Turkey No. 1 (2016)

Security Agreement

between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the Republic of Turkey concerning the Protection of Defence Classified Information

Ankara, 25 February 2016

[The Agreement has not entered into force]

Presented to Parliament
by the Secretary of State for Foreign and Commonwealth Affairs
by Command of Her Majesty
November 2016

Cm 9376

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at Treaty Section, Foreign and Commonwealth Office, King Charles Street, London, SW1A 2AH

Print ISBN 9781474139137
Web ISBN 9781474139144

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

ID P002848098 57714 11/16

Printed on paper containing 30% recycled fibre content minimum

SECURITY AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND THE GOVERNMENT OF THE REPUBLIC OF TURKEY CONCERNING THE PROTECTION OF DEFENCE CLASSIFIED INFORMATION

PREAMBLE

The Government of the United Kingdom of Great Britain and Northern Ireland (hereinafter referred to as the United Kingdom) and the Government of the Republic of Turkey, (hereinafter referred to individually as Party, collectively as Parties),

Wishing to ensure the protection of Classified Information on defence exchanged, transferred or generated between the two countries and Organisations in either of the two countries, the Parties have concluded this Security Agreement (hereinafter referred to as the "Agreement"),

Stating this Agreement does not cover the exchange of Nuclear, Biological or Chemical (NBC) information related to equipment commonly referred to as Weapons of Mass Destruction (WMD) for which a separate arrangement would be required,

Confirming that this Agreement shall not affect the commitments arising from other international agreements to which either country is a party and shall not be used against the interests, security and/or territorial integrity of other States,

For the purposes of this Agreement and in the interests of national security the following arrangements have been established.

ARTICLE 1

Purpose and Scope

The Purpose of this Agreement is to establish the procedures and principles for ensuring security of Classified Information related to defence in the scope of cooperation activities carried out between the Organisations defined in this Agreement in accordance with their respective national security laws and regulations.

ARTICLE 2

Definitions

2.1 The following terms are defined in the interests of clarity:

2.2 **"Classified Contract"** means an agreement between two or more parties which contains or involves access to or the generation, use or transmission of Classified Information.

2.3 **"Classified Information"** means any information, irrespective of its form, carrier and manner of recording, including documents and materials also in the process of being generated, which require protection against unauthorised disclosure in accordance with the national security laws and regulations of either Party and this Agreement.

2.4 **"Classified Project"** means all kinds of works within the scope of the Classified Contract.

2.5 **"Competent Security Authority (CSA)"** means a security authority subordinate to the Designated Security Authority (DSA) responsible for undertaking specific administrative or implementation aspects of the provisions of this Agreement.

2.6 **"Contractor"** means an individual or legal entity possessing the legal capability to undertake Classified Contracts.

2.7 **"Designated Security Authority (DSA)"** means the Government authority responsible for defence security in each country.

2.8. **"Facility"** means a Government establishment or Contractor premises.

2.9 **"Facility Security Clearance"** means a determination by a respective DSA or CSA that a Facility under its jurisdiction is security cleared and has in place appropriate security measures to access and protect Classified Information in accordance with the relevant national security laws and regulations and as such has been granted a clearance certificate if required by national security laws and regulations.

2.10 **"Host Party"** means the country receiving the personnel during the visits.

2.11 **"Need-to-Know"** means the necessity to have access to Classified Information in connection with an individual's duties and/or for the performance of a specific task.

2.12 **"Organisation"** means government entities or private companies, where Classified Information exists or where a Classified Project is being carried out or which involve the implementation of the Classified Contracts.

2.13 **"Originating Party"** means the Party, or a Contractor under its jurisdiction, of the country initiating the Classified Information.

2.14 **"Owner"** means the government authority in a Party which, in accordance with its national security laws and regulations, is responsible for any decisions affecting Classified Information generated or exchanged under this Agreement. Contractors under the jurisdiction of a Party may generate or provide Classified Information, but they are not considered the Owner for the purposes of this Agreement.

