AGREEMENT BETWEEN

THE GOVERNMENT OF AUSTRALIA

AND

THE GOVERNMENT OF THE FRENCH REPUBLIC

REGARDING THE EXCHANGE AND RECIPROCAL PROTECTION OF

CLASSIFIED INFORMATION

The Government of Australia and the Government of the French Republic (hereinafter referred to as “the Parties” and separately as “a Party”);

DESIRING to ensure the protection of Classified Information;

Have agreed as follows:

ARTICLE 1
Purpose

The Parties shall, in accordance with their respective Laws and Policies, ensure the protection of Classified Information exchanged between them or between the Parties and their Contractors.

ARTICLE 2
Definitions

For the purposes of this Agreement:

2.1 **"Classified Information"** means any information (namely, knowledge that can be communicated) or material, regardless of the form, determined to require protection against unauthorised disclosure or compromise which has been so designated with a Security Classification.

2.2 **"Laws and Policies"** means any law or legislative instrument enacted in accordance with the respective constitutional arrangements of a Party, or any policies set out in official instructions as established by a Party.

2.3 **"Contractor"** means any individual or legal entity (other than those engaged by a Party under a contract of employment) entering into or bound by a Classified Contract and includes sub-contractors.

2.4 **"Contract"** or **"Sub-contract"** means a legally enforceable agreement under the terms of which the parties to it enter into mutual obligations.

2.5 **"National Security Authority" (NSA)** means the national authority of a Party that is responsible for the general control and implementation of this Agreement

2.6 **"Competent Security Authority" (CSA)** means any designated security authority or any other competent entity authorised in accordance with the Laws and Policies of a Party and which is responsible for the implementation of this Agreement according to the fields concerned.

2.7 **"Recipient Party"** means the Party to which the Classified Information is transferred or provided

2.8 **"Originating Party"** means the Party which provides Classified Information, having assigned it a Security Classification.

2.9 **"Security Classification"** is the designation assigned to information or material by the Originating Party as provided under Article 5 to indicate the minimum level of protection that information or material must be afforded to safeguard it from unauthorised disclosure or compromise.

2.10 **"Need-to-Know"** means the principle that access to Classified Information should be limited to those who need to use such information in order to perform their official or contracted duties.

2.11 **"Areas and facilities"** means any site, location, facility or premises in which Classified Information is used or stored in the territory of a Party, including Contractor areas or facilities.

2.12 **"Third Party"** means any government, including legal entities, individuals or organisations under its jurisdiction, or an international organisation, not being a Party to this Agreement.

2.13 **"Personnel Security Clearance"** means a certification provided by a NSA or relevant CSA to an individual which indicates that individual is security cleared in accordance with the Laws and Policies of the certifying Party for access to Classified Information at specified security levels.

2.14 **"Information and Communications Technology"** means any electronic device or application used to develop, handle, transfer, process, store, transport, present or destroy information. This includes but is not limited to those relating to radio, television, cellular phones, computer and network hardware and software, satellite systems, as well as the various services and applications associated with them, including videoconferencing.

2.15 **"Classified Contract"** means a Contract or a Sub-contract, or pre-contractual negotiations, which contains, or the preparation and/or performance of which requires access to, Classified Information or the generation, use or transfer of Classified Information.

2.16 **"Host Party"** means the Party to whose territory a visit takes place.

2.17 **"Facility Security Clearance"** means a certification provided by a National Security Authority or relevant CSA which indicates that a facility is security cleared in accordance with the Laws and Policies of the certifying Party to a specified security level and also has safeguards in place to that specified security level to store and protect Classified Information.

2.18 **"Visiting Party"** means the Party sending personnel to visit the Host Party.

ARTICLE 3
Scope

This Agreement sets out the security policies and practices for the exchange between the Parties, or receipt by one Party from the other, of Classified Information and for the protection of such Classified Information. This Agreement also provides for visits between the Parties and measures applying to the protection of Classified Information in the course of commercial and industry engagements by the Parties in either of the two countries.

ARTICLE 4
Authorised Bodies

4.1 The NSA for each of the Parties is:

For the French Republic:
Le Secrétariat général de la défense et de la sécurité nationale (S.G.D.S.N.)

