

**No. 48440\***

---

**United Kingdom of Great Britain and Northern Ireland  
and  
Spain**

**General Security Agreement between the United Kingdom of Great Britain and Northern Ireland and the Kingdom of Spain concerning the protection of classified information exchanged between the two countries. Madrid, 26 February 2009**

**Entry into force:** *1 March 2011 by notification, in accordance with article 16*

**Authentic texts:** *English and Spanish*

**Registration with the Secretariat of the United Nations:** *United Kingdom of Great Britain and Northern Ireland, 18 March 2011*

*\*No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.*

---

**Royaume-Uni de Grande-Bretagne et d'Irlande du Nord  
et  
Espagne**

**Accord général de sécurité entre le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et le Royaume d'Espagne relatif à la protection des informations classifiées échangées entre les deux pays. Madrid, 26 février 2009**

**Entrée en vigueur :** *1er mars 2011 par notification, conformément à l'article 16*

**Textes authentiques :** *anglais et espagnol*

**Enregistrement auprès du Secrétariat des Nations Unies :** *Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, 18 mars 2011*

*\* Numéro de volume RTNU n'a pas encore été établie pour ce dossier. Les textes reproduits ci-dessous, s'ils sont disponibles, sont les textes authentiques de l'accord/pièce jointe d'action tel que soumises pour l'enregistrement et publication au Secrétariat. Pour référence, ils ont été présentés sous forme de la pagination consécutive. Les traductions, s'ils sont inclus, ne sont pas en form finale et sont fournies uniquement à titre d'information.*

[ ENGLISH TEXT – TEXTE ANGLAIS ]

I, THE UNDERSIGNED SECRETARY OF STATE, hereby certify that the attached text is a true and complete copy of the General Security Agreement between the United Kingdom of Great Britain and Northern Ireland and the Kingdom of Spain concerning the Protection of Classified Information Exchanged between the Two Countries, done at Madrid on 26 February 2009, that it includes all reservations or declarations or objections made by the Signatories or Parties thereto, and that it was concluded in the following languages: English and Spanish. I further certify that the additional copy of the General Security Agreement contained in the diskette is a true and complete copy of the General Security Agreement between the United Kingdom of Great Britain and Northern Ireland and the Kingdom of Spain concerning the Protection of Classified Information Exchanged between the Two Countries, done at Madrid on 26 February 2009.

I FURTHER CERTIFY THAT the General Security Agreement came into force on 1 March 2011 by the exchange of notes, in accordance with Article 16 of the Agreement, and that it was signed by Denise Holt on behalf of the United Kingdom of Great Britain and Northern Ireland and Alberto Saiz for the Kingdom of Spain.

Foreign and Commonwealth Office  
London

09 March 2011

For the Secretary of State

The Agreement was previously  
published as Spain No.1 (2010)  
Cm 7873



Treaty Series No. 8 (2011)

# General Security Agreement

between the United Kingdom of Great Britain and Northern Ireland and  
the Kingdom of Spain concerning the Protection of Classified  
Information Exchanged between the Two Countries

Madrid, 26 February 2009

[The Agreement entered into force on 1 March 2011]

*Presented to Parliament  
by the Secretary of State for Foreign and Commonwealth Affairs  
by Command of Her Majesty  
March 2011*

Cm 8040

£6.00

**GENERAL SECURITY AGREEMENT BETWEEN THE UNITED  
KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND THE  
KINGDOM OF SPAIN CONCERNING THE PROTECTION OF  
CLASSIFIED INFORMATION EXCHANGED BETWEEN THE TWO  
COUNTRIES**

The United Kingdom of Great Britain and Northern Ireland (hereinafter referred to as the UK) and The Kingdom of Spain (together hereinafter referred to as the Parties) have, in the interests of national security, established the following arrangements which are set out in this General Security Agreement (GSA), wishing to ensure the protection of Classified Information transferred between the two countries or to commercial and industrial organisations in either of the two countries.

This GSA incorporates the security provisions of Part 4 of the Framework Agreement, between the French Republic, the Federal Republic of Germany, the Italian Republic, the Kingdom of Spain, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland concerning measures to facilitate the restructuring and operation of the European Defence Industry<sup>1</sup>, signed at Farnborough on 27 July 2000, hereafter referred to as “the Framework Agreement”.

ARTICLE 1

**Applicability**

1. This GSA sets out procedures for the protection of Classified Information exchanged between the Parties and falling under the responsibility of the respective National Security Authorities (NSA’s)/Designated Security Authorities (DSA’s).
2. This GSA shall not cover the exchange of Nuclear, Biological or Chemical information related to equipment commonly referred to as Weapons of Mass Destruction (WMD).

ARTICLE 2

**Definitions**

The following terms are defined in the interests of clarity:

1. “Classified Information” means any information (namely, knowledge that can be communicated in any form) or Material determined to require protection against unauthorised disclosure which has been so designated by a security classification.

---

<sup>1</sup> Treaty Series No. 33 (2001) Cm 5185

2. “Material” means any item or substance from which information can be derived. This includes Documents, equipment, weapons or components.
3. “Document” means any recorded information regardless of physical form or characteristics, e.g. written or printed matter (inter alia, letter, drawing, plan), computer storage media (inter alia, fixed disc, diskette, chip, magnetic tape, CD), photograph and video recording, optical or electronic reproduction of them.
4. “Contractor” means an individual or legal entity possessing the legal capability to undertake contracts.
5. “Designated Security Authority (DSA)/Competent Security Authority (CSA)” means a Government Authority responsible for implementing the security requirements covered by this GSA.
6. “Contract” means an agreement between two or more parties creating and defining enforceable rights and obligations between them.
7. “Classified Contract” means a Contract which contains or involves Classified Information.
8. “National Security Authority (NSA)” means the ultimate Government Authority in the Parties responsible for the security of Classified Information covered by this GSA.
9. “Originating Party” means the Party originating the Classified Information as represented by the NSA.
10. “Recipient Party” means the Party to which the Classified Information is transmitted as represented by the NSA.
11. “Facility” means an installation, plant, factory, laboratory, office, university or other educational institution or commercial undertaking (including any associated warehouses, storage areas, utilities and components which when related by function and location, form an operating entity), and any government department, agency or establishment.
12. “Security Official” means an individual designated by a NSA/DSA to implement industrial security requirements at a government establishment or contractor’s premises.

ARTICLE 3

**Responsible National Security Authorities**

1. The National Security Authorities (NSA) responsible for security of Classified Information under this GSA in each country are:

FOR THE UNITED KINGDOM

Cabinet Office  
Security Policy Division  
26 Whitehall  
London SW1A 2WH  
United Kingdom

FOR THE KINGDOM OF SPAIN

Secretario de Estado, Director del Centro Nacional de Inteligencia  
National Security Office  
Avda. Padre Huidobro, s/n  
28023 Madrid  
España

2. For the purpose of implementing this GSA, the Parties shall inform each other of their respective DSAs or CSAs.

ARTICLE 4

**Security Classifications**

The security classifications and their equivalents in the two countries are:

<b>IN THE UK</b>	<b>IN SPAIN</b>
UK SECRET	RESERVADO
UK CONFIDENTIAL	CONFIDENCIAL
UK RESTRICTED	DIFUSIÓN LIMITADA

ARTICLE 5

**Restrictions on Use and Disclosure of Exchanged Classified Information**

1. Subject to the provisions of paragraph (2) of this Article, unless express written consent is given to the contrary, the Receiving Party shall not disclose or

use, or permit the disclosure or use of, any Classified Information except for the purposes and within any limitations stated by or on behalf of the Originating Party.

2. Within the scope of its national law, the Receiving Party shall take all steps reasonably available to it to keep Classified Information transmitted to it by the Originating Party free from disclosure under any legislative provision or other rule of law, unless the Originating Party consents to such disclosure. If there is any request to declassify or disclose any Classified Information transmitted under the provisions of this GSA, the Receiving Party shall immediately notify the Originating Party and both Parties shall consult each other before any decision is taken.

3. Subject to the provisions of paragraph (2) of this Article, the Recipient Party shall not release, disclose or permit the release or disclosure of the Classified Information transmitted under the provisions of this GSA to any Government official, contractor or national of a third country or to any international organisation without the prior written consent of the Originating Party.

4. Personal Security Clearances for nationals of the Parties residing and requiring access to Classified Information in their own country shall be undertaken by their NSA/DSA/CSA.

5. However, Personal Security Clearances for nationals of the Parties who are legally resident in the country of the other Party and apply for a job in that country shall be undertaken by the NSA/DSA/CSA of that country conducting overseas checks as appropriate, and notifying the country of origin.

6. A Personal Security Clearance issued by one NSA/DSA/CSA shall be accepted by the other NSAs/DSAs/CSAs of the Parties for employment involving access to Classified Information within a company in their country.

## ARTICLE 6

### **Protection of Classified Information**

1. Within the scope of their national laws, the Parties shall take all appropriate measures to ensure the security protection of Classified Information transmitted between them or transmitted to, held by, or generated by a Contractor or a Facility in connection with a Classified Contract placed by one Party within the territory or jurisdiction of the other Party.

2. The Originating Party shall ensure that the Recipient Party is informed of:

- a. the security classification of the information and any conditions of release or limitations on its use, and that such information is so marked.
- b. any subsequent change in security classification.

3. The Recipient Party shall:
  - a. in accordance with its national laws or regulations, afford any Classified Information received from the other Party a level of security protection that is afforded to its own Classified Information of an equivalent classification in accordance with Article 4 above.
  - b. ensure that Classified Information is marked with its own security classification in accordance with Article 4 above.
  - c. ensure that security classifications are not altered, except as authorised in writing by or on behalf of the Originating Party.
  
4. In order to achieve and maintain comparable standards of security, each NSA shall, on request, provide the other with information about its security standards, procedures and practices for safeguarding Classified Information, and shall for this purpose facilitate visits by the other NSA or DSA/CSA as appropriate.

