

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE
CANBERRA

**Agreement between the Government of Australia
and the Kingdom of Spain
for the Mutual Protection of Classified Information of Defence Interest**

(Madrid, 17 November 2011)

Not yet in force
[2011] ATNIF 29

**AGREEMENT BETWEEN THE GOVERNMENT OF AUSTRALIA
AND THE KINGDOM OF SPAIN
FOR THE MUTUAL PROTECTION OF
CLASSIFIED INFORMATION OF DEFENCE INTEREST**

THE GOVERNMENT OF AUSTRALIA AND THE KINGDOM OF SPAIN (hereinafter referred to as “the Parties”)

NOTING the close co-operation between them in Defence matters;

RECOGNISING the benefits to be achieved through the exchange of information, including Classified Information; and

HAVING a mutual interest in the protection of Classified Information which is Defence-related and which is exchanged between them;

HAVE AGREED as follows:

**ARTICLE 1
DEFINITIONS**

For the purposes of this Agreement, the following definitions shall apply:

1. “Classified Contract” means any contract or subcontract between the Parties or with or between Contractors or potential Contractors, which contains, or the performance of which requires, access to Classified Information of either Party;
2. “Classified Information” means all information and material of Defence interest which requires protection in the interests of national security and which is subject to a national security classification of the Originating Party. The information may be in oral, visual, electronic, or documentary form, or in the form of material including equipment or technology;
3. “Contractor” means an individual, organisation or other entity, with the legal capacity to conclude contracts, including a Sub-Contractor that has entered into a Classified Contract with either of the Parties or each other;

4. "Facility Security Clearance" means a certification provided by a National Security Authority or an authority recognised by a National Security Authority which indicates that the facility is security cleared to a specified level and also has safeguards in place at a specified level to safeguard Classified Information;
5. "National Security Authority" means the authority designated by a Party as being responsible for the implementation and supervision of this Agreement;
6. "Need-to-Know" means a determination made by an authorised holder of Classified Information that a prospective recipient requires access to specific Classified Information in order to perform their official duties;
7. "Originating Party" means that Party which provides the Classified Information and accords it a national security classification, and which transmits Classified Information to the other Party;
8. "Personnel Security Clearance" means a certification provided by a National Security Authority or an authority recognised by the National Security Authority concerning the level of personnel security clearance held by a citizen of the certifying Party's country;
9. "Pre-contractual Arrangement" includes requests for tender, proposals, quotations or any other pre-contractual documentation relating to a potential Classified Contract;
10. "Recipient Party" means that Party which receives Transferred Classified Information from the Originating Party;
11. "Third Party" means any person or entity whose government is not a Party to this Agreement (including any third country government or international organisation, any citizen of a third country, and any Contractor); and
12. "Transferred Classified Information" means Classified Information which is passed between the Parties regardless of whether it is passed orally, visually, electronically, in writing, through the handing over of material or in any other form or manner.

ARTICLE 2 SCOPE

1. This Agreement sets out security procedures and practices for the exchange of Classified Information of Defence interest between the Parties and for the protection of such Transferred Classified Information. Each Party shall implement its obligations under this Agreement in accordance with its laws and regulations. Provisions relating to visit requirements and industrial operations are an integral part of this Agreement and are set out in Annexes A and B.
2. This Agreement shall not cover the exchange of classified information related to terrorism and intelligence. Such exchanges will require the negotiation of specific arrangements undertaken on the basis of this Agreement between the responsible authorities.

ARTICLE 3
NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities of the Parties shall be responsible for the implementation and supervision of this Agreement. Unless otherwise advised in writing, the National Security Authorities shall be:

For the Kingdom of Spain –

Secretary of State, Director of the National Intelligence Centre
National Security Office
Avda. del Padre Huidobro, s/n
28023 Madrid
SPAIN

For the Government of Australia –

Head Defence Security Authority
Department of Defence
Campbell Park Offices
Canberra ACT 2600
AUSTRALIA

2. The official channel of communication between the Parties for all matters relating to this Agreement shall be through the National Security Authorities.

