP ITR No: 2009/04  
ANNEX C**

Ser	Defence or DISP Workgroup Location	Responsible DSA Office	Licence Type
3	Victoria	<b>VIC TAS (Melbourne)</b>	
4	Tasmania		
5	New South Wales	<b>NSW (Sydney)</b>	
6	Southern Queensland	<b>QLD (Brisbane)</b>	
7	Northern Queensland	<b>QLD (Townsville)</b>	
8	South Australia	<b>SA (Edinburgh)</b>	
9	Northern Territory	<b>NT (Darwin)</b>	
10	Western Australia	<b>WA (Rockingham)</b>	

**Travel Requirements**

1. Contractors engaged in the conduct of security Compliance activities must have the capacity to undertake such work anywhere in Australia and must be prepared to travel to undertake that work. Travel expenses may be paid in accordance with Defence travel allowance rates. Contractors will be provided with applicable Defence travel rates as and when required.

**Contractor Training Competency Levels**

1. The Contractor will be required to undertake or have completed training:
  - 1.1 To be a SCEC endorsed consultant;
  - 1.2 For Certificate IV Security Risk Management;
  - 1.3 Additional training requirements to be provided

**Ad Hoc Meetings**

1. If scheduling *ad hoc* meetings, the party calling the meeting will provide the other party with reasonable advance notice of such meetings.
2. If the DSA Representative calls the meeting, the DSA Representative will advise the Contractor of the specific requirements for the meeting, the nature of the issues to be discussed, and the requirements for preparation and delivery of associated information by the Contractor.
3. If the Contractor calls the meeting, the Contractor will be required to advise the DSA Representative of the requirements for the meeting, the nature of the issues to be discussed, and the requirements for preparation and delivery of associated information by the DSA Representative.
4. The party calling the *ad hoc* meeting will be required to chair the meeting unless otherwise mandated by the DSA Representative.
5. The party calling the *ad hoc* meeting will deliver an agenda to the other party ASAP before each *ad hoc* meeting.
6. Unless otherwise agreed by the DSA Representative, the Contractor will be required to provide the facilities (including the meeting venue), materials and Services reasonably required for the conduct of *ad hoc* meetings.
7. The party that chairs the meeting will prepare and deliver minutes for each *ad hoc* meeting. If applicable, travel expenses may be paid to the Contractor in accordance with Defence travel allowance rates.

**ISIP ITR No: 2009/04  
ANNEX C**

**Contractor Operating Performance Reviews**

1. The Contractor will convene with the DSA's Representative for Operating Performance Reviews once every **three** months.
2. Meetings will be held at the relevant DSA Office or at the Contractor's facility, as agreed by the DSA's Representative, and will be chaired by the DSA's Representative. If applicable, travel expenses may be paid to the Contractor in accordance with Defence travel allowance rates.
3. The Contractor is advised that the meetings will:
  - 3.1 discuss the Contractor's performance in relation to the requirements of the Contract.
  - 3.2 identify and determine action requirements arising from the Contractor's performance in the previous period; and
  - 3.3 identify and determine action requirements for longer-term Operating Support and related logistics planning.
4. The Contractor will be required, upon request, to make supporting data for reviews available to the DSA's Representative

**CONTRACTOR QUALITY RESPONSIBILITIES**

**Quality Management System**

1. The Contractor will be required to have a Quality Management System Certified to AS/NZS ISO 9001:2000 at the Operative Date.
2. The Contractor will be required to take whatever action is necessary to correct a quality system/process/product non-conformance within any period agreed in writing by the DSA's Representative and will advise the DSA's Representative immediately upon taking corrective action. The DSA may perform an Audit to verify that the non-conformance has been corrected.

**Audit and Surveillance activities**

1. During progress of work under the Contract, the DSA may at its discretion perform Audit and Surveillance activities in relation to the work performed, including any of the following:
  - 1.1 System Audit;
  - 1.2 Process Audit; or
  - 1.3 Product Audit.

**Subcontractors**

1. The Contractor will be required to ensure that all **DSA approved** sub-contractors have quality management systems that are appropriate to the work required under the subcontract.
2. The Contractor will be required to ensure that all work performed under a subcontract meets the requirements of the quality system to be applied by the Contractor