#### ARTICLE 7

##### **Access to Classified Information**

1. Access to Classified Information at the UK CONFIDENTIAL /CONFIDENCIAL level and above shall be limited to those persons who have a "need to know" and have been security cleared by the Recipient Party NSA/DSA/CSA in accordance with their national laws or regulations, to the level appropriate to the classification of the information to be accessed.
  
2. Access to Classified Information at the UK CONFIDENTIAL /CONFIDENCIAL and UK SECRET/RESERVADO levels by a person holding the sole nationality of a Party to the Framework Agreement may be granted without prior authorisation of the Originating Party.
  
3. Access to Classified Information at the UK CONFIDENTIAL /CONFIDENCIAL and UK SECRET/RESERVADO levels by a person holding the dual nationality of both a Party and a European Union country may be granted without prior authorisation of the Originating Party.
  
4. Access to Classified Information at the UK CONFIDENTIAL /CONFIDENCIAL and UK SECRET/RESERVADO levels by a person not holding the nationality described in paragraphs 2 and 3 of this Article shall be subject to prior consultation with the Originating Party. The consultation process concerning such persons shall be as described in sub-paragraphs a-e below.



- a. the Parties shall notify and consult each other when there is a need to grant access to Classified Information related to a specific project/programme to non-Parties nationals.
  - b. the consultation process shall be initiated before the start or, as appropriate, in the course of a project/programme.
  - c. the information shall be limited to the nationality of the persons concerned.
  - d. a Party receiving such notification shall examine whether access to its Classified Information by non-Participant nationals is acceptable or not.
  - e. such consultations shall be given urgent consideration with the objective of reaching consensus. Where this is not possible the Originating Party decision shall be accepted.
5. Access to Classified Information at the UK RESTRICTED/DIFUSIÓN LIMITADA level shall be limited to those persons who have a "need to know". A Personal Security Clearance is not required.

## ARTICLE 8

### **Transmission of Classified Information**

1. Classified Information at the UK CONFIDENTIAL/CONFIDENCIAL and UK SECRET/RESERVADO levels shall normally be transmitted between the Parties through Government-to-Government diplomatic bag channels or through channels approved by the NSAs/DSAs of the Parties.
3. In cases of urgency, i.e. only when the use of Government-to-Government diplomatic bag channels cannot meet the requirements, Classified Information at the UK CONFIDENTIAL/CONFIDENCIAL level may be transmitted via private courier companies, provided that the following criteria are met:
  - a. the courier company is located within the territory of the Parties and has established a protective security programme for handling valuable items with a signature service, including a record of continuous accountability on custody through either a signature and tally record, or an electronic tracking/tracing system.
  - b. the courier company must obtain and provide to the sender proof of delivery on the signature and tally record, or it must obtain receipts against package numbers.

- c. the courier company must ensure that the consignment shall be delivered to the recipient prior to a specific time and date within a 24-hour period under regular circumstances.
- d. the courier company may charge a commissioner or sub-contractor. However, the responsibility for fulfilling the above requirements must remain with the courier company.

3. Classified Information at the UK RESTRICTED/DIFUSIÓN LIMITADA level shall be transmitted between the Parties in accordance with the national regulations of the Originating Party, which may include the use of private courier companies.

4. Classified Information at the UK CONFIDENTIAL/CONFIDENCIAL and UK SECRET/RESERVADO levels must not be transmitted electronically in clear text. Only cryptographic systems approved by the NSAs/DSAs concerned shall be used for the encryption of Classified Information at the UK CONFIDENTIAL/CONFIDENCIAL and UK SECRET/RESERVADO levels, irrespective of the method of transmission. Classified Information at the UK RESTRICTED/ DIFUSIÓN LIMITADA level may be transmitted or accessed electronically (e.g. by means of point-to-point computer links) via a public network like the Internet, only using government or commercial encryption devices mutually accepted by the competent national authorities. However, telephone conversations, video conferencing or facsimile transmissions containing Classified Information at the UK RESTRICTED/ DIFUSIÓN LIMITADA level may be in clear text, if an approved encryption system is not available.

5. Where large volumes of Classified Information are to be transmitted, the means of transport, the route and the escort (if any) shall be jointly determined on a case-by-case basis by the competent authorities of the Parties.

## ARTICLE 9

### Visits

1. Each Party, based on a mutual interest, shall permit visits involving access to Classified Information to its Facilities, by civilian or military representatives of the other Party or by their contractor employees, provided that the visitor has an appropriate Personal Security Clearance and a need-to-know.

2. All visiting personnel shall comply with the security regulations of the host Party. Any Classified Information disclosed or made available to visitors shall be treated as if supplied to the Party sponsoring the visiting personnel, and shall be protected accordingly.

3. For visits in the context of sharable Classified Information to Government establishments of the other Party or to Facilities of a Contractor where access to

Classified Information at the UK CONFIDENTIAL/CONFIDENCIAL and UK SECRET/RESERVADO levels is required, the following procedure shall apply:

1. Subject to the following provisions, such visits shall be arranged directly between the sending Facility and the Facility to be visited.
2. For these visits the following prerequisites must also be met:
  - a) The visit shall be for an official purpose.
  - b) Any Facility of a Contractor to be visited shall have the appropriate Facility Security Clearance.
  - c) Prior to arrival, confirmation of the visitor's Personal Security Clearance must be provided directly to the Facility to be visited by the security official of the sending Facility. To confirm identity the visitor must be in possession of an ID card or passport for presentation to the security authorities at the Facility to be visited.
4. It is the responsibility of the security officials of:
  - a. the sending Facility to ensure with their NSA/DSA/CSA that any company Facility to be visited is in possession of an appropriate Facility Security Clearance;
  - b. both the sending Facility and the Facility to be visited to agree that there is a need for the visit.
5. The Security Official of a company Facility to be visited or, where appropriate, a Government establishment must ensure that records are kept of all visitors, including their name, the organisation they represent, the date of expiry of the Personal Security Clearance, the date(s) of the visit(s) and the name(s) of the person(s) visited. Such records are to be retained according to national laws and regulations and, in any case, for a period of no less than two years.
6. The NSA/DSA/CSA of the host Party has the right to require prior notification from their Facilities to be visited for visits of more than 21 days' duration. This NSA/DSA/CSA may then grant approval, but should a security problem arise it shall consult with the NSA/DSA/CSA of the visitor.
7. For visits in the context of Classified Information to Government establishments of the other Party or to Facilities of a Contractor where access to Classified Information at the UK CONFIDENTIAL/CONFIDENCIAL and UK SECRET/RESERVADO levels is required, which has not been pre-determined as sharable, the normal international visit procedure shall be applied.

8. Visits relating to Classified Information at the UK RESTRICTED/DIFUSIÓN LIMITADA level shall also be arranged directly between the sending Facility and the Facility to be visited.

## ARTICLE 10

### **Contracts**

1. When proposing to place, or authorising a Contractor in its country to place, a Contract involving Classified Information at the UK CONFIDENTIAL /CONFIDENCIAL level or above with a Contractor in the other country the Originating Party shall obtain prior assurance from the NSA/DSA/CSA of the other country that the proposed Contractor is security cleared to the appropriate level and also has suitable security safeguards to provide adequate protection of Classified Information. The assurance shall carry a responsibility that the security conduct by the cleared Contractor shall be in accordance with national security laws or regulations and monitored by his NSA/DSA/CSA. This requirement does not apply where a Contract exclusively contains Classified Information at the UK RESTRICTED/ DIFUSIÓN LIMITADA level.

2. The NSA/DSA/CSA of the country placing the contract shall ensure that Contractors receiving Contracts placed as a consequence of these pre-contract enquiries are aware of the following provisions:

- a. The definition of the term "Classified Information" and of the equivalent levels of classification specified in this GSA.
- b. The names of the Government Authority of each of the two countries empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Contract.
- c. The channels to be used for the transfer of the Classified Information between the Government Authorities and/or Contractors involved.
- d. The procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its security classification or because protection is no longer necessary.
- e. The procedures for the approval of visits, access or inspection by personnel of one country to Facilities of the other country which are covered by the Contract.
- f. An obligation that the Contractor shall disclose the Classified Information only to persons who are appropriately security cleared for access, have a need to know, and are employed on, or engaged in the performance of the Contract.

- g. An obligation that the Contractor shall not disclose the Classified Information or permit it to be disclosed to any person not appropriately security cleared and expressly authorised to have such access.
  - h. An obligation that the Contractor shall immediately notify his NSA/DSA/CSA of any actual or suspected loss, leak or compromise of the Classified Information of this Contract.
3. The NSA/DSA/CSA of the Originating Party shall pass a copy of the relevant parts of the Classified Contract to the NSA/DSA/CSA of the Recipient Party, to allow adequate monitoring of the classified aspects of the Contract.
4. Each Classified Contract shall contain guidance on the security requirements and on the classification of each aspect/element of the Contract. In the UK the notification shall be contained in specific security clauses and in a Security Aspects Letter (SAL). In the Kingdom of Spain this notification shall be set out in the Contract. The notification must identify each classified aspect of the Contract, or any classified aspect which is to be generated by the Contract, and allocate to it a specific security classification. Changes in the requirements or to the aspects/elements shall be notified as and when necessary and the Originating Party shall notify the Recipient Party when all the information has been de-classified.

## ARTICLE 11

### **Security Assurances**

1. Each NSA/DSA/CSA shall provide details of the security status of a Facility in its country when requested by the other. Each NSA/DSA/CSA shall also provide details of the security clearance status of one of its nationals when so requested. These notifications shall be known as Facility Security Clearance (FSC) and Personal Security Clearance (PSC) assurance respectively.
2. When requested the NSA/DSA/CSA shall establish the security clearance status of the Facility/individual which/who is the subject of the enquiry and forward a security clearance assurance if the Facility/individual is already cleared. If the Facility/individual does not have a security clearance, or the clearance is at a lower level than that required, notification shall be sent that the security clearance assurance cannot be issued immediately. In such cases further steps shall be initiated to meet the requirement. Following successful enquiries a security clearance shall be provided.
3. If a Facility is deemed by the NSA/DSA/CSA, in the country in which it is registered, to be ineligible for a FSC assurance, the requesting NSA/DSA/CSA shall be notified.