For Australia:
The Attorney-General's Department of the Commonwealth of Australia.

4.2 The Parties shall inform each other in writing through diplomatic channels of significant changes to their designated NSA which affects the implementation of this Agreement.

4.3 The Parties shall inform each other in writing of their relevant CSAs as appropriate.

ARTICLE 5
Security of Classified Information

5.1 The Recipient Party shall ensure that the Classified Information and anything incorporating Classified Information from the Originating Party is stamped, marked or otherwise designated with the name of the Originating Party.

5.2 The Recipient Party shall stamp, mark or otherwise designate Classified Information assigned a Security Classification with the corresponding Security Classification as provided in the table below:

FRANCE	**AUSTRALIA**
TRÈS SECRET DÉFENSE	TOP SECRET
SECRET DÉFENSE	SECRET See paragraph 5.3
CONFIDENTIEL DÉFENSE	CONFIDENTIAL
See Paragraph 5.4	PROTECTED

5.3 France shall handle and protect Australian Classified Information marked SECRET bearing the caveat "Handle as CONFIDENTIEL DÉFENSE" as CONFIDENTIEL DÉFENSE. Australia shall apply this caveat for Australian SECRET classified information in circumstances where it is practicable to do so. This shall be agreed either as part of a Program Security Instruction or in any other appropriate documentation approved by the NSAs or relevant CSAs of the Parties.

5.4 France shall handle and protect Australian Classified Information marked PROTECTED as CONFIDENTIEL DÉFENSE. Australia shall handle and protect French Classified Information marked CONFIDENTIEL DÉFENSE bearing the caveat "Handle as PROTECTED" as PROTECTED.

5.5 The Parties shall, where it is practicable to do so, protect sensitive information in accordance with their respective Laws and Policies.

5.6 The Recipient Party shall not downgrade or de-classify transferred or received Classified Information without the prior written consent of the Originating Party.

5.7 The Originating Party shall promptly notify the Recipient Party, in writing, of any change in the Security Classification of Classified Information, and the Recipient Party shall alter the Security Classification accordingly upon the Origination Party's notification.

5.8 If the Recipient Party generates any documents or material containing Classified Information of the Originating Party, the Recipient Party shall ensure that the documents or material are marked as containing Classified Information provided by the Originating Party and classified to at least the same level as that Classified Information.

5.9 When the Originating Party requires that access to Classified Information shall be limited to only persons having the nationality of one of the Parties, such information shall bear the additional caveat "FRANCE / AUSTRALIA EYES ONLY" and "SPECIAL FRANCE-AUSTRALIE".

ARTICLE 6
Protection and Use of Classified Information

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

(a) the Recipient Party shall provide Classified Information transferred or received from the Originating Party protection to a standard no less than that given to the Recipient Party's own national Classified Information of corresponding Security Classification as provided under Article 5;

(b) unless express written consent is given to the contrary, the Recipient Party shall not disclose or use, or permit the disclosure or use of, any Classified

Information communicated by the other Party except for the purposes and within any limitations stated by, or on behalf of, the Originating Party;

(c) access to Classified Information shall be strictly limited to those who have a Need-to-Know and hold an appropriate security clearance and who have been informed of their responsibilities for the protection of Classified Information prior to being granted access;

(d) the Parties shall ensure that any requirements arising from their Laws and Policies in relation to the security of areas and facilities under their jurisdiction are complied with, including by means of security inspection visits;

(e) subject to Article 6.2, the Recipient Party shall not disclose, release or provide access to Classified Information or anything incorporating Classified Information transferred under this Agreement to any Third Party without the prior written consent of the Originating Party;

(f) Classified Information jointly originated by the Parties shall be assigned a Security Classification that is mutually determined by the Parties. The applicable Security Classification markings for jointly originated Classified Information shall be applied in accordance with Article 5. Classified Information jointly originated by the Parties shall not be disclosed, released or provided by one Party to a Third Party without the prior written consent of the other Party; and

(g) the Parties shall maintain appropriate accountability and control procedures to manage the dissemination of, and access to, Classified Information exchanged or generated under this Agreement.