2.15 **"Personnel Security Clearance"** means a determination by a respective DSA or CSA that an individual has been security cleared to a specific level and may access on a Need-to-Know basis and handle Classified Information in accordance with its national security laws and regulations and as such has been granted a clearance certificate if required by national security laws and regulations.

2.16 **"Recipient Party"** means the Party, or a Contractor under its jurisdiction, of the country to which the Classified Information is transmitted.

2.17 **"Third Party"** means a State, international organisation or any other entity which is not a Party to this Agreement or an individual who does not hold the nationality of the country of either of the Parties.

2.18 **"Visitor"** means any personnel who visits a Facility located in the country of the other Party where Classified Information is held or where a Classified Contract is being undertaken or a Classified Project being performed.

ARTICLE 3

Security Authorities

3.1 The DSA's in each country responsible for Defence Security are:

FOR THE UNITED KINGDOM

Defence Security
Ministry of Defence
Main Building
Whitehall
London SW1A 2HB

FOR THE REPUBLIC OF TURKEY

Ministry of National Defence
Technical Services Department
Lt.Gen.Mehmet Sırrı Seyrek Barracks
Merasim St. No:10
06100 Yücetepe
Ankara

3.2 The above mentioned DSA's shall advise each other about any subordinate CSAs responsible for specific administrative or implementation aspects of the provisions of this Agreement.

ARTICLE 4

Security Classification Levels

4.1 Within the framework of the security measures prescribed by the respective national security laws and regulations, the DSA's or CSA's and the Organisations in the country of the Parties agree to duly ensure the protection of the Classified Information exchanged or generated by mutual cooperation, and shall adopt the equivalence of levels of security classification as shown in the table below:

For the United Kingdom:	For the Republic of Turkey:
UK TOP SECRET	"ÇOK GİZLİ"
UK SECRET	"GİZLİ"
No equivalent (see paragraph 4.2 of this Article)	"ÖZEL"
UK OFFICIAL-SENSITIVE	"HİZMETE ÖZEL"

4.2 The United Kingdom shall afford Classified Information marked "ÖZEL" an equivalent level of protection as it would for Classified Information at the level of UK SECRET.

4.3 Classified Information provided under this Agreement shall be suitably prefixed to indicate the country of the Party that provided or which owns the information as required by national security laws and regulations.

4.4 The Recipient Party shall ensure that the security classification levels assigned to Classified Information provided by the Originating Party are not altered or revoked, except with the prior written authorisation of the Owner.

4.5 The DSA's or CSA's of the Parties agree to mutually inform each other about any changes made to the security classification levels identified in Article 4.1 above.

4.6 In the event that Classified Information at the UK TOP SECRET/ÇOK GİZLİ level needs to be generated and/or exchanged, additional security measures shall be agreed between the DSA's of the Parties.

ARTICLE 5

Restrictions on Use and Disclosure

5.1 Unless express prior written consent is given to the contrary by the Owner, the Recipient 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.

5.2 The Recipient Party shall not pass to a Government official, Contractor, Contractor's employee or to any other person holding the nationality of any third country, or to any Third Party or international organisation, any Classified Information supplied under the provisions of this Agreement, nor shall it publicly disclose any Classified Information, without the prior written permission of the Originating Party.

5.3 Within the scope of its national security laws and regulations the Recipient Party shall take all reasonable steps legally 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. If there is any request to declassify or disclose any Classified Information transmitted under the provisions of this Agreement, the Recipient Party shall immediately notify the Originating Party and both Parties shall consult each other before any decision is taken.

5.4 Nothing in this Agreement shall be taken as an authority for, or to govern the release, use, exchange or disclosure of information in which intellectual property rights exist, until the specific written authorisation of the Owner of these rights has first been obtained, whether the Owner is one of the Parties or a Third Party.