4. If either NSA/DSA/CSA learns of any adverse information about an individual for whom a PSC assurance has been issued, it shall notify the other NSA/DSA/CSA of the nature of the information and the action it intends to take, or has taken. Either NSA/DSA/CSA may request a review of any PSC assurance which has been furnished previously by the other NSA/DSA/CSA provided that the request is accompanied by a reason. The requesting NSA/DSA/CSA shall be notified of the results of the review and any subsequent action.
5. If information becomes available which raises doubts about the suitability of a cleared Facility to continue to hold or retain Classified Information in the other country then details of this information shall be promptly notified to the NSA/DSA/CSA to allow an investigation to be carried out.
6. If either NSA/DSA/CSA suspends or takes action to revoke a PSC, or suspends or takes action to revoke access which is granted to a national of the other country based upon a PSC, the other Party shall be notified and given the reasons for such an action.
7. Each NSA/DSA/CSA may request the other to review any FSC assurance, provided that their request is accompanied by the reasons for seeking the review. Following the review, the requesting NSA/DSA/CSA shall be notified of the results and be provided with the facts supporting any decisions taken.
8. If required by the other Party each NSA/DSA/CSA shall co-operate in reviews and investigations concerning Personal and Facility Security Clearances.

## ARTICLE 12

### **Breach of Security**

1. In the event of a security infringement involving Classified Information provided by the other Party or suspicion that Classified Information has been disclosed to unauthorised persons, the NSA/DSA/CSA of the Recipient Party shall immediately inform the NSA/DSA/CSA of the Originating Party.
2. An immediate investigation shall be carried out by the Recipient Party, with assistance from the Originating Party if required, in accordance with the laws or regulations in force in the recipient's country for the protection of Classified Information. The Recipient Party shall inform the Originating Party about the circumstances, outcome of the investigation and the measures adopted to prevent a recurrence as soon as is practicable.

ARTICLE 13

**Costs**

Each Party shall bear its own costs incurred by the implementation and supervision of the measures and obligations expressed in this GSA.

ARTICLE 14

**Amendment**

The provisions of this GSA may be amended with the mutual consent in writing of both Parties. Such amendments shall become effective in accordance with the procedure set out in Article 17.

ARTICLE 15

**Disputes**

Any dispute regarding the interpretation or application of this GSA shall be resolved by consultation between the Parties.

ARTICLE 16

**Effective Date**

This GSA is subject to approval in accordance with the national legal procedures of each Party and shall become effective on the first day of the second month following the exchange of notifications between the Parties to the effect that the necessary requirements set by internal laws or regulations for this GSA to enter into operation have been met.

ARTICLE 17

**Termination/Review**

1. This GSA shall remain in operation for ten years or until terminated by either Party giving the other six months written notice of termination. In such case the validity of the GSA shall expire after 180 days following the day on which the notice of termination was served to the other Party. Both Parties shall remain responsible after termination for the safeguarding of all Classified Information exchanged under the provisions of this GSA.

2. Similarly, any Classified Information which is exchanged under the cover of this GSA shall also be safeguarded, even though its transfer may occur following notice by either of the Parties to terminate.

3. In the event of termination, solutions to any outstanding problems shall be sought by consultation between the two Parties.

Done in Madrid on the twenty sixth of February 2009 in two originals, each in the English and Spanish languages, both texts equally authentic.

**For the United Kingdom of  
Great Britain and  
Northern Ireland:**

**For the Kingdom of Spain:**

**DENISE HOLT**

**ALBERTO SAIZ**



[ SPANISH TEXT – TEXTE ESPAGNOL ]

**ACUERDO GENERAL DE SEGURIDAD**

**ENTRE**

**EL REINO DE ESPAÑA**

**Y**

**EL REINO UNIDO DE GRAN BRETAÑA**  
**E IRLANDA DEL NORTE**

**RELATIVO A LA PROTECCIÓN**

**DE LA INFORMACIÓN CLASIFICADA INTERCAMBIADA**

**ENTRE LOS DOS PAÍSES**

El Reino de España y el Reino Unido de Gran Bretaña e Irlanda del Norte (en lo sucesivo denominado RU, y, junto con el Reino de España, en lo sucesivo denominados las Partes), han establecido, en interés de la seguridad nacional, los siguientes acuerdos que se recogen en el presente Acuerdo General de Seguridad (AGS), movidos por el deseo de garantizar la protección de la información clasificada transmitida entre los dos países o a las organizaciones comerciales e industriales de cualquiera de los dos países.

El presente AGS incorpora las disposiciones sobre seguridad contenidas en la Parte 4 del Acuerdo Marco entre la República Federal de Alemania, el Reino de España, la República Francesa, la República Italiana, el Reino Unido de Gran Bretaña e Irlanda del Norte y el Reino de Suecia, relativo a las medidas encaminadas a facilitar la reestructuración y funcionamiento de la industria europea de defensa, firmado en Farnborough el 27 de julio de 2000, en adelante denominado “el Acuerdo Marco”.

## ARTÍCULO 1

### APLICABILIDAD

1. El presente AGS establece procedimientos para la protección de la información clasificada intercambiada entre las Partes y bajo la responsabilidad de las respectivas Autoridades Nacionales de Seguridad (ANS) / Autoridades Designadas de Seguridad (ADS).
2. El presente AGS no abarcará el intercambio de información nuclear, biológica o química relativa a equipos habitualmente conocidos como armas de destrucción masiva (ADM).

## ARTÍCULO 2

### DEFINICIONES

Los siguientes términos se definen en aras de la claridad:

1. Por “**información clasificada**” se entenderá cualquier información (a saber, conocimientos que puedan comunicarse de cualquier forma) o material respecto de los cuales se decida que requieren protección contra su divulgación no autorizada y a los que se ha asignado una clasificación de seguridad.
2. Por “**material**” se entenderá cualquier artículo o sustancia del que pueda obtenerse información. Este término incluye los documentos, equipos, armas y componentes.
3. Por “**documento**” se entenderá cualquier información registrada, con independencia de su forma o características físicas, por ejemplo, material escrito o impreso (entre otros, cartas, dibujos o planos), soportes informáticos (entre otros, disco fijo, disquete, chip, cinta magnética o CD), fotografía y las grabaciones en vídeo y su reproducción óptica o electrónica.

4. Por **“contratista”** se entenderá toda persona física o jurídica que tenga la capacidad jurídica necesaria para celebrar contratos.
5. Por **“autoridad designada de seguridad (ADS) / autoridad competente de seguridad (ACS)”** se entenderá la autoridad pública responsable de la aplicación de las estipulaciones en materia de seguridad a que se refiere el presente AGS.
6. Por **“contrato”** se entenderá un acuerdo entre dos o más partes por el que se crean y definen derechos y obligaciones exigibles entre ellas.
7. Por **“contrato clasificado”** se entenderá un contrato que contenga o se refiera a información clasificada.
8. Por **“autoridad nacional de seguridad (ANS)”** se entenderá la autoridad pública de las Partes responsable en última instancia de la seguridad de la información clasificada a que se refiere el presente AGS.
9. Por **“Parte remitente”** se entenderá la Parte de la que proceda la información clasificada, representada por su ANS.
10. Por **“Parte receptora”** se entenderá la Parte a la que se transmita la información clasificada, representada por su ANS.
11. Por **“establecimiento”** se entenderá cualquier instalación, planta, fábrica, laboratorio, oficina, universidad u otra institución docente o empresa comercial (incluido cualquier almacén, zonas de almacenamiento, servicios y componentes asociados que formen una entidad operativa cuando estén relacionados por su función y ubicación), y cualquier departamento, organismo o centro público.
12. Por **“oficial de seguridad”** se entenderá la persona designada por una ANS/ADS para aplicar las exigencias de seguridad industrial en un centro público o en los locales de un contratista.

### **ARTÍCULO 3**

#### **AUTORIDADES NACIONALES DE SEGURIDAD RESPONSABLES**

1. Las autoridades nacionales de seguridad (ANS) responsables de la seguridad de la información clasificada en virtud del presente AGS serán:

**EN ESPAÑA**

Secretario de Estado, Director del Centro Nacional de Inteligencia  
Oficina Nacional de Seguridad  
Avda. Padre Huidobro s/n  
28023 MADRID  
España

**EN EL REINO UNIDO**

Cabinet Office  
Security Policy Division  
26 Whitehall  
London SW1A 2WH  
United Kingdom

2. A efectos de la aplicación del presente AGS, las Partes se comunicarán recíprocamente sus ADS o ACS respectivas.

**ARTÍCULO 4**

**CLASIFICACIONES DE SEGURIDAD**

Las clasificaciones de seguridad y sus equivalencias en los dos países son:

<b>EN ESPAÑA</b>	<b>EN REINO UNIDO</b>
RESERVADO	UK SECRET
CONFIDENCIAL	UK CONFIDENTIAL
DIFUSIÓN LIMITADA	UK RESTRICTED

**ARTÍCULO 5**

**RESTRICCIONES DE USO Y DIVULGACIÓN DE LA INFORMACIÓN  
CLASIFICADA INTERCAMBIADA**

1. Con sujeción a las disposiciones del apartado 2 del presente artículo, y salvo que se dé consentimiento expreso por escrito en contrario, la Parte receptora no divulgará ni utilizará la información clasificada, ni permitirá su divulgación o utilización por un tercero, excepto para los fines y dentro de los límites indicados por la Parte remitente o en su nombre.
2. Dentro del marco de su legislación nacional, la Parte receptora adoptará todas las medidas de que razonablemente disponga para impedir que la información clasificada que le

transmita la Parte remitente sea divulgada al amparo de cualquier disposición legislativa u otra norma legal, salvo si la Parte remitente consiente en dicha divulgación. En caso de que se solicite la desclasificación o divulgación de cualquier información clasificada transmitida según lo dispuesto en el presente AGS, la Parte receptora lo notificará inmediatamente a la Parte remitente y ambas Partes se consultarán mutuamente antes de adoptar una decisión.

