

**No. 47944\***

---

**European Union  
and  
United States of America**

**Agreement between the European Union and the Government of the United States of America on the security of classified information. Washington, 30 April 2007**

**Entry into force:** 30 April 2007 by signature, in accordance with article 20

**Authentic text:** *English*

**Registration with the Secretariat of the United Nations:** *Council of the European Union, 4 October 2010*

\*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.

---

**Union européenne  
et  
États-Unis d'Amérique**

**Accord entre l'Union européenne et le Gouvernement des États-Unis d'Amérique concernant la sécurité d'informations classifiées. Washington, 30 avril 2007**

**Entrée en vigueur :** 30 avril 2007 par signature, conformément à l'article 20

**Texte authentique :** *anglais*

**Enregistrement auprès du Secrétariat des Nations Unies :** *Conseil de l'Union européenne, 4 octobre 2010*

\* 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 ]

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

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 EUROPEAN UNION



FOR THE GOVERNMENT  
OF THE UNITED STATES  
OF AMERICA



[TRANSLATION – TRADUCTION]

## ACCORD ENTRE L'UNION EUROPÉENNE ET LE GOUVERNEMENT DES ÉTATS-UNIS D'AMÉRIQUE SUR LA SÉCURITÉ DES INFORMATIONS CLASSIFIÉES

Le Gouvernement des États-Unis d'Amérique, ci-après dénommé « l'USG » et l'Union européenne, ci-après dénommée « l'UE », dénommés conjointement « les Parties »,

Considérant que l'USG et l'UE ont en commun les objectifs consistant à renforcer leur propre sécurité par tous les moyens et à offrir à leurs citoyens un niveau élevé de sécurité à l'intérieur d'un espace de sécurité,

Considérant que l'USG et l'UE estiment qu'il convient de développer les consultations et la coopération entre elles sur des questions d'intérêt commun portant sur la sécurité,

Considérant que, dans ce contexte, il existe par conséquent un besoin permanent d'échanger des informations classifiées entre l'USG et l'UE,

Reconnaissant que des consultations et une coopération optimales et effectives peuvent exiger l'accès à des informations classifiées de l'USG et l'UE, ainsi que l'échange d'informations classifiées entre l'USG et l'UE,

Conscients du fait qu'un tel accès et un tel échange d'informations classifiées exigent des mesures de sécurité appropriées,

Sont convenus de ce qui suit :

### *Article premier. Champ d'application*

1. Le présent Accord s'applique aux informations classifiées fournies ou échangées entre les Parties.

2. Chaque Partie protège les informations classifiées qu'elle reçoit de l'autre Partie, en particulier contre la divulgation non autorisée, conformément aux dispositions du présent Accord et aux lois et réglementations respectives des Parties.

### *Article 2. Définitions*

1. Aux fins du présent Accord, « l'UE » désigne le Conseil de l'Union européenne (ci-après dénommé « le Conseil »), le Secrétaire général/Haut représentant et le Secrétariat général du Conseil, ainsi que la Commission des Communautés européennes (ci-après dénommée « la Commission européenne »).

2. Aux fins du présent Accord, on entend par « informations classifiées » les informations et le matériel visés par le présent Accord (i) dont la divulgation non autorisée pourrait, à différents degrés, porter préjudice aux intérêts de l'USG ou de l'UE ou d'au moins l'un de ses États membres; (ii) qui doivent être protégés contre une divulgation

non autorisée afin de préserver les intérêts de l'USG ou de l'UE en matière de sécurité; et (iii) qui comportent une classification de sécurité attribuée par l'USG ou par l'UE. Ces informations peuvent être orales, visuelles, électroniques, magnétiques ou documentaires, ou se présenter sous forme de matériel, y compris l'équipement ou la technologie.

### *Article 3. Classifications de sécurité*

1. Les informations classifiées portent les mentions suivantes :

a) Pour l'USG, les informations classifiées portent les mentions TOP SECRET, SECRET ou CONFIDENTIAL.

b) Pour l'UE, les informations classifiées portent les mentions, TRÈS SECRET UE/EU TOP SECRET, SECRET UE, CONFIDENTIEL UE ou RESTREINT UE.

2. Les classifications de sécurité et leurs correspondances sont les suivantes :

Dans l'Union européenne	Aux États-Unis d'Amérique
TRÈS SECRET UE/EU TOP SECRET	TOP SECRET
SECRET UE	SECRET
CONFIDENTIEL UE	CONFIDENTIAL
RESTREINT UE	(Pas d'équivalent aux États-Unis)

3. Les informations classifiées communiquées par une Partie à l'autre doivent être assorties d'un cachet, d'une mention ou autre indication portant le nom de la Partie émettrice. Les informations classifiées communiquées par une Partie à l'autre sont protégées par la Partie destinataire à un degré au moins équivalent à celui que leur accorde la Partie émettrice.

### *Article 4. Protection des informations classifiées*

1. Chaque Partie dispose d'un système de sécurité et de mesures de sécurité répondant aux principes fondamentaux et aux normes minimales de sécurité définies dans sa législation et sa réglementation de manière qu'un niveau équivalent de protection soit appliqué aux informations classifiées. Chaque Partie communique à l'autre Partie, à la demande de celle-ci, les informations relatives aux normes, aux procédures et aux pratiques qu'elle applique ainsi qu'aux formations qu'elle dispense en matière de sécurité aux fins de protection des informations classifiées.

2. La Partie destinataire accorde aux informations classifiées qui lui ont été communiquées par la Partie émettrice un niveau de protection au moins équivalent à celui que leur accorde la Partie émettrice.

