

DEFENSE

Security of Information

**Agreement Between
the UNITED STATES OF AMERICA
and the EUROPEAN UNION**

Signed at Washington April 30, 2007



NOTE BY THE DEPARTMENT OF STATE

Pursuant to Public Law 89—497, approved July 8, 1966
(80 Stat. 271; 1 U.S.C. 113)—

“ . . .the Treaties and Other International Acts Series issued under the authority of the Secretary of State shall be competent evidence . . . of the treaties, international agreements other than treaties, and proclamations by the President of such treaties and international agreements other than treaties, as the case may be, therein contained, in all the courts of law and equity and of maritime jurisdiction, and in all the tribunals and public offices of the United States, and of the several States, without any further proof or authentication thereof.”

EUROPEAN UNION

Defense: Security of Information

*Agreement signed at Washington April 30, 2007;
Entered into force April 30, 2007.*

AGREEMENT
BETWEEN
THE GOVERNMENT OF THE
UNITED STATES OF AMERICA
AND
THE EUROPEAN UNION
ON THE SECURITY
OF CLASSIFIED INFORMATION

USG/EU/en 1

USG/EU/en 2

THE GOVERNMENT OF THE UNITED STATES OF AMERICA, hereafter referred to as "the
USG"

and

THE EUROPEAN UNION, hereafter referred to as "the EU", hereafter referred to as "the Parties",

CONSIDERING THAT the USG and the EU share the objectives to strengthen their own security
in all ways and to provide their citizens with a high level of safety within an area of security,

CONSIDERING THAT the USG and the EU agree that consultations and co-operation should be
developed between them on questions of common interest relating to security,

CONSIDERING THAT, in this context, a permanent need therefore exists to exchange classified
information between the USG and the EU,

RECOGNISING THAT full and effective consultation and co-operation may require access to USG
and EU classified information, as well as the exchange of classified information between the USG
and the EU,

CONSCIOUS THAT such access to and exchange of classified information requires appropriate
security measures,

HAVE AGREED AS FOLLOWS:

ARTICLE 1

Scope

1. This Agreement shall apply to classified information provided or exchanged between the Parties.
2. Each Party shall protect classified information received from the other Party, in particular against unauthorised disclosure, in accordance with the terms set forth herein and in accordance with the Parties' respective laws and regulations.

ARTICLE 2

Definitions

1. For the purpose of this Agreement "the EU" shall mean the Council of the European Union (hereafter referred to as "the Council"), the Secretary-General/High Representative and the General Secretariat of the Council, and the Commission of the European Communities (hereafter referred to as "the European Commission").

2. For the purpose of this Agreement "classified information" shall mean information and material subject to this Agreement (i) the unauthorised disclosure of which could cause varying degrees of damage or harm to the interests of the USG, or of the EU or one or more of its Member States; (ii) which requires protection against unauthorised disclosure in the security interests of the USG or the EU; and (iii) which bears a security classification assigned by the USG or the EU. The information may be in oral, visual, electronic, magnetic or documentary form, or in the form of material, including equipment or technology.

ARTICLE 3

Security classifications

1. Classified information shall be marked as follows:
 - (a) For the USG, classified information shall be marked TOP SECRET, SECRET or CONFIDENTIAL.
 - (b) For the EU, classified information shall be marked TRES SECRET UE/EU TOP SECRET, SECRET UE, CONFIDENTIEL UE or RESTREINT UE.

2. The corresponding security classifications are:

| In the European Union | In the United States of America |
|------------------------------|---------------------------------|
| TRES SECRET UE/EU TOP SECRET | TOP SECRET |
| SECRET UE | SECRET |
| CONFIDENTIEL UE | CONFIDENTIAL |
| RESTREINT UE | (No U.S. equivalent) |

3. Classified information provided by one Party to the other shall be stamped, marked or designated with the name of the releasing Party. Classified information provided by one Party shall be protected by the recipient Party in a manner at least equivalent to that afforded to it by the releasing Party.

ARTICLE 4

Protection of classified information

1. Each Party shall have a security system and security measures in place based on the basic principles and minimum standards of security laid down in its respective laws and regulations, in order to ensure that an equivalent level of protection is applied to classified information. On request, each Party shall provide the other Party with information about its security standards, procedures and practices, including training, for safeguarding classified information.

