



Spain No.1 (2010)

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 is not in force]

*Presented to Parliament
by the Secretary of State for Foreign and Commonwealth Affairs
by Command of Her Majesty
May 2010*

© Crown Copyright 2010

The text in this document (excluding the Royal Arms and other departmental or agency logos) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

ISBN: 9780101787321

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID: 2369762 05/10

Printed on paper containing 75% recycled fibre content minimum.

**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 Industry¹, 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.

¹ 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:

IN THE UK	IN SPAIN
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



Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, telephone, fax and email

TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/general enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop

12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/general enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: <http://www.bookshop.parliament.uk>

TSO@Blackwell and other accredited agents

Customers can also order publications from:

TSO Ireland
16 Arthur Street, Belfast BT1 4GD
Telephone orders/general enquiries: 028 9023 8451
Fax orders: 028 9023 5401

ISBN 978-0-10-178732-1