3. Con sujeción a las disposiciones del apartado 2 del presente artículo, la Parte receptora no cederá, divulgará ni permitirá la cesión ni la divulgación de la información clasificada transmitida con arreglo a lo dispuesto en el presente AGS a ningún funcionario público, contratista o nacional de un tercer país, ni a ninguna organización internacional, sin el consentimiento previo por escrito de la Parte remitente.

4. Las Habilitaciones Personales de Seguridad para los nacionales de las Partes que residan en su propio país y que requieran el acceso a información clasificada en el mismo serán tramitadas por su ANS/ADS/ACS.

5. No obstante, las Habilitaciones Personales de Seguridad para los nacionales de las Partes que residan legalmente en el país de la otra Parte y soliciten un trabajo en ese país serán tramitadas por la ANS/ADS/ACS de ese país, que realizará las comprobaciones en el extranjero que sean necesarias y lo notificará al país de origen.

6. Una Habilitación Personal de Seguridad expedida por una ANS/ADS/ACS será aceptada por las demás ANS/ADS/ACS de las Partes para un puesto de trabajo que conlleve el acceso a información clasificada en una empresa de sus respectivos países.

## **ARTÍCULO 6**

### **PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA**

1. Dentro del marco de sus legislaciones nacionales, las Partes adoptarán todas las medidas apropiadas para garantizar la protección de la seguridad de la información clasificada transmitida entre ellas o transmitida, poseída o generada por un contratista o un establecimiento en relación con un contrato clasificado adjudicado por una Parte en el territorio o jurisdicción de la otra Parte.

2. La Parte remitente se asegurará de informar a la Parte receptora de:

- a. la clasificación de seguridad de la información y cualesquiera condiciones para su cesión o limitaciones en cuanto a su uso, y de que los documentos lleven la indicación correspondiente;
- b. cualquier cambio posterior de la clasificación de seguridad.

3. La Parte receptora:

- a. de conformidad con sus leyes y reglamentos nacionales, dará a la información clasificada recibida de la otra Parte el mismo nivel de protección de la seguridad que otorgue a su propia información de clasificación equivalente, según lo dispuesto en el anterior artículo 4;
  - b. se asegurará de que la información clasificada lleve indicada su propia clasificación de seguridad, según lo dispuesto en el anterior artículo 4;
  - c. se asegurará de que no se modifican las clasificaciones de seguridad, salvo autorización por escrito de la Parte remitente o en su nombre.
4. Con objeto de alcanzar y mantener criterios comparables de seguridad, cada ANS facilitará a la otra, previa petición, información sobre sus criterios de seguridad y sus procedimientos y prácticas para custodiar la información clasificada, y facilitará a tal fin las visitas de la ANS o ADS/ACS de la otra Parte, según proceda.

## **ARTÍCULO 7**

### **ACCESO A LA INFORMACIÓN CLASIFICADA**

1. El acceso a la información clasificada de nivel CONFIDENCIAL/UK CONFIDENCIAL o superior se limitará a las personas que tengan “necesidad de conocer” y que posean una habilitación de seguridad expedida por la ANS/ADS/ACS de la Parte receptora, de conformidad con sus leyes y reglamentos nacionales, correspondiente al nivel de clasificación de la información a la que se vaya a tener acceso.
2. El acceso a información clasificada de niveles CONFIDENCIAL/UK CONFIDENCIAL y RESERVADO/UK SECRET por una persona que posea como única nacionalidad la de una de las Partes en el Acuerdo Marco podrá concederse sin necesidad de autorización previa de la Parte remitente.
3. El acceso a información clasificada de niveles CONFIDENCIAL/UK CONFIDENCIAL y RESERVADO/UK SECRET por una persona que posea doble nacionalidad, la de una de las Partes y la de otro país de la Unión Europea, podrá concederse sin necesidad de autorización previa de la Parte remitente.
4. El acceso a información clasificada de niveles CONFIDENCIAL/UK CONFIDENCIAL y RESERVADO/UK SECRET por una persona que no cumpla los requisitos de nacionalidad indicados en los apartados 2 y 3 del presente artículo estará sujeto a consulta previa con la Parte remitente. El proceso de consulta respecto de dichas personas será el expuesto en las siguientes letras a) a e).
  - a. las Partes se notificarán y consultarán recíprocamente cuando surja la

necesidad de conceder a nacionales de países que no sean Partes el acceso a información clasificada relacionada con un proyecto/programa concreto;

- b. el proceso de consulta se iniciará antes del comienzo o, según proceda, en el curso de un proyecto/programa;
- c. la información se limitará a la nacionalidad de las personas interesadas;
- d. la Parte que reciba esa notificación examinará si es aceptable o no el acceso a su información clasificada por nacionales de países no participantes;
- e. a estas consultas se les dará tratamiento de urgencia con objeto de alcanzar un consenso. Cuando éste no sea posible, se aceptará la decisión de la Parte remitente.

5. El acceso a información clasificada de niveles DIFUSIÓN LIMITADA/UK RESTRICTED estará limitado a las personas que tengan “necesidad de conocer”. No se requerirá Habilitación Personal de Seguridad.

## **ARTÍCULO 8**

### **TRANSMISIÓN DE INFORMACIÓN CLASIFICADA**

1. La información clasificada de los niveles CONFIDENCIAL/ UK CONFIDENTIAL y RESERVADO/UK SECRET se transmitirán normalmente entre las Partes por valija diplomática de Gobierno a Gobierno, o por otros conductos aprobados por las ANS/ADS de las Partes.

2. En casos urgentes, es decir, únicamente cuando la utilización de la valija diplomática de Gobierno a Gobierno no cumpla los requisitos, la información clasificada de nivel CONFIDENCIAL/UK CONFIDENTIAL podrá transmitirse a través de empresas privadas de mensajería, siempre que se cumplan las siguientes condiciones:

- a. que la empresa de mensajería esté localizada en el territorio de las Partes y haya establecido un programa protector de seguridad para manejar objetos de valor con un servicio de firmas, incluido un registro de responsabilidad continuada sobre la custodia mediante un registro de firma y recuento o mediante un sistema de seguimiento/rastreo electrónico;
- b. que la empresa de mensajería obtenga y proporcione al remitente la prueba de la entrega en el registro de firma y recuento, o bien obtenga recibos contra los números de paquetes;

- c. que la empresa de mensajería garantice que el envío se entregará al destinatario antes de una hora y fecha determinadas, dentro de un plazo de 24 horas en circunstancias normales;
- d. que la empresa de mensajería pueda recurrir a un comisionista o subcontratista. No obstante, la responsabilidad de cumplir los anteriores requisitos seguirá siendo de la empresa de mensajería.

3. La información clasificada de nivel DIFUSIÓN LIMITADA/UK RESTRICTED se transmitirá entre las Partes de conformidad con las normas nacionales de la Parte remitente, que pueden incluir la utilización de empresas privadas de mensajería.

4. La información clasificada de niveles CONFIDENCIAL/UK CONFIDENTIAL y RESERVADO/UK SECRET no podrá transmitirse electrónicamente en texto claro. Para el cifrado de información clasificada de niveles CONFIDENCIAL/UK CONFIDENTIAL o RESERVADO/UK SECRET únicamente se usarán los sistemas de cifra aprobados por las ANS/ADS interesadas, independientemente del método de transmisión. La información clasificada de nivel DIFUSIÓN LIMITADA/UK RESTRICTED podrá transmitirse electrónicamente o podrá tenerse acceso a ella electrónicamente (por ejemplo, por medio de enlaces informáticos punto a punto) a través de una red pública como Internet, únicamente utilizando dispositivos estatales o comerciales de cifrado mutuamente aceptados por las autoridades nacionales competentes. No obstante, podrán hacerse en texto claro las conversaciones telefónicas, videoconferencias o transmisiones por fax que contengan información clasificada de nivel DIFUSIÓN LIMITADA/UK RESTRICTED si no se dispone de un sistema de cifra aprobado.

5. Cuando deba transmitirse un gran volumen de información clasificada, las autoridades competentes de las Partes determinarán conjuntamente caso por caso el medio de transporte, el itinerario y la escolta (en su caso).