ARTICLE 6

Marking, Protection, Translation, Reproduction and Destruction of Classified Information

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

(a) The classification of the information by marking it with a security classification.

(b) Any conditions of release or limitations on its use.

(c) Any subsequent change in security classification.

6.2 The Recipient Party shall:

(a) In accordance with its national security laws and regulations, afford Classified Information received from the other Party a level of security protection that is afforded to national Classified Information of an equivalent classification originated by the Recipient Party, to the extent that they provide a degree of protection no less stringent than that provided for NATO Classified Material as detailed in the document "Security Within the North Atlantic Treaty Organisation" (C-M (2002)49) dated 17th June 2002 and its subsequent amendments.

(b) If required by national security laws and regulations ensure that Classified Information is marked with its own classification in accordance with Article 4.1 above.

(c) Ensure that classifications are not altered, except as authorised in writing by or on behalf of the Owner.

(d) Ensure that, when it is no longer required or it becomes void, Classified Information received from the Originating Party is either returned or destroyed in accordance with the national security laws and regulations of the Recipient Party in such a manner as to prevent its partial or total reconstruction.

(e) Only reproduce Classified Information in accordance with its national security laws and regulations. Any reproduced information shall be given the same protection as the original. The number of copies shall be limited to the minimum required for official purposes.

(f) Ensure that translations of Classified Information are made by appropriately security cleared individuals and marked with the same security classification level as the original.

(g) Subject to Article 5, not disclose Classified Information to a Third Party, without the prior approval of the Owner.

6.3 In order to achieve and maintain comparable standards of security, each DSA shall, on request, provide to the other information about its security standards, procedures and practices for safeguarding Classified Information, and shall for this purpose facilitate visits by the DSA or CSA of the other Party. In the event that either Party significantly lowers its security standards to an extent that it shall have an adverse effect on the protection afforded to Classified Information received from the other Party it shall notify the other Party and both Parties shall mutually agree the appropriate course of action.

ARTICLE 7

Access to Classified Information

7.1 Access to Classified Information at the UK SECRET and ÖZEL or GİZLİ levels shall be limited to those persons who have a Need-to-Know, and who have been granted an appropriate Personnel Security Clearance by the recipient DSA/CSA in accordance with their national security laws and regulations and standards, to the level appropriate to the security classification level of the information to be accessed.

7.2 The national standards of the Personnel Security Clearance process shall be designed to determine the honesty, reliability and trustworthiness of individuals to be granted access to Classified Information.

7.3 Access to Classified Information at the UK OFFICIAL-SENSITIVE and HIZMETE ÖZEL levels shall be limited to individuals who have a Need-to-Know. As a minimum, individuals having such access should be subjected to basic recruitment checks which should establish proof of identity; confirm that they satisfy all legal requirements for employment; and verify their employment record. Criminal record checks should also be conducted on the individual if permissible under national security laws and regulations of the Parties. The requirement for these recruitment checks shall be included in the Classified Contract security requirements clause.

ARTICLE 8

Transmission of Classified Information

8.1 Classified Information at the UK SECRET and ÖZEL or GİZLİ levels shall be transmitted between the Parties in accordance with their respective national security laws and regulations. The normal route shall be through official diplomatic Government-to-Government channels, but other arrangements may be established, if mutually acceptable to both Parties.

8.2 Classified Information at the UK OFFICIAL-SENSITIVE/HIZMETE ÖZEL levels shall be transmitted in accordance with the national security laws and regulations of the Originating Party, which may include the use of international postal services or commercial courier companies.

8.3 Where large volumes of Classified Information are to be transmitted between the Parties as freight, the means of transport, the route and any escort requirements shall be the subject of a transportation plan mutually agreed in advance by the DSAs or CSAs of the Parties.

8.4 Classified Information shall not be transmitted electronically unless encrypted devices mutually approved by both Parties are used. However exceptionally in urgent circumstances, and only if the Owner approves in accordance with national security laws and regulations, Classified Information at the UK OFFICIAL-SENSITIVE/HIZMETE ÖZEL levels may be transmitted electronically in clear text if a suitable encryption device is not available.