2. The recipient Party shall afford classified information received from the releasing Party a degree of protection at least equivalent to that afforded it by the releasing Party.
3. The recipient Party shall not use or permit the use of classified information for any other purpose than that for which it was provided without the prior written approval of the releasing Party.
4. The recipient Party shall not further release or disclose classified information without the prior written approval of the releasing Party.
5. The recipient Party shall comply with any limitations on the further release of classified information as may be specified by the releasing Party when it discloses it.
6. The recipient Party shall ensure that the rights of the originator of classified information provided or exchanged under this Agreement, as well as intellectual property rights such as patents, copyrights or trade secrets, are adequately protected.
7. No individual shall be entitled to have access to classified information received from the other Party solely by virtue of rank, appointment, or security clearance. Access to classified information shall be granted only to those individuals whose official duties require such access and who, where needed, have been granted the requisite personnel security clearance in accordance with the prescribed standards of the Parties.

8. The recipient Party shall ensure that all individuals having access to classified information are informed of their responsibilities to protect the information in accordance with applicable laws and regulations.

ARTICLE 5

Personnel security clearances

1. The Parties shall ensure that all persons who in the conduct of their official duties require access, or whose duties or functions may afford access, to information classified CONFIDENTIEL UE or CONFIDENTIAL or above provided or exchanged under this Agreement are appropriately security-cleared before they are granted access to such information.
2. The determination by a Party on the granting of a personnel security clearance to an individual shall be consistent with that Party's security interests and shall be based upon all available information indicating whether the individual is of unquestionable loyalty, integrity, and trustworthiness.
3. Each Party's security clearances shall be based on an appropriate investigation conducted in sufficient detail to provide assurance that the criteria referred to in paragraph 2 have been met with respect to any individual to be granted access to classified information. For the EU, the parent government National Security Authority (NSA) of the individual concerned is the competent authority responsible for conducting the necessary security investigations on its nationals.

ARTICLE 6

Transfer of custody

The releasing Party shall ensure that all classified information is adequately protected until custody of the information is transferred to the recipient Party. The recipient Party shall ensure that all classified information of the other Party is adequately protected as soon as it has custody of the information released to it.

ARTICLE 7

Security of facilities and establishments of the Parties
where classified information is kept

In accordance with applicable laws and regulations, each Party shall ensure the security of facilities and establishments where classified information released to it by the other Party is kept, and shall ensure for each such facility or establishment that all necessary measures are taken to control and protect the information.

ARTICLE 8

Release of classified information to contractors

1. Classified information received from the other Party may be provided to a contractor or prospective contractor with the prior written consent of the releasing Party. Prior to the release or disclosure to a contractor or prospective contractor of any classified information received from the other Party, the recipient Party shall ensure that such contractor or prospective contractor, and the contractor's facility, have the capability to protect the information and have an appropriate clearance.
2. This Article shall not apply to personnel engaged by the European Union under a contract of employment or by the United States under a personal services contract.

ARTICLE 9

Transmission

1. Classified information shall be transmitted between the Parties through mutually agreed channels.

For the purposes of this Agreement:

- (a) As regards the EU, all classified information in written form shall be sent to the Chief Registry Officer of the Council of the European Union. All such information shall be forwarded by the Chief Registry Officer of the Council to the Member States and to the European Commission, subject to paragraph 3;
- (b) As regards the USG, all classified information in written form shall be sent, unless otherwise provided for, via the Mission of the United States of America to the European Union, at the following address:

Mission of the United States of America to the European Union
Registry Officer
Rue Zinner 13
B-1000 Brussels

2. The electronic transmission of classified information up to the level CONFIDENTIAL/CONFIDENTIEL UE between the USG and the EU and between the EU and the USG shall be encrypted in accordance with the releasing Party's requirements as outlined in its security policies and regulations. The releasing Party's requirements shall be met when transmitting, storing and processing classified information in internal networks of the Parties.

3. Exceptionally, classified information from one Party which is accessible to only specific competent officials, organs or services of that Party may, for operational reasons, be addressed and be accessible to only specific officials, organs or services of the other Party specifically designated as recipients, taking into account their competences and according to the need-to-know principle. As far as the EU is concerned, such information shall be transmitted through the Chief Registry Officer of the Council, or the Chief Registry Officer of the European Commission Security Directorate when such information is addressed to the European Commission.

ARTICLE 10

Visits to facilities and establishments of the Parties

When required, the Parties shall confirm personnel security clearances through mutually agreed channels for visits by representatives of one Party to facilities and establishments of the other Party.