## **ARTÍCULO 9**

### **VISITAS**

1. Cada Parte permitirá, con un criterio de interés mutuo, las visitas a sus establecimientos que impliquen acceso a información clasificada por representantes civiles o militares de la otra Parte o por empleados de sus contratistas, siempre que el visitante tenga una Habilitación Personal de Seguridad adecuada y la necesidad de conocer.
2. Todo el personal visitante cumplirá las normas de seguridad de la Parte anfitriona. Se tratará toda la información clasificada divulgada a los visitantes o puesta a su disposición como si hubiera sido proporcionada a la Parte que patrocine al personal visitante, y será protegida en consonancia.
3. Para las visitas relacionadas con información clasificada susceptible de ser compartida a centros públicos de la otra Parte o a establecimientos de un contratista en las que se necesite



tener acceso a información clasificada de niveles CONFIDENCIAL/UK CONFIDENTIAL y RESERVADO/UK SECRET, se seguirá el siguiente procedimiento:

1. Con sujeción a las disposiciones siguientes, estas visitas serán preparadas directamente entre el establecimiento de origen y el establecimiento objeto de la visita.
2. Estas visitas estarán sujetas también a las siguientes condiciones:
  - a. que la visita tenga una finalidad oficial;
  - b. que el establecimiento de un contratista que vaya a visitarse tenga la Habilitación de Seguridad para Establecimientos apropiada;
  - c. antes de la llegada, el oficial de seguridad del establecimiento de origen deberá proporcionar directamente al establecimiento objeto de la visita la confirmación de la Habilitación Personal de Seguridad del visitante. Para confirmar su identidad, el visitante deberá estar en posesión de una tarjeta de identidad o pasaporte para su presentación a las autoridades de seguridad del establecimiento objeto de la visita.
4. Será responsabilidad de los oficiales de seguridad:
  - a. del establecimiento de origen, asegurarse con su ANS/ADS/ACS de que cualquier establecimiento empresarial que vaya a visitarse esté en posesión de una Habilitación de Seguridad para Establecimientos adecuada,
  - b. del establecimiento de origen y del establecimiento objeto de la visita, ponerse de acuerdo en que existe la necesidad de la visita.
5. El oficial de seguridad del establecimiento empresarial que vaya a ser visitado o, en su caso, del centro público deberá asegurarse de que se llevan registros de todos los visitantes, incluidos su nombre, la organización a la que representan, la fecha de expiración de la Habilitación Personal de Seguridad, la(s) fecha(s) de la(s) visita(s) y el/los nombre(s) de la(s) persona(s) visitada(s). Dichos registros deberán conservarse de conformidad con las leyes y reglamentos nacionales y, en cualquier caso, por un plazo no inferior a dos años.
6. La ANS/ADS/ACS de la Parte anfitriona tendrá derecho a exigir la notificación previa por parte de sus establecimientos cuando vayan a recibir visitas de más de 21 días de duración. A continuación, la ANS/ADS/ACS podrá conceder su aprobación, pero si surgiese algún problema de seguridad consultará a la ANS/ADS/ACS del visitante.
7. Para las visitas relacionadas con información clasificada a centros públicos de la otra Parte o a establecimientos de un contratista en las que se necesite tener acceso a información clasificada de niveles CONFIDENCIAL/UK CONFIDENTIAL y RESERVADO/UK SECRET, de la que no se haya determinado previamente que es susceptible de ser compartida, se aplicará

el procedimiento habitual para las visitas internacionales.

8. Las visitas relativas a información clasificada de nivel DIFUSIÓN LIMITADA/UK RESTRICTED se concertarán también directamente entre el establecimiento de origen y el establecimiento objeto de la visita.

## **ARTÍCULO 10**

### **CONTRATOS**

1. Cuando se proponga adjudicar o cuando autorice a un contratista de su país a adjudicar un contrato relacionado con información clasificada de nivel CONFIDENCIAL/UK CONFIDENTIAL o superior a un contratista del otro país, la Parte remitente obtendrá previamente garantía de la ANS/ADS/ACS del otro país de que el contratista propuesto posee habilitación de seguridad del nivel correspondiente y de que dispone también de salvaguardas apropiadas de seguridad para proporcionar una protección adecuada de la información clasificada. La garantía implicará asumir la responsabilidad de que la conducta en materia de seguridad del contratista habilitado será conforme con las leyes y reglamentos nacionales de seguridad y objeto de seguimiento por su ANS/ADS/ACS. Este requisito no se exigirá cuando el contrato contenga exclusivamente información clasificada de nivel DIFUSIÓN LIMITADA/UK RESTRICTED.

2. La ANS/ADS/ACS del país que adjudique el contrato se asegurará de que los contratistas adjudicatarios de un contrato como resultado de estos controles previos tengan conocimiento de las siguientes disposiciones:

- a. La definición de el término “información clasificada” y de las equivalencias entre los niveles de clasificación especificados en el presente AGS.
- b. Los nombres de las autoridades públicas de cada uno de los dos países facultadas para autorizar la cesión de información clasificada relacionada con el contrato y para coordinar su protección.
- c. Los conductos que deban utilizarse para la transmisión de la información clasificada entre las autoridades públicas y/o contratistas implicados.
- d. Los procedimientos y mecanismos para comunicar cualquier cambio que afecte a la información clasificada, sea como consecuencia de una modificación de su clasificación de seguridad, sea porque la protección deje de ser necesaria.
- e. Los procedimientos para la autorización de visitas, del acceso o de inspecciones por personal de uno de los países a establecimientos del otro país que estén comprendidos en el contrato.
- f. La obligación del contratista de divulgar la información clasificada únicamente a personas que hayan recibido previamente habilitación de seguridad para el

acceso , que tengan necesidad de conocer y que estén empleadas o se ocupen de la ejecución del contrato.

- g. La obligación del contratista de no divulgar la información clasificada ni permitir su divulgación a personas que no hayan recibido la habilitación de seguridad apropiada y que no hayan sido expresamente autorizadas para tener dicho acceso.
- h. La obligación del contratista de comunicar inmediatamente a su ANS/ADS/ACS cualquier pérdida, filtración o exposición, real o presunta, de la información clasificada relacionada con el contrato.

3. La ANS/ADS/ACS de la Parte remitente enviará una copia de las partes pertinentes del contrato clasificado a la ANS/ADS/ACS de la Parte receptora, con objeto de hacer posible un seguimiento adecuado de los aspectos clasificados del contrato.

4. Cada contrato clasificado contendrá una guía sobre las exigencias de seguridad y la clasificación de cada aspecto/elemento del contrato. En el Reino de España la notificación figurará en el contrato. En el Reino Unido dicha notificación estará contenida en cláusulas de seguridad específicas y en un Documento sobre Aspectos en materia de Seguridad (*SAL: Security Aspects Letter*). La notificación deberá identificar cada aspecto clasificado del contrato, y cualquier aspecto clasificado que vaya a ser generado por el contrato, y asignar al mismo una clasificación de seguridad determinada. Todo cambio de las exigencias o de los aspectos/elementos se notificará cuando sea necesario y, cuando toda la información haya sido desclasificada, la Parte remitente lo notificará a la Parte receptora.

## ARTÍCULO 11

### GARANTÍAS DE SEGURIDAD

1. Cada ANS/ADS/ACS notificará el nivel de seguridad de cualquier establecimiento situado en su país cuando lo solicite la otra. Asimismo, cada ANS/ADS/ACS notificará el nivel de habilitación de seguridad de cualquiera de sus nacionales, cuando así se le solicite. Estas notificaciones se denominarán, respectivamente, garantía de Habilitación de Seguridad para Establecimiento y garantía de Habilitación Personal de Seguridad.

2. Previa petición, la ANS/ADS/ACS determinará el nivel de habilitación de seguridad del establecimiento/persona que sea objeto de investigación y remitirá una garantía de habilitación de seguridad si el establecimiento/persona dispone ya de habilitación. Si el establecimiento/persona no dispone de habilitación de seguridad, o si ésta es inferior al nivel de seguridad requerido, se enviará una notificación de que no puede emitirse inmediatamente una garantía de habilitación de seguridad. En tales casos, se iniciará el procedimiento necesario para cumplir la solicitud. Si el resultado de las pesquisas es positivo, se otorgará una habilitación de seguridad.

3. Cuando la ANS/ADS/ACS del país en el que esté registrado un establecimiento considere que éste no cumple los requisitos para que se emita respecto del mismo una garantía de Habilitación de Seguridad para Establecimiento, lo comunicará a la ANS/ADS/ACS requirente.
4. Si cualquiera de las ANS/ADS/ACS tiene conocimiento de información negativa sobre una persona respecto de la cual se ha emitido una garantía de Habilitación Personal de Seguridad, informará a la otra ANS/ADS/ACS de la naturaleza de la información y de las medidas que pretende adoptar o que ha adoptado. Cualquiera de las ANS/ADS/ACS podrá solicitar una revisión de cualquier garantía de Habilitación Personal de Seguridad proporcionada previamente por la otra ANS/ADS/ACS, siempre que la solicitud esté motivada. Se informará a la ANS/ADS/ACS requirente del resultado de la revisión y de cualquier medida adoptada en consecuencia.
5. Si se recibe información que suscite dudas sobre la idoneidad de un establecimiento habilitado para seguir custodiando o conservando información clasificada en el otro país, se comunicarán sin demora los detalles de dicha información a la ANS/ADS/ACS para que pueda realizarse una investigación.
6. Si una ANS/ADS/ACS deja en suspenso una Habilitación Personal de Seguridad o toma medidas para revocarla, o deja en suspenso o toma medidas para revocar el acceso concedido a un nacional del otro país sobre la base de una Habilitación Personal de Seguridad, se informará de ello a la otra Parte y se le comunicarán los motivos de dicha actuación.
7. Cualquiera de las ANS/ADS/ACS podrá solicitar a la otra que revise cualquier garantía de Habilitación de Seguridad para Establecimiento, siempre que la solicitud se acompañe de las razones por las que se solicita la revisión. Tras la revisión, se informará del resultado a la ANS/ADS/ACS requirente y se le comunicarán los hechos en que se basó la decisión adoptada.
8. Cuando lo solicite la otra Parte, cualquier ANS/ADS/ACS cooperará en las revisiones e investigaciones relativas a las Habilitaciones Personales de Seguridad o para Establecimiento.

## **ARTÍCULO 12**

### **INFRACCIÓN DE LA SEGURIDAD**

1. En caso de que se produzca una violación de la seguridad que afecte a la información clasificada proporcionada por la otra Parte o exista la sospecha de que se ha divulgado información clasificada a personas no autorizadas, la ANS/ADS/ACS de la Parte receptora lo comunicará inmediatamente a la ANS/ADS/ACS de la Parte remitente.
2. La Parte receptora realizará inmediatamente una investigación, en caso necesario, con la ayuda de la Parte remitente, de conformidad con las leyes y reglamentos vigentes en el país receptor para la protección de la información clasificada. La Parte receptora, informará lo

antes posible a la Parte remitente de las circunstancias, el resultado de la investigación y las medidas adoptadas para prevenir situaciones recurrentes.

### **ARTÍCULO 13**

#### **GASTOS**

Cada Parte correrá con sus propios gastos relacionados con la aplicación y supervisión de las medidas y obligaciones expresadas en el presente AGS.