6.2 Within the scope of its Laws and Policies, the Recipient Party shall take all steps available to it to protect Classified Information from disclosure other than for the purpose for which it was provided. In the event of a request to declassify or disclose any Classified Information provided under this Agreement, the Recipient Party shall immediately notify the Originating Party in writing, and both Parties shall consult each other in writing before a disclosure decision is taken by the Recipient Party. The expectation is that, within the scope of the Recipient Party's Laws and Policies, no Classified Information shall be released in response to any request without the Originating Party's express written consent.

6.3 Subject to Article 6.4, when any Classified Information is no longer required for the purpose for which it was provided, the Recipient Party shall destroy the Classified Information in accordance with its Laws and Policies and shall notify the Originating Party of its destruction.

6.4 Subject to Article 6.5, Classified Information at the level TOP SECRET / TRÈS SECRET DÉFENSE shall not be destroyed. When no longer required by the Recipient Party it shall be returned to the Originating Party in accordance with this Agreement.

6.5 In an emergency situation, where Classified Information exchanged or generated in accordance with this Agreement may be at imminent risk of compromise, Parties shall use their best efforts to destroy the Classified Information immediately. The NSA of the Recipient Party shall immediately notify the NSA or relevant CSA of the Originating Party about the destruction of the Classified Information.

ARTICLE 7
Access to Classified Information

7.1 Access to Classified Information exchanged or created under this Agreement shall be limited to persons who have a Need-to-Know and who have been granted a security clearance at the relevant Security Classification level.

7.2 A Personnel Security Clearance issued by the NSA or a CSA of one Party shall be accepted by the other Party where access to Classified Information is required.

7.3 For Australian and French nationals residing in their own territory and requiring access to Classified Information of either Party, the responsibility for undertaking the Personnel Security Clearance process rests with their respective NSA or relevant CSA.

7.4 For Australian and French nationals residing on the territory of the other Party and requiring access to Classified Information the Personnel Security Clearance process may be undertaken by the NSA or relevant CSA of the country of residence, in consultation with the other Party.

7.5 Each Party shall, in accordance with its respective Laws and Policies, assist the other Party in obtaining relevant information for Personnel Security Clearances in relation to nationals of one Party who are, or were, legally resident or located in the territory of the other Party.

7.6 The NSA or relevant CSA of one Party shall inform the NSA or relevant CSA of the other Party of significant changes affecting the Personnel Security Clearances of individuals having access to Classified Information exchanged under this Agreement, particularly in the event of the withdrawal or the downgrading of a Personnel Security Clearance.

ARTICLE 8
Translation and Reproduction of Classified Information

8.1 The Recipient Party shall mark translations and reproductions made as per the Security Classification markings on the originals and give them the same protection.

8.2 The information classified TRÈS SECRET DÉFENSE shall not be translated or reproduced by the Australian Recipient Party. Additional original documents or translations may be provided upon written request made to the French Originating Party.

8.3 The translation and reproduction of Classified Information marked SECRET DÉFENSE shall be done only with the prior written consent of the French Originating Party.

8.4 The translation and reproduction of Classified Information marked TOP SECRET and SECRET shall be done only with the prior written consent of the Australian Originating Party.

8.5 Subject to Article 8.2, translations and reproductions shall be limited to the minimum required for an official purpose, and shall be made only by individuals with a Need-to-Know and who hold a Personnel Security Clearance level of the Classified Information being reproduced or translated.

ARTICLE 9
Transfer of Classified Information

9.1 Transfer of Classified Information under this Agreement shall be in accordance with the Laws and Policies of the Originating Party.

9.2 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 in cases of urgency, the NSAs and respective CSAs of the Parties may mutually approve other methods for transfer of Classified Information.

9.3 The Parties shall ensure that the transfer of Classified Information in a physical form complies with the following requirements:

(a) the Parties shall register Classified Information transferred between them and shall provide upon request an extract of the relevant register to the other Party;

(b) Classified Information shall be packed and sealed in accordance with the Laws and Policies of the Party transferring the Classified Information;

(c) the Party transferring the Classified Information shall be provided with a receipt by the other Party on every occasion; and

(d) where a courier is used, the courier must be issued a certificate granted by the Party transferring the Classified Information.