ARTICLE 9

Visits

9.1 Except as determined in paragraph 9.7 of this Article requests for visits between the Parties shall be submitted in accordance with the Multinational Industrial Security Working Group (MISWG) Document No.7. Requests for such visits shall be submitted on a government-to-government basis by the Parties' DSAs or CSAs.

9.2 Requests shall include the following information:

9.2.1 Name of proposed Visitor, date and place of birth, nationality and passport number/identity card number.

9.2.2 Official status of the Visitor together with the name of the Facility or Organisation, which he/she represents or to which he/she belongs.

9.2.3 Certification of level of Personnel Security Clearance held by the Visitor.

9.2.4 Name and address of the Facility or Facilities to be visited.

9.2.5 Name and status of the person(s) to be visited, if known.

9.2.6 Purpose of the visit.

9.2.7 Date of the visit. In cases of recurring visits the total period covered by the visits should be stated.

9.3 All Visitors shall comply with the national security laws and regulations of the Host Party.

9.4 Visit requests shall be submitted to the Host Party in accordance with its normal visit procedures. Short notice visits may be arranged in urgent cases by special mutually determined arrangements.

9.5 In cases involving a specific Classified Contract or Classified Project it may, subject to the approval of both Parties, be possible to establish recurring Visitors lists. These lists shall be valid for an initial period not exceeding 12 months and may be extended for a further period of time (not to exceed 12 months) subject to the prior written approval of the DSAs or CSAs. They shall be submitted in accordance with the national security laws and regulations of the Host Party. Once a list has been approved, visit arrangements shall be made direct between the Facilities involved in respect of listed individuals.

9.6 Any information which may be provided to visiting personnel, or which may come to the notice of visiting personnel, shall be treated by them as if such information had been furnished pursuant to the provisions of this Agreement.

9.7 Visits to Organisations in the Republic of Turkey requiring access only to Classified Information at the level of UK OFFICIAL-SENSITIVE/HIZMETE ÖZEL shall be processed in accordance with paragraphs 9.1-9.6 of this Article or as subject to local national security laws and regulations. Visits involving such Classified Information to Organisations in the United Kingdom shall be arranged directly between the sending Facility and the Facility to be visited. Such visits do not require the Visitors to have a Personnel Security Clearance however the Visitors shall have been the subject of basic recruitment checks in accordance with paragraph 7.3 of Article 7.

ARTICLE 10

Classified Contracts

10.1 When proposing to place, or authorising a Contractor in its country to place, a Classified Contract at the UK SECRET and ÖZEL or GIZLI levels with a Contractor in the other country, the DSA or CSA of the respective Party shall obtain prior assurance from the DSA or CSA of the other Party that the proposed Contractor Facility has been granted a Facility Security Clearance to the appropriate level and also has suitable security safeguards to provide adequate protection for Classified Information. The assurance shall carry a responsibility that the security conduct by the cleared Contractor shall be in accordance with national security laws and regulations and monitored by the DSA or CSA.

10.2 The DSA or CSA of the Party awarding a Classified Contract shall ensure that Contractors under the jurisdiction of the DSA or CSA of the other Party that receive Classified Contracts placed as a consequence of these pre-Contract enquiries are aware of the following provisions:

10.2.1 The definition of the term "Classified Information" and of the equivalent security classification levels of the two Parties in accordance with the provisions of paragraph 4.1 of Article 4.

10.2.2 A statement that Classified Information provided or generated as a consequence of the Classified Contract shall be protected in accordance with applicable national security laws and regulations.

10.2.3 The names of the contracting authority in each of the countries empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Classified Contract.

10.2.4 The channels to be used for the transfer of the Classified Information between the contracting authorities and/or Contractors involved, which shall be in accordance with Article 8 of this Agreement.