ARTICLE 4
NATIONAL SECURITY CLASSIFICATIONS

1. Before transmission to the Recipient Party, the Originating Party shall assign all Classified Information with one of the following equivalent national security classifications:

In Spain	In Australia
RESERVADO	SECRET
CONFIDENCIAL	CONFIDENCIAL

2. The Recipient Party shall then assign the Transferred Classified Information with a national security classification no lower than the corresponding national security classification assigned by the Originating Party. Translations and reproductions shall be marked with the same national security classification as the originals, unless advised otherwise in writing by the Originating Party.

3. Anything produced by one Party that contains Transferred Classified Information provided by the other Party shall be marked SPAIN/AUSTRALIA or AUSTRALIA/SPAIN followed by the appropriate national security classification.

4. For Classified Information where a marking is not physically possible, the Originating Party shall inform the Recipient Party of the national security classification.

ARTICLE 5 DETAILS OF SECURITY STANDARDS

In order to achieve and maintain comparable standards of security the Parties shall on request provide each other with information about their national security standards, practices and procedures for the safeguarding of Classified Information, including those standards, practices and procedures which relate to its industrial operations. Each Party shall inform the other Party in writing of any changes to those security standards, practices and procedures which have an effect on the manner in which Transferred Classified Information is protected.

ARTICLE 6 SECURITY IMPLEMENTATION AND INSPECTIONS

1. Each Party shall ensure that establishments, facilities and organisations within its territory that handle Transferred Classified Information protect such Transferred Classified Information in accordance with the provisions of this Agreement.

2. Each Party shall ensure that within its territory necessary security inspections are carried out and appropriate security regulations and procedures are complied with in order to protect Transferred Classified Information.

ARTICLE 7 PROTECTION AND USE OF TRANSFERRED CLASSIFIED INFORMATION

The Parties shall apply the following rules for the protection and use of Transferred Classified Information:

1. the Recipient Party shall accord the Transferred Classified Information a standard of physical and legal protection, no less stringent than that which it accords its own Classified Information of a corresponding national security classification;
2. the Recipient Party shall obtain the prior written consent of the Originating Party prior to downgrading the national security classification or declassifying the Transferred Classified Information;
3. the Originating Party shall inform the Recipient Party of any changes in the national security classification of the Transferred Classified Information;
4. the Recipient Party shall not use the Transferred Classified Information for any purpose other than that for which it was provided, without the prior written consent of the Originating Party;
5. the Recipient Party shall not disclose, release or permit the disclosure or release of Transferred Classified Information under this Agreement to any Third Party, without the prior written consent of the Originating Party;
6. the Recipient Party shall take all appropriate steps legally available to it to keep Transferred Classified Information free from disclosure;
7. the Recipient Party shall comply with any additional limitations on the use, disclosure, release and access to Transferred Classified Information which may be specified by, or on behalf of, the Originating Party; and
8. when the Transferred Classified Information is no longer required for the purpose for which it was provided, the Recipient Party shall, subject to any specific instructions of the Originating Party return the Classified Information to the Originating Party or destroy the Classified Information in accordance with its security procedures, national security laws and regulations.

ARTICLE 8 ACCESS

1. Subject to the terms of this Agreement, access to Transferred Classified Information and to areas where classified activities are performed or where Transferred Classified Information is stored, shall be limited to those personnel of a Party who:
 - a) are citizens of either of the Parties, unless the Originating Party has given its prior written consent otherwise;
 - b) have been granted a Personnel Security Clearance to an appropriate level, in accordance with the Recipient Party's laws and regulations; and
 - c) have a Need-to-Know.
2. Notwithstanding Article 8(1)(b) above, a Spanish CONFIDENCIAL Personnel Security Clearance shall be required as a minimum for Spanish personnel accessing Australian RESTRICTED Classified Information.