9.4 When transferring Classified Information by electronic means the Parties shall use a method of encryption accepted by the respective NSAs or relevant CSAs in accordance with the Parties' Laws and Policies.

9.5 The transfer of a significant amount of Classified Information under Articles 9.2 to 9.4 shall be organised between the Parties' respective NSAs or relevant CSAs on a case-by-case basis.

ARTICLE 10
Information and Communications Technology

Information and Communications Technology networks, systems and infrastructure used for handling Classified Information in connection with this Agreement shall be protected in accordance with methods and standards mutually recognised and agreed upon by the NSAs or relevant CSAs of the Parties.

ARTICLE 11
Exchange of Security Standards and Cooperation

11.1 In order to maintain equivalent security standards, each Party shall provide the other Party with information about its security standards and its Laws and Policies for the protection of Classified Information. Each Party shall also inform the other Party in writing of any significant changes that affect the way in which Classified Information transferred or received from the other Party is protected. Each Party shall facilitate contacts between their respective NSAs and CSAs.

11.2 The principles for security cooperation between the Parties are detailed in Annex A.

ARTICLE 12
Classified Contracts

12.1 A Party intending to enter into, or authorise a Contractor in its territory to enter into, a Classified Contract with a Contractor in the territory of the other Party shall obtain written:

(a) confirmation of the security clearance status of the Contractor, and of the Contractor's personnel who are likely to require access to Classified Information provided to the Contractor in the performance of the Classified Contract; and

(b) information on whether the Contractor is owned or controlled by a Third Party;

in accordance with the principles for security cooperation at Annex A.

12.2 The NSA and relevant CSAs of the Party in which territory the Contractor is located shall be responsible for the administration of the security requirements

performed under Classified Contracts and ensuring the security conduct of Contractors within its territory.

12.3 Classified Contracts entered into following receipt of the written confirmation provided for in this Article shall contain security requirements incorporating at least the provisions as outlined in Annex B to this Agreement.

12.4 For Classified Contracts involving jointly originated Classified Information the NSAs or relevant CSAs may consult each other and shall mutually agree the provisions of the security requirements clause to be included in the Classified Contract.

12.5 Where a Classified Contract is performed, either in full or in part, in the territory of the other Party, the NSA or relevant CSA of the contracting Party shall provide a copy of the relevant parts of the Classified Contract to the other Party's NSA or relevant CSA, to allow adequate security monitoring.

12.6 The Party who has entered into the Classified Contract with a Contractor shall ensure that the Contractor:

(a) obtains approval from its NSA or relevant CSA prior to executing a Classified Contract with a sub-contractor, and provides that sub-contractor with the relevant security requirements clause; and

(b) requires a sub-contractor to comply with the same security conditions as a Contractor as set out in this Agreement.

12.7 The Parties shall not disclose or release or provide access to Classified Information to any Contractor unless such disclosure, release or access is in accordance and continuing compliance with the provisions of this Agreement.

ARTICLE 13
Compliance and Security Inspections

13.1 Each Party shall ensure that areas and facilities, Contractors and other organisations within its territory that handle Classified Information exchanged or generated under this Agreement protect such Classified Information in accordance with the provisions of this Agreement.

13.2 Each Party shall ensure that, within its territory, security inspections are carried out as appropriate and that its Laws and Policies are complied with in order to protect Classified Information on an ongoing basis.

ARTICLE 14
General Principles of Visits

14.1 Visits by personnel of a Party requiring access to Classified Information held by the other Party, or access to areas and facilities of the other Party, shall be

undertaken only with the prior approval, in writing, of the NSA or relevant CSA of the Host Party.

14.2 Visits by a Third Party to areas and facilities where access to Classified Information exchanged or generated under this Agreement is directly possible, shall be subject to prior approval, in writing, from the NSAs or relevant CSAs of both Parties.