10.2.5 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.

10.2.6 The procedures for the approval of visits, access or inspection by personnel of one Party to the Contractor Facility of the other Party that is covered by the Classified Contract.

10.2.7 A statement that the Contractor shall disclose the Classified Information only to a person who has previously been granted a Personnel Security Clearance for access, who needs to know, and is employed on, or engaged in, the carrying out of the Classified Contract.

10.2.8 A statement that the Contractor shall not disclose the Classified Information or permit it to be disclosed to any person not granted a Personnel Security Clearance by his DSA or CSA or to a Third Party without the prior written consent of the Owner.

10.2.9 The requirement that the Contractor shall immediately notify his DSA or CSA of any actual or suspected loss, leak or compromise of the Classified Information relating to the Classified Contract.

10.2.10 The procedures for the translation, reproduction and destruction of the Classified Information which shall be in accordance with the requirements of Article 6.

10.3 The DSA or CSA of the Party of the country placing the Classified Contract shall pass two copies of the relevant parts of the Classified Contract to the DSA or CSA of the Party in whose country the Classified Contract has been placed, to allow adequate security monitoring.

10.4 Each Classified Contract shall contain guidance on the security requirements and on the classification of each aspect/element of the Classified Contract. In the United Kingdom the guidance shall be contained in a specific security clause in the Classified Contract and in a Security Aspects Letter. In the Republic of Turkey this guidance shall be set out in the Project Security Instruction. The guidance shall identify each classified aspect of the Classified Contract, or any classified aspect, which is to be generated by the Classified 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 any of the information has been declassified.

10.5 Classified Contracts that contain or relate to Classified Information no higher that UK OFFICIAL-SENSITIVE or HİZMETE ÖZEL level shall contain an appropriate security requirements clause to define the minimum security requirements to be applied by the Contractor for the protection of UK OFFICIAL-SENSITIVE or HİZMETE ÖZEL Classified Information that is either received or generated in the course of the Classified Contract.

ARTICLE 11

Security Cooperation

11.1 Each DSA or CSA shall notify the security status of a Facility in its country when requested by the other Party. Each DSA or CSA shall also notify the Personnel Security Clearance status of one of its nationals when so requested. These notifications shall be known as Facility Security Clearance (FSC) and Personnel Security Clearance (PSC) assurance respectively.

11.2 When requested, the DSA or CSA shall establish the security clearance status of the Facility/individual which is the subject of the enquiry and forward a FSC/PSC 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 security level than that which has been requested, notification shall be sent that the FSC/PSC assurance cannot be issued immediately, but that action is being taken to process the request. Following successful enquiries a FSC/PSC assurance shall be provided.

11.3 A Facility which is deemed by the DSA or CSA, in the country in which it is registered, to be under the ownership, control or influence of a Third Party whose aims are not compatible with those of the Host Party is not eligible for a FSC assurance and the requesting DSA or CSA shall be notified.

11.4 If either DSA or CSA learns of any derogatory information about an individual for whom a PSC assurance has been issued, it shall notify the other DSA or CSA of the nature of the information and the action it intends to take, or has taken. Either DSA or CSA may request a review of any PSC assurance which has been furnished earlier by the other DSA or CSA, provided that the request is accompanied by a reason. The requesting DSA or CSA shall be notified of the results of the review and any subsequent action.

11.5 If a Party becomes aware of information that raises doubts about the suitability of a Facility with a FSC that is located in the country of the other Party to continue to have access to Classified Information, then details of this information shall be promptly notified to the DSA or CSA of the other Party to allow an investigation to be carried out. The Party that provided the information shall be informed of the outcome of the investigation when it is completed.

11.6 If either DSA or 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 Party based upon a security clearance, the other Party shall be notified and given the reasons for such an action.

11.7 Each DSA or CSA may request the other to review any FSC assurance, provided that the request is accompanied by the reasons for seeking the review.