3. The Parties acknowledge that the elected parliamentary representatives in both countries may continue to have access to Classified Information provided they apply their current practices when accessing such information.

ARTICLE 9 TRANSFER OF CLASSIFIED INFORMATION

1. Classified Information shall be transferred between the Parties in accordance with the national laws, security regulations and procedures of the Party transmitting the Classified Information.

2. Unless otherwise mutually determined by the Parties, the method of transfer of Classified Information shall be through government to government channels. If the use of such channels would be impractical or would unduly delay receipt of the Classified Information, transfers may be undertaken by appropriately security cleared and authorised government officials furnished with a courier certificate issued by the Party forwarding the Classified Information.

3. The Parties may transfer Classified Information by secure electronic means in accordance with security procedures mutually determined by the Parties' National Security Authorities.

ARTICLE 10 VISITS

1. Visits by personnel from one Party to the territory of the other Party requiring access to Classified Information or requiring access to areas which require a Personnel Security Clearance from the other Party, shall be subject to prior written approval of the National Security Authority of the Party whose territory the visit is occurring in.

2. The procedure for authorisation of such visits is outlined in Annex A to this Agreement.

ARTICLE 11 INTELLECTUAL PROPERTY RIGHTS

Nothing in this Agreement diminishes or limits any intellectual property right (including patents and copyrights) associated with Transferred Classified Information to which either Party, its Contractors or any Third Party may be entitled.

ARTICLE 12 BREACH OF SECURITY

In the case of a known or suspected breach of security with respect to Transferred Classified Information, the National Security Authority of the Recipient Party shall inform the National Security Authority of the Originating Party as soon as possible. The Recipient Party shall immediately investigate the circumstances of the breach and shall, without delay, inform the Originating Party of the circumstances, the findings of the investigation and any corrective action taken or to be taken.

ARTICLE 13 SETTLEMENT OF DISPUTES

Any disputes between the Parties arising from the implementation, interpretation or application of this Agreement shall be resolved amicably and expeditiously by consultation or negotiation between the National Security Authorities of the Parties and shall not be referred to any national or international tribunal or any Third Party for resolution.

ARTICLE 14 COSTS

Each Party shall bear its own costs incurred in the implementation of this Agreement.

ARTICLE 15 REVIEW

1. The Parties may review this Agreement at any time at the request of either Party.
2. Unless otherwise mutually determined in writing, the Parties shall review the implementation of the Agreement after every period of five years from the date of signature, to ensure that national security classifications of the Parties continue to correspond and to examine any changes to the Agreement which may be necessary to ensure that comparable standards for the protection of Transferred Classified Information are maintained.

ARTICLE 16 ENTRY INTO FORCE, AMENDMENT AND TERMINATION

1. This Agreement shall enter into force when the Parties have notified each other in writing that their respective requirements for the entry into force have been satisfied. The date of entry into force of the Agreement shall be the date of the last notification.
2. This Agreement may be amended at any time by the mutual determination of the Parties expressed in writing. Such amendments shall enter into force in accordance with paragraph 1 of Article 16.

3. This Agreement may be terminated at any time by mutual determination in writing or by either Party giving the other written notice of its intention to terminate the Agreement in which case it shall terminate six (6) months after the giving of such notice.

4. Notwithstanding termination, the responsibilities and obligations of the Parties in relation to the protection, disclosure and use of Transferred Classified Information shall continue to apply, in accordance with the provisions set forth herein, until the Originating Party releases the Recipient Party from this obligation.

IN WITNESS WHEREOF, the undersigned, being duly authorised thereto by their respective Governments, have signed this Agreement.

Done in duplicate at Madrid, on this seventeenth day of November 2011, in two originals each one in the Spanish and English languages, each version being equally authentic.