14.3 The procedure for requesting and approving such visits is outlined in Annex C to this Agreement.

ARTICLE 15
Security Inspection Visits

15.1 For the purposes of ensuring appropriate implementation of this Agreement, and in order to achieve and maintain comparable security standards and procedures for the protection of Classified Information, each Party may permit security inspection visits to areas and facilities within a Party's territory where Classified Information exchanged or generated under this Agreement is stored or accessed. Security inspection visits will occur when mutually convenient and in accordance with the visit procedures set out in Annex C to this Agreement.

15.2 Security inspection visits shall be subject to prior approval, in writing, by the NSA or relevant CSA of the Host Party.

15.3 Each Party shall assist the authorised security personnel of the other Party in the exercise of their functions under Article 15.1.

ARTICLE 16
Security Violations

16.1 Violations of the provisions on the protection and use of Classified Information described in this Agreement, in respect of which unauthorised disclosure, destruction, misappropriation, loss or access has occurred or is suspected, shall be notified to the other Party as soon as possible. The notice must contain sufficient details for the Party receiving the notice to assess fully the consequences of the suspected or actual violation, the circumstances of the violation and the outcomes of any investigation carried out.

16.2 In such a case, the NSA or relevant CSAs of the Party in whose jurisdiction the violation occurs shall carry out investigations and, where appropriate, institute disciplinary and/or legal proceedings in accordance with its Laws and Policies. The other Party may support or otherwise be involved in such investigations. The other Party shall also be informed of the outcome and measures adopted to prevent reoccurrence of the violation.

ARTICLE 17
Costs

The implementation of the provisions of this Agreement will not normally bear any specific cost.

ARTICLE 18
Dispute Settlement

Any dispute between the Parties in connection with the interpretation, implementation or application of this Agreement shall be settled exclusively by consultations between the Parties and shall not be referred to any national or international tribunal or third party for resolution.

ARTICLE 19
Miscellaneous

19.1 This Agreement shall supersede in its entirety the *Agreement between the Government of Australia and the Government of the French Republic relating to the exchange and communication of classified information* done in Paris on 15 July 1985. This Agreement shall also supersede in its entirety the *Arrangement between the Secretary of the Department of Defence of Australia and the Secretary General of National Defence of the French Republic relating to the exchange and communication of classified information* done in Paris on 15 July 1985.

19.2 As required, the NSAs or relevant CSAs of the Parties shall hold consultations on specific technical aspects relating to the implementation of this Agreement.

19.3 The NSAs or CSAs of the Parties may enter into instruments to support implementation of this Agreement.

19.4 Each Party shall promptly notify the other Party of any change in its Laws and Policies that is likely to have an effect on the protection and use of Classified Information under this Agreement. In this case, the Parties shall hold consultations in order to examine any possible changes to this Agreement. At all times, Classified Information shall continue to be protected in accordance with the terms of this Agreement.

19.5 Annexes to this Agreement form an integral part of this Agreement.

ARTICLE 20
Entry into Force, Amendment and Termination

20.1 Each Party shall notify the other Party of the completion of its internal procedures required to bring this Agreement into force. The Agreement shall enter into force on the date of the last note.

20.2 The terms of this Agreement may be amended by mutual agreement in writing by the Parties. These amendments shall enter into force in accordance with the terms set forth in Article 20.1, unless otherwise provided for by the Parties.

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

20.4 Notwithstanding termination, the responsibilities and obligations of the Parties in relation to the protection, disclosure and use of transferred, received or created Classified Information shall continue to apply, in accordance with the terms of this Agreement.

IN WITNESS WHEREOF, the representatives of both Parties, duly authorised by their respective governments, have signed this Agreement.

Done at …… on…….…… in two counterparts in French and English; both versions being equally authentic.

For the Government of Australia

For the Government of the French Republic

ANNEX A

PRINCIPLES FOR SECURITY COOPERATION

1. When the NSA or a relevant CSA of a Party requires confirmation of the Facility Security Clearance of a Contractor in the territory of the other Party, it shall submit a formal written request to the NSA or relevant CSA of that Party, providing at least:

   (a) the name and address of the Contractor;

   (b) the highest level of Security Classification of Classified Information to be provided to the Contractor; and

   (c) the reasons for the request.