ARTICLE 11

Reciprocal security visits

Implementation of the security requirements set out in this Agreement may be verified through reciprocal visits by security personnel of the Parties with a view to evaluating the effectiveness of measures taken under this Agreement and the technical security arrangement to be established pursuant to Article 13 to protect classified information provided or exchanged between the Parties. Accordingly, security representatives of each Party, after prior consultation, may be permitted to visit the other Party and to discuss and observe the implementing procedures of the other Party. The host Party shall assist the visiting security representatives in determining whether classified information received from the visiting Party is being protected adequately.

ARTICLE 12

Oversight

1. For the USG, the Secretaries of State and Defense and the Director of National Intelligence shall oversee the implementation of this Agreement.
2. For the EU, the Secretary-General of the Council and the Member of the Commission responsible for security matters shall oversee the implementation of this Agreement.

ARTICLE 13

Technical security arrangement

1. In order to implement this Agreement, a technical security arrangement shall be established among the three authorities designated in paragraphs 2 to 4 in order to lay down the standards for the reciprocal security protection of classified information provided or exchanged between the Parties under this Agreement.
2. The U.S. Department of State, acting in the name of the USG and under its authority, shall be responsible for developing the technical security arrangement mentioned in paragraph 1 for the protection and safeguarding of classified information provided to or exchanged with the USG under this Agreement.
3. The Security Office of the General Secretariat of the Council, under the direction and on behalf of the Secretary-General of the Council, acting in the name of the Council and under its authority, shall be responsible for developing the technical security arrangement mentioned in paragraph 1 for the protection and safeguarding of classified information provided to or exchanged with the Council or the General Secretariat of the Council under this Agreement.

4. The European Commission Security Directorate, acting under the authority of the Member of the Commission responsible for security matters, shall be responsible for developing the technical security arrangement mentioned in paragraph 1 for the protection of classified information provided or exchanged under this Agreement with the European Commission.

5. For the EU, the arrangement shall be subject to approval by the Council Security Committee.

ARTICLE 14

Downgrading and declassification

1. The Parties agree that classified information should be downgraded in classification as soon as information ceases to require that higher degree of protection or should be declassified as soon as the information no longer requires protection against unauthorised disclosure.

2. The releasing Party has complete discretion concerning downgrading or declassification of its own classified information. The recipient Party shall not downgrade the security classification or declassify classified information received from the other Party, notwithstanding any apparent declassification instructions on the document, without the prior written consent of the releasing Party.

ARTICLE 15

Loss or compromise

The releasing Party shall be informed upon discovery of any proven or suspected loss or compromise of its classified information, and the recipient Party shall initiate an investigation to determine the circumstances. The results of the investigation and information regarding measures taken to prevent recurrence shall be forwarded to the releasing Party. The authorities referred to in Article 13 may establish procedures to that effect.

ARTICLE 16

Dispute settlement

Any differences between the Parties arising under or relating to this Agreement shall be settled solely through consultations between the Parties.

ARTICLE 17

Costs

Each Party shall be responsible for bearing its own costs incurred in implementing this Agreement.

ARTICLE 18

Ability to protect

Prior to the provision or exchange of classified information between the Parties, the responsible security authorities referred to in Article 12 must agree that the recipient Party is able to protect and safeguard the information subject to this Agreement in a way consistent with the technical security arrangement to be established pursuant to Article 13.

ARTICLE 19

Other agreements

Nothing in this Agreement shall alter existing agreements or arrangements between the Parties, nor agreements between the USG and Member States of the European Union. This Agreement shall not preclude the Parties from concluding other Agreements relating to the provision or exchange of classified information subject to this Agreement provided they are not incompatible with the obligations under this Agreement.

ARTICLE 20

Entry into force, amendment and denunciation

1. This Agreement shall enter into force on the date of the last signature by the Parties.
2. Each Party shall notify the other Party of any changes in its laws and regulations that could affect the protection of classified information referred to in this Agreement. In such cases, the Parties shall consult with a view to amending this Agreement as necessary in accordance with paragraph 3.

3. Amendments to the present Agreement shall be made by mutual written agreement of the Parties.

4. Either Party may denounce this Agreement by notifying the other Party, in writing, ninety days in advance of its intention to denounce the Agreement. Notwithstanding the denunciation of this Agreement, all classified information provided pursuant to this Agreement shall continue to be protected in accordance with this Agreement. The Parties shall consult immediately on the disposition of such classified information.

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

Done at Washington this thirtieth day of April 2007 in two copies, each in the English language.

FOR THE GOVERNMENT
OF THE UNITED STATES
OF AMERICA



FOR THE EUROPEAN UNION