FOR THE GOVERNMENT OF AUSTRALIA

FOR THE KINGDOM OF SPAIN

HE Zorica McCarthy

Félix Sanz Roldán

Ambassador

Secretary of State
and Director of the National
Intelligence Centre

ANNEX A VISIT PROCEDURES

1. Visits by personnel of a Party requiring access to Classified Information held by the other Party, or requiring access to areas where access is restricted to individuals who have been security cleared require the prior approval of the National Security Authority of that other Party. Approval for such visits will be granted only to personnel who possess a valid Personnel Security Clearance to the appropriate level and have a Need-to-Know.
2. The National Security Authority of the visiting Party shall submit a request for visit to the National Security Authority of the host Party containing details of the planned visit, which shall be received at least twenty (20) working days prior to the date of the proposed visit.
3. In urgent cases, the request for visit should be transmitted at least five (5) working days or as soon as practicable prior to the date of the proposed visit.
4. The Parties shall inform each other in writing of the Authorities to be responsible for the procedure, control and supervision of the requests for visit.
5. The request for visit shall include:
 - a) visitor's full name, date and place of birth, citizenship, passport number;
 - b) name of the agency, establishment, facility or organisation they represent or to which they belong, their present position, and if appropriate, their rank;
 - c) certification of the visitor's Personnel Security Clearance, its validity, and any limitations;
 - d) particulars of the agency, establishment, facility or organisation to be visited;
 - e) whether the visit is sponsored by a Party or a Contractor or potential Contractor and whether the visit is being initiated by the requesting agency, or by the establishment, facility or organisation to be visited;
 - f) purpose of the requested visit;
 - g) anticipated highest level of Classified Information to be involved;
 - h) proposed date and duration of the requested visit and whether the request is for an intermittent recurring visit approval. In case of recurring visits the total period covered by the visits should be stated; and
 - i) identification and telephone number of a government official of the visiting Party who can provide additional information concerning the visit; the point of contact at the establishment/facility to be visited; previous contacts; and any other information useful to determine the justification of the visit or visits.

6. The validity of visit authorisation including for intermittent recurring visits to a specified establishment shall not exceed twelve months. When it is expected that a particular visit shall not be completed within the approved period, or that an extension of the period for intermittent recurring visits is required, the visiting Party shall submit a new request for visit approval at least twenty (20) working days prior to the lapse of the current visit approval.

7. The National Security Authority of the host Party shall inform the security officials of the agency, establishment, facility or organisation to be visited, of the details of those individuals whose visit request has been approved. Once approval has been given, visit arrangements for individuals who have been given approval for an intermittent recurring visit may be made directly with the agency, establishment, facility or organisation concerned.

8. All visitors shall comply with the national security laws and regulations on the protection of Classified Information and the relevant establishment instructions of the host Party.

9. Each Party shall guarantee the protection of personal data of the visitors according to their respective national laws and regulations.

ANNEX B
INDUSTRIAL OPERATIONS

1. INTRODUCTION

1.1. The additional provisions set out in this Annex relate to industrial operations and shall be applied in respect of:

- a) the administration of Classified Contracts and Pre-contractual Arrangements of one Party which are to be performed in the country of the other Party;
- b) the protection of Classified Information transferred between the Parties in the context of industrial operations; and
- c) the protection of Classified Information generated pursuant to Classified Contracts or Pre-contractual Arrangements.

1.2. Any Sub-Contractor must fulfil the same security obligations as the Contractor.

2. ADMINISTRATION OF CLASSIFIED CONTRACTS AND PRE-CONTRACTUAL ARRANGEMENTS

2.1. The National Security Authorities shall be responsible for the:

- a) administration of the security aspects of Classified Contracts and Pre-contractual Arrangements being performed within their respective countries; and
- b) implementation of security standards, practices and procedures for the protection of Classified Information transferred between the Parties pursuant to Classified Contracts or Pre-contractual Arrangements.