2. When the NSA or relevant CSA of a Party requires confirmation of a Personnel Security Clearance of an individual residing in the territory of the other Party, it shall submit a formal written request to the NSA or relevant CSA of that Party, providing at least:

   (a) the name of the individual;

   (b) the date and place of birth;

   (c) the nationality of the individual;

   (d) the name of the organisation which employs the individual; and

   (e) the reasons for the request.

3. On receipt of a request as described in paragraphs 1 or 2 of this Annex, the NSA or relevant CSA shall provide a written confirmation to the other Party concerning:

   (a) the Facility Security Clearance status of the Contractor, and its capability to store and safeguard Classified Information;

   (b) the Personnel Security Clearance status of the individual, including the person's appropriate Security Classification level and date of expiry of the Personnel Security Clearance.

4. If a Facility Security Clearance or a Personnel Security Clearance confirmation cannot be provided promptly, the requesting Party shall be informed of the action being taken to process the request.

5. If the Contractor or individual does not currently hold a Facility Security Clearance or Personnel Security Clearance respectively, or the clearance is at a lower level than that required, the NSA or relevant CSA receiving the request shall inform the requesting NSA or CSA of that fact. If required in the original

request, the notification to the relevant NSA or CSA shall also state whether action is also being taken to issue a Facility Security Clearance or Personnel Security Clearance at the required level or to upgrade an existing Facility Security Clearance or Personnel Security Clearance to the required level.

6. The NSAs and CSAs shall assist each other in carrying out Facility Security Clearance or Personnel Security Clearance security investigations on request and in accordance with the Laws and Policies of the relevant Party.

7. If information comes to the attention of the NSA or CSA of either Party which raises doubt about the relevant Contractor's or individual's current security clearance status, the NSA or CSA of the other Party shall be promptly notified. The NSA or CSA which provided the Facility Security Clearance or Personnel Security Clearance confirmation shall conduct a review of the security clearances issued and shall notify the NSA or CSA of the other Party whether any change in respect of the Contractor's Facility Security Clearance or individual's Personnel Security Clearance status is proposed.

8. Where a Party has significant concerns regarding the status of a Facility Security Clearance or Personnel Security Clearance granted by the other Party's NSA or a CSA, that Party may request the NSA or relevant CSA to undertake a review of the Facility Security Clearance or Personnel Security Clearance. On completion of such review, the NSA or CSA shall notify the requesting NSA or CSA of the results of the review and, where appropriate, any subsequent action taken.

9. Where a NSA or CSA has deemed that a facility of a Contractor within its territory is not eligible for a Facility Security Clearance as the Contractor is under the ownership, control or influence of a Third Party whose aims are not compatible with the interests of that Party, the NSA or relevant CSA of the other Party shall be notified of this fact.

10. If a NSA or CSA withdraws or downgrades an existing Facility Security Clearance or Personnel Security Clearance issued to a Contractor or person for whom a confirmation has been provided, the NSA or relevant CSA of the other Party shall be notified in writing as soon as is practicable.

11. Where a Party intends to enter into a Classified Contract with a Contractor located in the territory of the other Party, the latter Party shall:

    (a) use its best endeavours to determine whether the Contractor is owned or controlled by a Third Party; and

    (b) provide the NSA or relevant CSA of the first Party with information relevant to the ownership or control of the Contractor as soon as reasonably practicable, to the extent that information is available.

12. Security cooperation between the Parties shall be to the extent permitted by the Laws and Policies of each Party.

ANNEX B

PERFORMANCE OF CLASSIFIED CONTRACTS

Classified Contracts entered into in accordance with Article 12 of this Agreement shall contain a security requirements clause incorporating at least the following provisions:

(a) the definition of the term "Classified Information" and of the comparable levels of Security Classifications of the two Parties in accordance with the provisions of this Agreement;

(b) a statement that Classified Information exchanged or generated pursuant to the Classified Contract shall be protected by the Contractor in accordance with the applicable Laws and Policies;

(c) the names of the NSA and/or relevant CSAs of each of the Parties authorised to release, oversee and co-ordinate the safeguarding of Classified Information related to the Classified Contract;