Following the review, the requesting DSA or CSA shall be notified of the results and shall be provided with facts supporting any decisions taken.

11.8 If required by the other Party each DSA or CSA shall co-operate in reviews and investigations concerning FSC's or PSCs.

11.9 Where required for Classified Contracts at the UK OFFICIAL-SENSITIVE and HIZMETE ÖZEL levels, a DSA or CSA of a Party may request the DSA or CSA of the other Party to provide a letter of authorisation following confirmation from a Contractor under its jurisdiction that it shall be compliant with the security requirements clause referenced in paragraph 10.5 of Article 10 and national security laws and regulations that are contained in the Contract. This authorisation letter replaces the requirement for an FSC for access to Classified Information at the level of UK OFFICIAL-SENSITIVE or HIZMETE ÖZEL.

ARTICLE 12

Loss or Compromise

12.1 In the event of a security incident involving the actual or suspected loss or compromise of Classified Information or suspicion that Classified Information has been disclosed to unauthorised persons or a Third Party, the DSA or CSA of the Recipient Party shall immediately inform the DSA or CSA of the Originating Party. Both Parties shall take any appropriate measures according to their national security laws and regulations to limit the consequences of any loss or compromise or unauthorised disclosure of the Classified Information.

12.2 In such circumstances an immediate investigation shall be carried out by the Recipient Party (with assistance from the Originating Party if required) in accordance with its national security laws and regulations for the protection of Classified Information. The Recipient Party shall inform the Originating Party about the circumstances, the outcome of the investigation and the measures adopted to prevent a recurrence as soon as is practicable.

ARTICLE 13

Financial Matters

Each Party shall cover its own expenses resulting from the implementation of the provisions of this Agreement.

ARTICLE 14

Amendment/Review

Amendments to or a review of this Agreement may be proposed by the DSA of either Party by written notification through diplomatic channels. If both Parties agree that amendment or a review is necessary negotiations shall be started as soon as practicable following the receipt of the written request. Any agreed amendments will enter into force on the date of the last written notification by which the Parties notify each other of the completion of their internal procedures required for the amendment to enter into force.

ARTICLE 15

Disputes

Any dispute between the Parties arising from the interpretation, application or implementation of this Agreement shall be resolved by consultation and negotiations between the Parties DSAs and shall not be referred to any national or international tribunal or Third Party for settlement.

ARTICLE 16

Termination

16.1 This Agreement may be terminated by mutual consent or unilaterally, to take effect after a period of six months following the date of the written notice to the other Party. Notification of an intention of a Party to terminate the Agreement shall be communicated through diplomatic channels. Both Parties shall remain responsible after termination for the safeguarding of all Classified Information exchanged under the provisions of this Agreement.

16.2 Any Classified Information which is exchanged, transferred or generated under cover of this Agreement shall also be safeguarded, even though its transfer may occur following notice by either of the Parties to terminate.

16.3 In the event of termination, solutions to any outstanding disputes shall be sought by consultation between the Parties.

ARTICLE 17

Effective Date/Signatures

17.1 This Agreement shall enter into force on the date of the receipt of the last written notification by which the Parties notify each other, through diplomatic channels, of the completion of their internal legal procedures required for its entry into force.

17.2 This Agreement shall remain in force for a period of five years and shall then be automatically renewed for five-year periods unless terminated by either Party in accordance with Article 16.

17.3 After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures so as to have this Agreement registered by Secretariat of the United Nations in accordance with Article 102 of the UN Charter. The other Party shall be notified of the registration and of the registration number in the UN Treaty Series as soon as the UN Secretariat has issued it.

17.4 Done at Ankara, on the twenty fifth day of February 2016, in duplicate in the English and Turkish languages, both texts being equally authentic.

for the Government of the United Kingdom of Great Britain and Northern Ireland:	**for the Government of the Republic of Turkey:**
RICHARD PETER MOORE	SABAN UMUT

ISBN 978-1-4741-3913-7