### **ARTÍCULO 14**

#### **ENMIENDA**

Las disposiciones del presente AGS podrán enmendarse con el consentimiento mutuo por escrito de ambas Partes. Dichas enmiendas entrarán en vigor con arreglo al procedimiento previsto en el artículo 17.

### **ARTÍCULO 15**

#### **CONTROVERSIAS**

Cualquier controversia relativa a la interpretación o aplicación del presente AGS se resolverá mediante consultas entre las Partes.

### **ARTÍCULO 16**

#### **FECHA DE EFECTO**

El presente AGS estará sujeto a la aprobación de conformidad con los procedimientos legales nacionales de cada Parte y entrará en vigor el primer día del segundo mes siguiente al del intercambio de las notificaciones entre las Partes de que se han cumplido los requisitos necesarios establecidos por las leyes y reglamentos internos para que el presente AGS entre en vigor.

### **ARTÍCULO 17**

#### **DENUNCIA / REVISIÓN**

1. El presente AGS permanecerá en vigor durante un período de diez años o hasta que sea denunciado por cualquiera de las Partes, notificando la denuncia a la otra Parte con seis meses de antelación. En tal caso, el AGS dejará de ser válido 180 días después de la fecha en la que se haya notificado la denuncia a la otra Parte. Tras la denuncia, ambas Partes seguirán siendo responsables de custodiar toda la información clasificada intercambiada en virtud de las disposiciones del presente AGS.

2. Se custodiará igualmente toda información clasificada intercambiada al amparo del presente AGS, aun cuando su transmisión tuviera lugar después de la notificación de la denuncia por una de las Partes.

3. En caso de denuncia, cualquier problema pendiente se resolverá mediante consultas entre las dos Partes.

Hecho en ....., el ....., en dos originales, cada uno de ellos en español e inglés, siendo ambos textos igualmente auténticos.

.....  
**POR**  
**EL REINO DE ESPAÑA**

.....  
**POR**  
**EL REINO UNIDO DE GRAN**  
**BRETAÑA E IRLANDA DEL NORTE**

[TRANSLATION – TRADUCTION]

## ACCORD GÉNÉRAL DE SÉCURITÉ ENTRE LE ROYAUME-UNI DE GRANDE-BRETAGNE ET D'IRLANDE DU NORD ET LE ROYAUME D'ESPAGNE RELATIF À LA PROTECTION DES INFORMATIONS CLASSIFIÉES ÉCHANGÉES ENTRE LES DEUX PAYS

Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (ci-après dénommé le Royaume-Uni) et le Royaume d'Espagne (ci-après collectivement dénommés « les Parties ») ont dans l'intérêt de la sûreté nationale établi les dispositions suivantes telles que stipulées dans le présent Accord général de sécurité (AGS), désireux d'assurer la protection des informations classifiées transmises entre les deux pays ou à des organisations commerciales et industrielles situées dans l'un des deux pays.

Le présent AGS intègre les dispositions relatives à la sécurité figurant au chapitre 4 de l'Accord-cadre entre la République française, la République fédérale d'Allemagne, la République italienne, le Royaume d'Espagne, le Royaume de Suède et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord relatif aux mesures visant à faciliter les restructurations et le fonctionnement de l'industrie européenne de défense, signé à Farnborough le 27 juillet 2000, ci-après dénommé « l'Accord cadre ».

### *Article premier. Applicabilité*

1. Le présent AGS présente les procédures de protection des informations classifiées échangées entre les Parties et relevant de la responsabilité de leur Agence nationale de sécurité (ANS) ou de leur Autorité de sécurité désignée (ASD).

2. Le présent AGS ne concerne pas l'échange de renseignements nucléaires, biologiques ou chimiques liés aux équipements généralement connus sous le nom de « Armes de destruction massive » (ADM).

### *Article 2. Définitions*

Aux fins du présent Accord et par souci de précision :

1. L'expression « Informations classifiées » signifie toute information (notamment les connaissances susceptibles d'être communiquées sous quelque forme que ce soit) ou tout matériel nécessitant une protection contre toute divulgation non autorisée et désigné en tant que tel par une classification de sécurité.

2. Le terme « Matériel » s'entend de tout élément ou toute substance pour lequel/laquelle il est possible d'obtenir des informations. Ce concept couvre les documents, les équipements, les armes ou les composants.

3. Le terme « Document » désigne toute information enregistrée indépendamment de sa forme physique ou de ses caractéristiques, telle que les informations écrites ou imprimées (entre autres les lettres, dessins, plans), les supports de stockage informatique

(notamment les disques fixes, disquettes, puces, bandes magnétiques, CD), les photographies, les enregistrements en vidéo et leur reproduction optique ou électronique.

4. Le terme « Entrepreneur » s'entend d'une personne physique ou morale possédant la capacité juridique de conclure des contrats.

5. L'expression « Autorité de sécurité désignée (ASD)/Autorité de sécurité compétente (ASC) » s'entend d'une autorité gouvernementale chargée de mettre en application les exigences de sécurité prévues par le présent AGS.

6. Le terme « Contrat » s'entend d'un accord souscrit entre deux ou davantage de parties et qui crée et identifie des droits et des obligations contraignants.

7. L'expression « Contrat classifié » désigne tout contrat qui prévoit des dispositions pour l'utilisation de renseignements classifiés.

8. L'expression « Agence nationale de sécurité (ANS) » désigne l'autorité gouvernementale des Parties chargée en dernier ressort de la sécurité des informations classifiées traitées dans le présent AGS.

9. L'expression « Partie d'origine » s'entend de la Partie qui communique les informations classifiées, telle que représentée par l'ANS.

10. L'expression « Partie destinataire » s'entend de la Partie à laquelle les informations classifiées sont transmises, telle que représentée par l'ANS.

11. Le terme « installation » désigne une installation, centrale, usine, laboratoire, bureau, université ou autre institut d'enseignement ou entreprise commerciale (y compris tout type d'entrepôts associés, de zones d'entreposage, d'entreprises de services collectifs et composants qui, lorsqu'ils sont reliés par fonction et emplacement, forment une entité opérationnelle), et tout établissement, organisme ou département gouvernemental.

12. L'expression « Responsable de la sécurité » s'entend d'une personne désignée par une ANS/ASD pour faire appliquer les exigences de sécurité industrielle dans un établissement gouvernemental ou dans les locaux d'un contractant.

### *Article 3*

#### Agences nationales de sécurité responsables

1. Les Agences nationales de la sécurité (ANS) chargées des informations classifiées dans le cadre du présent AGS dans chacun des pays sont :

Pour le Royaume-Uni :

Cabinet Office

Security Policy Division

26 Whitehall

London SW1A 2WH

Royaume-Uni

Pour le Royaume d'Espagne :

Secretario de Estado, Director del Centro Nacional de Inteligencia (Centre national du renseignement)



National Security Office  
 Avda. Padre Huidobro, s/n  
 28023 Madrid  
 Espagne

2. Aux fins de la mise en application du présent AGS, les Parties se tiendront mutuellement informées de leurs ASD ou ASC respectives.

*Article 4. Classifications de sécurité*

Les classifications de sécurité et leurs équivalents applicables dans les deux pays sont :

Au Royaume-Uni	En Espagne
UK SECRET (secret)	RESERVADO
UK CONFIDENTIAL (Confidentiel)	CONFIDENCIAL
UK RESTRICTED (restreint)	DIFUSIÓN LIMITADA

*Article 5. Restrictions à l'exploitation et à la divulgation des informations classifiées échangées*

1. Sous réserve des dispositions du paragraphe 2 du présent article, sauf consentement écrit exprès contraire, la Partie destinataire ne divulgue ni n'exploite ni ne permet la divulgation ou l'exploitation d'informations classifiées à des fins autres que celles indiquées par la Partie d'origine ou en son nom et dans le cadre des limites posées par elle.

2. Dans le cadre de l'application de sa législation nationale, la Partie destinataire prend toutes les mesures qui lui sont raisonnablement accessibles pour conserver les informations classifiées qui lui ont été transmises par la Partie d'origine sans les divulguer en vertu de quelque disposition législative ou autre état de droit que ce soit, à moins que la Partie d'origine ne consente à cette divulgation. En cas de demande de mise en diffusion ou de communication de toute information classifiée transmise en vertu des dispositions du présent AGS, la Partie destinataire devra immédiatement avertir la Partie d'origine et les deux Parties se consulteront mutuellement avant d'adopter toute décision.

3. Sous réserve des dispositions du paragraphe 2 du présent article, la Partie destinataire ne pourra pas publier, divulguer ni permettre la publication ou la divulgation de renseignements classifiés qui ont été transmis en vertu des dispositions du présent AGS à tout responsable Gouvernemental, contractant ou ressortissant d'un pays tiers ou à une organisation internationale sans l'accord préalable écrit de la Partie d'origine.

4. Les habilitations personnelles de sécurité destinées aux ressortissants des Parties qui résident dans le pays et demandent un accès aux informations classifiées dans leur propre pays, sont à charge de leur ANS/ASD/ASC.

5. Toutefois, les habilitations personnelles de sécurité destinées aux ressortissants des Parties qui résident légalement dans le pays de l'autre Partie et sollicitent un emploi dans ce pays, sont à charge de l'ANS/ASD/ASC du pays qui effectue les contrôles appropriés à l'étranger et qui notifie le pays d'origine.

6. Une habilitation personnelle de sécurité délivrée par une ANS/ASD/ASC est acceptée par les autres ANS/ASD/ASC des Parties pour un emploi exigeant un accès à des informations classifiées au sein d'une société dans leur pays.

#### *Article 6. Protection des informations classifiées*

1. Dans le cadre de leur législation nationale, les Parties prendront toutes les mesures appropriées pour assurer la protection de la sécurité des informations classifiées transmises entre elles ou à un contractant ou une installation, ou détenues ou produites par un contractant ou une installation en relation avec un contrat classifié conclu par une Partie sur le territoire ou sous la juridiction de l'autre Partie.