2.2. The National Security Authorities shall ensure that Contractors and potential Contractors are aware of the following provisions and obligations at a minimum:

- a) the definition of the term “Classified Information” and of the equivalent levels of security classification of the two Parties in accordance with the provisions of this Agreement;
- b) the names of the Government authority of each Party responsible for obtaining release approval and for the safeguarding of Classified Information related to the Classified Contract or Pre-contractual Arrangement;
- c) the channels to be used for the transfer of the Classified Information between the Government authorities and/or Contractors and potential Contractors involved;
- d) the procedures and mechanisms for communicating any changes that may arise in respect of Classified Information either because of changes in its national security classification or because protection is no longer necessary;

- e) the procedures for the approval of visits and access by personnel of one Party to entities of the other Party, within the framework of the Classified Contract;
- f) an obligation that the Contractor or potential Contractor shall disclose the Classified Information only to a person who is a citizen of either of the Parties, has been granted a Personnel Security Clearance, who has a Need-to-Know, and is employed on, or engaged in the performance of the Classified Contract; and
- g) an obligation that the Contractor or potential Contractor shall immediately notify his or her National Security Authority of any actual or suspected breach of security.

3. TRANSMISSION OF CLASSIFIED INFORMATION

All Classified Information provided in the context of Classified Contracts or Pre-contractual Arrangements shall be transferred in accordance with Article 9 of this Agreement.

4. USE OF CLASSIFIED INFORMATION IN CONTRACTS

4.1. Where the Parties mutually agree the Recipient Party may give access to Transferred Classified Information provided by the Originating Party for the purpose of passing it to a Contractor or potential Contractor within its country who has a Personnel Security Clearance to the appropriate level and may authorise such Contractor or potential Contractor to give access to other Contractors or potential Contractors who have a Personnel Security Clearance to the appropriate level and who are located in the country of either Party subject to the following:

- a) any restrictions specified by the Originating Party in relation to access to or use or disclosure of the Transferred Classified Information;
- b) any necessary restrictions arising as a result of the purpose for which Transferred Classified Information was provided;
- c) any provisions of this Agreement which restrict access to Transferred Classified Information by Third Parties; and
- d) the access to the Transferred Classified Information is essential to the performance of a Classified Contract or Pre-contractual Arrangement.

4.2. The National Security Authority of the Party intending to give such access to Transferred Classified Information to a Contractor or potential Contractor in its own country shall ensure, prior to providing such access, that the Contractor or potential Contractor has Facility Security Clearance to store and protect the information in accordance with the security procedures of the Recipient Party.

4.3. The Originating Party shall notify the Recipient Party about any change in the security classification of the information it has provided.

5. ACCESS TO CLASSIFIED INFORMATION BY CONTRACTORS

5.1. The National Security Authorities of the Parties shall ensure that security practices and procedures are in place so that access to, or custody of, Transferred Classified Information provided to Contractors or potential Contractors shall be limited to those individuals who have a Need-to-Know, and who require such access for the performance of a Classified Contract or Pre-contractual Arrangements, where those individuals:

- a) are citizens of the country of either of the Parties, unless the Originating Party has given its prior written approval that nationals of a third country may have such access;
- b) have been given a Personnel Security Clearance to the appropriate level in accordance with the Recipient Party's national laws, security regulations and procedures; and
- c) have been furnished with instructions setting out their responsibility to protect the Classified Information in accordance with applicable security procedures prior to such access being granted.

6. RESTRICTIONS ON THIRD PARTY ACCESS TO TRANSFERRED CLASSIFIED INFORMATION

6.1. A Contractor or potential Contractor which is determined by the National Security Authority of the country in which it is located to be under financial, administrative, policy or management control of a Third Party, may participate in Classified Contracts or Pre-contractual Arrangements requiring access to Classified Information provided by the other Party only when enforceable measures are in effect to ensure that those Third Parties shall not have access to the Classified Information provided or to Classified Information generated therefrom. If enforceable measures are not in effect to preclude access by Third Parties, or where access by such Third Parties is necessary for the performance of the Classified Contract or Pre-contractual Arrangement, the consent, in writing, of the Originating Party shall be obtained prior to permitting such access.