(d) the channels to be used for the transfer of the Classified Information between the NSA or relevant CSAs and Contractors involved;

(e) the procedures and mechanisms for communicating changes that may arise in respect of Classified Information either because of changes to its Security Classification or because protection is no longer necessary;

(f) the procedures for the approval of visits, or access associated with the Classified Contract by personnel of one Party to the other Party, which shall be in accordance with Article 14 of this Agreement and Article 15 of this Agreement in the case of security inspection visits;

(g) the methods and procedures to be used for the transfer of Classified Information, which shall be in accordance with Article 9 of this Agreement;

(h) the procedures for the translation and reproduction of Classified Information, which shall be in accordance with the requirements of Article 8 of this Agreement;

(i) the procedures for the destruction or return of Classified Information, which shall be in accordance with the requirements of Article 6 of this Agreement;

(j) the requirement that the Contractor shall disclose Classified Information only to a person who has a Need-to-Know, has been granted a Personnel Security Clearance to the Security Classification level required, has been briefed on their responsibilities and has been charged with, or contributes to, the performance of the Classified Contract;

(k) the requirement that, subject to the provisions specified in (j) above of this Annex, the Contractor shall not disclose, or permit the disclosure of, Classified

Information to any Third Party without the express approval, in writing, of the Originating Party;

(l) the requirement that the Contractor shall use the Classified Information solely for the purpose for which it has been provided, or as further expressly authorised in writing by the Originating Party; and

(m) the requirement that the Contractor shall immediately notify its NSA or relevant CSA of any actual or suspected unauthorised disclosure, destruction, misappropriation, loss or access of Classified Information exchanged or generated under the Classified Contract, and the obligation to take all reasonable steps to assist in mitigating the effect of such a security violation.

ANNEX C

VISIT PROCEDURES

1. Approval for visits which will include access to:

   (a) Classified Information held by the Host Party;

   (b) areas and facilities where access to such Classified Information is directly possible; or

   (c) areas and facilities where access is restricted to individuals who have been security cleared;

   shall be granted only to personnel who possess a valid Personnel Security Clearance to the appropriate level and have a Need-to-Know.

2. Where a visit involves access to Classified Information of the level TRÈS SECRET DÉFENSE / TOP SECRET, requests shall be sent in the case of visits to France through diplomatic channels to the NSA, and in the case of visits to Australia to the NSA or relevant CSA of the Host Party. Requests shall be sent at least three (3) weeks prior to the date requested for the visit.

3. Where a visit involves access to Classified Information of the level of SECRET DÉFENSE / SECRET or lower, requests shall be processed directly between NSAs or respective CSAs. Requests shall be sent at least three (3) weeks prior to the date requested for the visit.

4. In urgent cases, the Visiting Party shall submit a visit request at least five (5) working days or as soon as practicable prior to the date of the proposed visit.

5. The Visiting Party shall ensure that visit requests include:

   (a) the visitor's full name, date and place of birth, citizenship and passport number;

   (b) the name of the agency, 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, facility or organisation to be visited;

   (e) whether the visit is hosted by a Party or a Contractor or potential Contractor and whether the visit is being initiated by the requesting agency, or by the facility or organisation to be visited;

   (f) the purpose of the requested visit;

(g) the highest level of Classified Information expected to be involved; and

(h) the proposed date and duration of the requested visit and whether the request is for a recurring visit approval. In the case of recurring visits, the total period covered by the visits should be stated.

6. The validity of a visit authorisation including for recurring visits to a specified establishment shall not exceed twelve (12) months. When it is expected that a particular visit will not be completed within the approved period, or that an extension of the period for recurring visits will be required, the Visiting Party shall submit a new request for visit approval at least three (3) weeks prior to the expiration of the current visit authorisation period.

7. The NSA of the Host Party shall inform the security officials of the agency, 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 recurring visits may be made directly with the agency, facility or organisation concerned.

8. The Visiting Party shall ensure that its personnel, when in the Host Party's territory, comply with the Laws and Policies on the protection of Classified Information and instructions of the Host Party relevant to any area and facility being visited.

9. Each Party shall guarantee the protection of personal data of visitors according to its Laws and Policies.