2. La Partie d'origine veillera à ce que la Partie destinataire soit informée :

a. De la classification de sécurité des renseignements, de toutes conditions de leur divulgation ou des limites imposées à leur exploitation et que lesdits renseignements sont marqués en conséquence.

b. De toute modification ultérieure de leur classification de sécurité.

3. La Partie destinataire devra :

a. Dans le respect de ses lois et règlements nationaux, accorder à des informations classifiées reçues de l'autre Partie un niveau de protection équivalent à celui qui est assuré à ses propres informations classifiées bénéficiant d'une classification équivalente conformément à l'article 4 ci-dessus.

b. Veiller à ce que sa propre classification de sécurité soit indiquée sur les informations classifiées, conformément à l'article 4 ci-dessus.

c. S'assurer que les classifications de sécurité ne sont pas modifiées, sauf avec l'autorisation écrite de la Partie d'origine ou en son nom.

4. Afin que les Parties puissent atteindre des normes de sécurité comparables et les maintenir, chacune des ANS devra, sur demande, fournir à l'autre des renseignements touchant les normes de sécurité, procédures et pratiques qu'elle applique aux fins de la sauvegarde de renseignements classifiés et faciliter à cette fin les visites des autres ANS ou ASD/ASC selon le cas.

#### *Article 7. Accès aux informations classifiées*

1. L'accès aux informations classifiées au niveau UK CONFIDENTIAL /CONFIDENCIAL et aux niveaux supérieurs est limité aux personnes dont les fonctions exigent ledit accès et auxquelles une habilitation de sécurité a été octroyée par l'ANS/ASD/ASC de la Partie destinataire conformément à leurs lois et réglementations nationales, du niveau correspondant à la classification des informations.

2. L'accès aux informations classifiées aux niveaux UK CONFIDENTIAL/CONFIDENCIAL et UK SECRET/RESERVADO par une personne ayant la seule nationalité d'une Partie à l'Accord cadre peut être accordé sans l'autorisation préalable de la Partie d'origine.

3. L'accès aux informations classifiées aux niveaux UK CONFIDENTIAL/CONFIDENCIAL et UK SECRET/RESERVADO par une personne ayant la double nationalité d'une Partie et d'un État de l'Union européenne peut être accordé sans l'autorisation préalable de la Partie d'origine.

4. L'accès aux informations classifiées aux niveaux UK CONFIDENTIAL/CONFIDENCIAL et UK SECRET/RESERVADO par une personne n'ayant pas la nationalité décrite aux paragraphes 2 et 3 du présent Article fera l'objet de consultations préalables avec la Partie d'origine. Le processus de consultation concernant ces personnes est décrit aux alinéas a à e ci-dessous.

a. Les Parties s'avertissent et se consultent lorsqu'il est nécessaire d'accorder l'accès à des renseignements classifiés relatifs à un projet/programme spécifique à des ressortissants autres que les Parties.

b. Le processus de consultation est lancé avant le début ou, le cas échéant, pendant un projet/programme.

c. Les informations sont limitées à la nationalité des personnes concernées.

d. La Partie qui reçoit une telle notification détermine si l'accès aux informations classifiées par des ressortissants non participants est acceptable ou non.

e. De telles consultations sont traitées d'urgence afin de parvenir à un consensus. Dans les cas où cela ne s'avère pas possible, la décision de la Partie d'origine est acceptée.

5. L'accès aux informations classifiées au niveau UK RESTRICTED/DIFUSIÓN LIMITADA est limité aux personnes dont les fonctions exigent ledit accès. Une habilitation personnelle de sécurité n'est pas nécessaire.

#### *Article 8. Transmission des informations classifiées*

1. Les informations classifiées aux niveaux UK CONFIDENTIAL/CONFIDENCIAL et UK SECRET/RESERVADO seront normalement transmises entre les Parties par la voie de valises diplomatiques de Gouvernement à Gouvernement, ou par les voies approuvées par les ANS/ASD des Parties.

2. En cas d'urgence, à savoir uniquement lorsque l'utilisation de la voie diplomatique de Gouvernement à Gouvernement ne peut pas répondre aux critères requis, des renseignements classifiés au niveau UK CONFIDENTIAL/CONFIDENCIAL peuvent être transmis via des entreprises privées de courrier, à condition que les critères suivants soient satisfaits :

a. L'entreprise de courrier est située sur le territoire des Parties et a établi un programme de sécurité et de protection pour la prise en charge d'articles de valeur avec un service de signature, incluant une surveillance et un enregistrement permanents permettant de déterminer à tout moment qui en a la charge, soit par un système de registre de signatures et de pointage, soit par un système électronique de localisation et de suivi.

b. La société de messagerie doit obtenir et fournir à l'expéditeur un justificatif de livraison sur le registre de signatures et de pointage, ou elle doit obtenir un reçu portant le numéro des colis correspondants.

c. L'entreprise de courrier doit assurer que l'expédition sera livrée au destinataire avant une heure et une date données, dans un délai de 24 heures, dans des circonstances normales.

d. L'entreprise de courrier peut confier la tâche à un commissaire ou à un sous-traitant mais restera responsable s'agissant de remplir les obligations ci-dessus.

3. Les informations classifiées au niveau UK RESTRICTED/DIFUSIÓN LIMITADA seront transmises entre les Parties, conformément aux règlements nationaux de la Partie d'origine, qui peuvent prévoir le recours à des entreprises privées de courrier.

4. Les informations classifiées aux niveaux UK CONFIDENTIAL/CONFIDENCIAL et UK SECRET/RESERVADO ne peuvent pas être transmises en texte clair par des moyens électroniques. Seuls les systèmes cryptographiques approuvés par les ANS/ASD concernées peuvent être utilisés pour le cryptage des informations classifiées aux niveaux UK CONFIDENTIAL/CONFIDENCIAL et UK SECRET/RESERVADO, quelle que soit la méthode de transmission. Les informations classifiées au niveau UK RESTRICTED/ DIFUSIÓN LIMITADA peuvent être transmises ou accessibles par des moyens électroniques (par ex. par des liaisons informatiques point à point) via un réseau public comme l'Internet, uniquement en utilisant des dispositifs de cryptage gouvernementaux ou commerciaux acceptés d'un commun accord entre les autorités nationales compétentes. Toutefois, les conversations téléphoniques, vidéoconférences ou transmissions par télécopie contenant des informations classifiées de niveau UK RESTRICTED/ DIFUSIÓN LIMITADA peuvent se faire en clair, en l'absence de système de cryptage approuvé.

5. Lorsque de gros volumes d'informations classifiées doivent être transmis, les moyens de transport, l'itinéraire et l'escorte, (le cas échéant) sont conjointement déterminés au cas par cas par les autorités compétentes des Parties.

#### *Article 9. Visites*

1. Chaque Partie, sur la base de l'intérêt mutuel, autorise des visites impliquant l'accès aux informations classifiées de ses installations, par des représentants civils ou militaires de l'autre Partie et par les employés de leur contractant, à condition que le visiteur dispose d'une habilitation personnelle de sécurité appropriée et fasse état d'un « besoin de savoir ».

2. Tous les visiteurs se conforment aux réglementations de sécurité de la Partie d'accueil. Toute information classifiée divulguée ou mise à la disposition de visiteurs est traitée comme si elle était fournie à la Partie répondant des visiteurs et est protégée en conséquence.

3. Pour les visites effectuées dans le cas d'informations classifiées partageables, dans des établissements gouvernementaux de l'autre Partie ou dans des installations d'un contractant qui demandent un accès à des informations classifiées aux niveaux UK

CONFIDENTIAL/CONFIDENCIAL et UK SECRET/RESERVADO, la procédure suivante est appliquée :

1. Sous réserve des dispositions suivantes, ces visites seront arrangées directement entre l'installation d'envoi et l'installation devant être visitée.

2. Pour ces visites les conditions préalables suivantes devront également être satisfaites :

a) La visite aura un but officiel.

b) Toute installation d'un contractant à visiter dispose d'une attestation de sécurité d'installation appropriée.

c) Avant l'arrivée du visiteur, le responsable de la sécurité de l'installation d'envoi doit fournir une confirmation de l'habilitation de sécurité personnelle dudit visiteur, directement à l'installation à visiter. Pour confirmer l'identité, le visiteur doit être porteur d'une carte d'identité ou d'un passeport à présenter aux autorités de sécurité de l'installation à visiter.

4. Il appartient aux responsables de la sécurité de :

a. L'installation d'envoi d'assurer avec leurs ANS/ASD/ASC que toute installation de société à visiter est en possession d'une habilitation de sécurité d'établissement appropriée;

b. L'installation d'envoi et de l'installation devant être visitée de convenir de la nécessité de la visite.

5. Le responsable de la sécurité de l'installation d'une société à visiter ou, si approprié, d'un établissement gouvernemental doit veiller à tenir un registre de tous les visiteurs, y compris leur nom, l'organisation qu'ils représentent, la date d'expiration de l'habilitation de sécurité individuelle, la/les dates de la/des visite(s) et le/les noms de la/des personnes visitées. Ces registres devront être conservés conformément aux lois et réglementations nationales et, en tout cas, pendant une période d'au moins deux ans.

6. L'ANS/ASD/ASC de la Partie d'accueil a le droit de demander une notification préalable à ses installations à visiter pour les visites d'une durée de plus de 21 jours. Cette ANS/ASD/ASC peut alors accorder l'approbation mais si un problème de sécurité se pose, elle consulte l'ANS/ASD/ASC du visiteur.