6.2. The negotiation or placing in a third country (by either a Party, or a Contractor located in the country of that Party) of a contract requiring access to Transferred Classified Information requires the prior written approval of the Originating Party. Such approval may be given subject to conditions for the protection of the Transferred Classified Information.

7. SECURITY CLASSIFICATION GUIDANCE

7.1. Every Classified Contract or Pre-contractual Arrangement concluded between entities of the Parties under the provisions of this Agreement shall include an appropriate security section with the security requirements and the classification of each aspect/element of the Classified Contract or Pre-contractual Arrangement.

7.2. The Parties or their Contractors negotiating or awarding a Classified Contract which is to be performed in the country of the other Party, shall furnish, through its National Security Authority to the National Security Authority of the other Party, a copy of a document providing security classification guidance for Classified Information related to a specific Classified Contract. In cases of doubt, the Contractor should refer back to the Originating Party. In Spain this document is called a Classification Guide. In Australia this document is called a Security Classification Grading Document (SCGD). Each Party shall monitor Classified Contracts and Pre-contractual Arrangements between that Party and its Contractors or potential Contractors to ensure compliance with the Classification Guide or SCGD as appropriate.

8. SECURITY REQUIREMENTS CLAUSE

8.1. The Parties, or Contractors acting on behalf of a Party, negotiating a Classified Contract which is to be performed in the country of the other Party shall incorporate appropriate security provisions to give effect to this Agreement in the Classified Contract and Pre-contractual Arrangements involving access to Classified Information.

8.2. At a minimum, a copy of the security section of any Classified Contract shall be forwarded to the National Security Authority of the Party where the work is to be performed, to allow adequate security monitoring.

9. SECURITY ASSURANCES

9.1. In accordance with its national laws, security regulations and procedures the National Security Authority of each Party shall, when requested by the National Security Authority of the other Party for defence purposes, ascertain the security status of a Contractor or individual and furnish a written assurance to the other Party concerning:

- a) the Facility Security Clearance status of the Contractor or potential Contractor including details regarding the capability to store and safeguard Classified Information; or
- b) the Personnel Security Clearance of the individual.

9.2. A favourable determination in either instance is referred to as a “security assurance”. If a written security assurance cannot be furnished promptly, the requesting Party shall be informed by the other Party of the action being taken to process the request.

9.3. Each Party shall promptly notify the other Party of any adverse information about an organisation, individual or other entity in respect of whom a security assurance has been provided pursuant to this Agreement.

9.4. If a security assurance is unable to be given due to an organisation, individual or other entity not having a security clearance to the appropriate level, the National Security Authority of a Party, when requested by the National Security Authority of the other Party to do so, shall conduct the necessary investigation and security evaluation to grant or upgrade the security clearance as required, and shall provide a written security assurance if a security clearance is granted or upgraded.

10. VISITS

10.1. Representatives of the National Security Authorities may periodically visit each other in order to analyse the efficiency of the measures adopted by a Contractor or potential Contractor for the protection of Classified Information involved in a Classified Contract or Pre-contract Arrangement. In this case, the date of the visit will be agreed between the National Security Authorities, giving notice of this fact thirty (30) days in advance.

10.2. Visits by Contractors or potential Contractors requiring access to Transferred Classified Information shall be in accordance with Annex A to this Agreement.

11. COMPLETION OF CLASSIFIED CONTRACTS

Upon completion of a Classified Contract, or other event where retention of the Transferred Classified Information is no longer required, all Classified Information furnished or generated pursuant to a Classified Contract or Pre-contractual Arrangement shall be returned to the Originating Party or destroyed in accordance with the Recipient Party's national security laws and regulations.