7. Pour les visites effectuées dans le contexte de renseignements classifiés, dans des établissements gouvernementaux de l'autre Partie ou dans des installations d'un contractant lorsque l'accès est demandé aux renseignements classifiés de niveaux UK CONFIDENTIAL/CONFIDENCIAL et UK SECRET/RESERVADO, qui n'ont pas été prédéfinis comme partageables, la procédure de visite internationale normale est appliquée :

8. Les visites concernant des informations classifiées au niveau UK RESTRICTED/DIFUSIÓN LIMITADA sont également organisées directement entre l'installation d'envoi et l'installation devant être visitée.

*Article 10. Contrats*

1. La Partie d'origine qui a l'intention de conclure un contrat portant sur des renseignements classifiés au niveau UK CONFIDENTIAL/CONFIDENCIAL ou à un niveau supérieur, avec un entrepreneur de l'autre pays, ou d'autoriser un entrepreneur de son pays à conclure un tel contrat, devra obtenir au préalable l'assurance de l'ANS/ASD/ASC de cet autre pays que l'entrepreneur proposé est titulaire d'une habilitation de sécurité du niveau approprié et que ses installations comportent les garanties de sécurité voulues pour protéger adéquatement les informations classifiées. L'assurance obligera l'entrepreneur habilité à appliquer des mesures de sécurité conformes au droit et aux règlements nationaux, sous la surveillance de son ANS/ASD/ASC. Cette obligation ne s'applique pas lorsqu'un contrat contient exclusivement des informations classifiées au niveau UK RESTRICTED/ DIFUSIÓN LIMITADA.

2. L'ANS/ASD/ASC du pays qui conclut le contrat doit s'assurer que les entrepreneurs qui reçoivent des contrats passés suite à ces enquêtes précontractuelles sont conscients des dispositions suivantes :

a. La définition de l'expression « Informations classifiées » et les équivalences de classification spécifiées dans le présent AGS.

b. Les noms de l'autorité gouvernementale de chacune des deux Parties habilitée à autoriser la communication des renseignements classifiés ainsi qu'à coordonner la sauvegarde des renseignements classifiés faisant l'objet du contrat.

c. Les voies de communication à utiliser pour le transfert des renseignements classifiés entre les autorités gouvernementales et/ou les entrepreneurs concernés.

d. Les procédures et mécanismes de communication des éventuelles modifications affectant les renseignements classifiés dues au fait que la classification de sécurité a changé ou que la protection n'est plus requise.

e. Les procédures que les agents d'un pays doivent suivre pour obtenir l'autorisation de se rendre en visite dans l'autre pays, d'avoir accès à ses installations et de les inspecter comme prévu par le contrat.

f. L'obligation de ne divulguer les renseignements classifiés qu'à des personnes dûment autorisées à accéder à ces renseignements, parce qu'elles ont besoin de les connaître ou qu'elles sont employées à l'exécution du contrat.

g. L'obligation faite à l'entrepreneur de ne pas divulguer les renseignements classifiés ou de ne pas autoriser leur divulgation à quiconque n'aurait pas été à ce dûment et expressément habilité pour la sécurité dont il relève.

h. L'obligation de notifier immédiatement son ANS/ASD/ASC de toute perte, fuite ou compromission constatée ou présumée des renseignements classifiés faisant l'objet de ce contrat.

3. L'ANS/ASD/ASC de la Partie d'origine transmettra une copie des sections pertinentes du contrat classifié aux ANS/ASD/ASC de la Partie destinataire pour permettre une surveillance adéquate des aspects classifiés du contrat.

4. Chaque contrat classifié contient des instructions relatives aux exigences de sécurité et à la classification de chaque modalité/élément du contrat. Au Royaume-Uni, la notification fera l'objet de clauses spécifiques de sécurité et d'une annexe de sécurité

(AS). Dans le Royaume d'Espagne, cette notification fera partie du contrat. La notification devra identifier chaque élément du contrat qui est classifié ou qui le deviendra suite au contrat, et lui allouera une classification de sécurité donnée. Les modifications des exigences ou des aspects/éléments seront notifiées si et dès que nécessaire et la Partie d'origine informera la Partie destinataire dès que l'ensemble des informations aura été déclassifié.

### *Article 11. Assurances de sécurité*

1. Chaque ANS/ASD/ASC donnera des détails sur le statut d'habilitation de sécurité d'une installation dans son pays lorsque l'autre le lui demandera. Chaque ANS/ASD/ASC fournira aussi sur demande des précisions sur le statut d'habilitation de sécurité octroyé à l'un de ses nationaux. Ces notifications seront connues sous le nom d'assurance d'habilitation de sécurité d'installation et assurance d'habilitation personnelle de sécurité, respectivement.

2. L'ANS/ASD/ASC établira sur demande le statut d'habilitation de sécurité de l'installation/la personne qui fait l'objet de l'enquête et transférera une assurance d'habilitation de sécurité si l'installation/la personne est déjà habilitée. Si tel n'est pas le cas ou si l'habilitation est d'un niveau inférieur à celui qui a été demandé, l'autorité compétente ayant demandé l'information sera informée que l'assurance d'habilitation de sécurité ne peut être octroyée immédiatement. Dans ce cas, d'autres mesures seront prises pour répondre à cette exigence. Si l'enquête aboutit, une habilitation de sécurité sera délivrée.

3. Si une installation est considérée par l'ANS/ASD/ASC, dans le pays où elle est enregistrée comme inéligible pour une assurance d'habilitation de sécurité d'installation accordée à un établissement, l'ANS/ASD/ASC ayant demandé l'information en sera informée.

4. Si des renseignements défavorables concernant une personne bénéficiant d'une habilitation personnelle de sécurité sont portés à la connaissance de l'une ou l'autre ANS/ASD/ASC, ladite autorité informera son homologue de la teneur des renseignements et des mesures qu'elle a l'intention de prendre ou qu'elle a déjà prises. Chacune des ANS/ASD/ASC pourra demander que soit reconsidérée toute habilitation personnelle de sécurité octroyée précédemment par l'autre ANS/ASD/ASC, à la condition de justifier sa demande; elle sera ensuite notifiée des résultats de l'examen et des mesures ultérieures.

5. Si des informations devenues disponibles suscitent des doutes sur l'aptitude d'une installation habilitée à continuer à détenir ou à conserver des informations classifiées dans l'autre pays, des précisions sur ces informations seront rapidement notifiées à l'ANS/ASD/ASC pour permettre la réalisation d'une enquête.

6. Lorsque l'une ou l'autre ANS/ASD/ASC révoque une habilitation personnelle de sécurité ou prend des mesures en vue de la révoquer ou révoque l'autorisation d'accès accordée à un national de l'autre pays bénéficiant d'une habilitation personnelle de sécurité ou prend des mesures pour révoquer cette autorisation, l'autre Partie sera informée des mesures prises et des raisons qui les ont inspirées.

7. Chaque ANS/ASD/ASC peut demander à l'autre de reconsidérer toute habilitation personnelle de sécurité à condition de justifier sa demande. À la suite de ce réexamen, l'ANS/ASD/ASC qui aura présenté la demande sera notifiée des résultats et informée des faits étayant toutes décisions prises.

8. Si l'autre Partie le demande, chaque ANS/ASD/ASC coopèrera aux réexamens et enquêtes concernant les habilitations de sécurité personnelles et d'installation.

#### *Article 12. Atteinte à la sécurité*

1. En cas d'atteinte à la sécurité portant sur des informations classifiées fournies par l'autre Partie ou en cas de soupçon que ces informations classifiées aient pu être divulguées à des personnes non autorisées, l'ANS/ASD/ASC de la Partie destinataire est tenue d'en informer immédiatement l'ANS/ASD/ASC de la Partie d'origine.

2. La Partie destinataire doit immédiatement ouvrir une enquête, le cas échéant avec l'assistance de la Partie d'origine, conformément à ses lois ou réglementation en vigueur dans le pays du destinataire, applicables à la protection des renseignements classifiés. La Partie destinataire informe dès que possible la Partie d'origine des circonstances de l'incident, des mesures prises et du résultat de l'enquête, pour éviter toute reproduction des faits.

#### *Article 13. Frais*

Chaque Partie supporte les frais qu'elle a encourus pour la mise en œuvre et la supervision des mesures et obligations exprimées dans le présent AGS.

#### *Article 14. Amendement*

Les dispositions du présent AGS peuvent être modifiées avec le consentement mutuel écrit des deux Parties. Les modifications entrent en vigueur conformément à la procédure décrite à l'article 17.

#### *Article 15. Différends*

Tout différend relatif à l'interprétation ou la mise en œuvre du présent AGS est résolu par voie de consultation entre les Parties.

#### *Article 16. Date d'entrée en vigueur*

Le présent AGS est soumis à approbation dans le respect des procédures légales nationales de chaque Partie et entrera en vigueur le premier jour du deuxième mois après l'échange de notifications entre les Parties aux termes desquelles les procédures nécessaires définies par les lois ou réglementations internes pour l'entrée en vigueur du présent AGS auront été satisfaites.



*Article 17. Dénonciation/révision*

1. Le présent AGS restera en vigueur pendant dix ans ou jusqu'à ce qu'il soit dénoncé par l'une ou l'autre Partie moyennant un préavis écrit de six (6) mois adressé à l'autre Partie. Dans ce cas, la validité de l'AGS expirera 180 jours après la date de notification de la dénonciation à l'autre Partie. Après l'expiration de l'Accord, les deux Parties demeurent responsables de la sauvegarde de tous les renseignements classifiés échangés en vertu des dispositions du présent AGS.

2. De même, toute information classifiée échangée en vertu du présent AGS sera également sauvegardée alors même que le transfert des renseignements s'est produit après que l'une des Parties a informé l'autre de son intention d'y mettre fin.

3. En cas de dénonciation, les solutions à tous problèmes non résolus seront cherchées par voie de consultation entre les deux Parties.

FAIT à Madrid, le 26 février 2009, en deux exemplaires originaux, chacun en langues anglaise et espagnole, les deux textes faisant également foi.

Pour le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord :

DENISE HOLT

Pour le Royaume d'Espagne :

ALBERTO SAIZ