3. La Partie destinataire ne peut utiliser des informations classifiées ou en autoriser l'utilisation à des fins autres que celles qui ont été prévues, sans l'accord préalable écrit de la Partie émettrice.

4. La Partie destinataire s'abstient de communiquer ou de divulguer des informations classifiées sans l'accord préalable écrit de la Partie émettrice.

5. La Partie destinataire respecte toute restriction concernant la transmission d'informations classifiées que la Partie émettrice aura spécifiée au moment de la communication desdites informations.

6. La Partie destinataire veille à ce que les droits de l'autorité d'origine des informations classifiées communiquées ou échangées en vertu du présent Accord, de même que les droits de propriété intellectuelle tels que les brevets, les droits d'auteur et les secrets professionnels soient dûment protégés.

7. Nul ne peut avoir accès aux informations classifiées reçues par l'autre Partie uniquement en raison de son rang, d'une nomination ou d'une habilitation de sécurité. L'accès aux informations classifiées est réservé aux personnes dont les fonctions officielles nécessitent un tel accès et qui, le cas échéant, se sont vu accorder l'habilitation de sécurité du personnel nécessaire conformément aux normes prescrites par les Parties.

8. La Partie destinataire veille à ce que toute personne ayant accès aux informations classifiées soit informée de la responsabilité qui lui incombe en matière de protection des informations conformément aux lois et aux règlements en vigueur.

#### *Article 5. Habilitations de sécurité du personnel*

1. Les Parties veillent à ce que toute personne qui, dans l'exercice de ses fonctions officielles, a besoin d'accéder ou, en raison de ses tâches ou fonctions, peut avoir accès à des informations classées CONFIDENTIEL UE ou CONFIDENTIEL ou d'un niveau de confidentialité supérieur, qui sont communiquées ou échangées en vertu du présent Accord, possède une habilitation de sécurité appropriée avant d'être autorisée à accéder à ces informations.

2. La décision par laquelle une Partie octroie une habilitation de sécurité du personnel à une personne doit être compatible avec les intérêts de cette Partie en matière de sécurité et se fonder sur toutes les informations disponibles permettant de déterminer si la personne concernée est d'une loyauté, d'une intégrité et d'une fiabilité irréprochables.

3. Les habilitations de sécurité octroyées par les Parties se fondent sur une enquête appropriée, menée de manière suffisamment détaillée pour s'assurer que toute personne devant obtenir l'accès à des informations classifiées remplit les critères visés au paragraphe 2. En ce qui concerne l'UE, l'autorité compétente pour mener les enquêtes de sécurité nécessaires sur ses ressortissants est l'Autorité nationale de sécurité (ANS) de l'État dont est issue la personne concernée.

#### *Article 6. Transfert de l'obligation de protection*

La Partie émettrice veille à ce que toutes les informations classifiées soient dûment protégées jusqu'à leur transfert à la Partie destinataire. La Partie destinataire veille à ce que toutes les informations classifiées que lui communique l'autre Partie soient dûment protégées dès qu'elle se trouve en leur possession.

#### *Article 7. Sécurité des installations et des établissements des Parties dans lesquels sont conservées les informations classifiées*

Conformément aux lois et aux règlements applicables, chaque Partie veille à la sécurité des installations et des établissements dans lesquels sont conservées les informations classifiées qui lui ont été communiquées par l'autre Partie et s'assure que toutes les mesu-

res nécessaires ont été prises dans les installations ou établissements en question pour contrôler et protéger les informations.

*Article 8. Communication d'informations classifiées à des contractants*

1. Les informations classifiées communiquées par l'autre Partie peuvent être transmises à un contractant ou à un contractant potentiel avec le consentement préalable écrit de la Partie émettrice. Avant la communication ou la divulgation à un contractant ou à un contractant potentiel de toute information classifiée émanant de l'autre Partie, la Partie destinataire doit s'assurer que ledit contractant ou contractant potentiel ainsi que ses installations sont en mesure de protéger les informations et qu'ils possèdent une habilitation appropriée.

2. Le présent article ne s'applique pas au personnel engagé par l'Union européenne dans le cadre d'un contrat de travail ou par le Gouvernement des États-Unis dans le cadre d'un contrat de services personnels.

*Article 9. Transmission*

1. Les informations classifiées sont transmises entre les Parties par le biais de canaux choisis d'un commun accord.

Aux fins du présent accord :

a) En ce qui concerne l'UE, toutes les informations classifiées se présentant sous forme écrite sont envoyées au Chief Registry Officer du Conseil de l'Union européenne. Sous réserve des dispositions du paragraphe 3, le Chief Registry Officer du Conseil transmet toutes ces informations aux États membres et à la Commission européenne;

b) En ce qui concerne l'USG, toutes les informations classifiées se présentant sous forme écrite sont transmises, sauf disposition contraire, par le biais de la Mission des États-Unis d'Amérique auprès de l'Union européenne, à l'adresse suivante :

Mission des États-Unis d'Amérique auprès de l'Union européenne

Registry Officer

Rue Zinner 13

B-1000 Bruxelles

2. La transmission électronique d'informations classifiées jusqu'au niveau CONFIDENTIEL/CONFIDENTIEL UE entre l'USG et l'UE et entre l'UE et l'USG est cryptée conformément aux exigences énoncées dans les orientations et dispositions réglementaires en matière de sécurité de la Partie émettrice. Les exigences de la Partie émettrice doivent être respectées lors de la transmission, du stockage et du traitement des informations classifiées dans les réseaux internes des Parties.

3. Exceptionnellement, les informations classifiées d'une Partie à laquelle n'ont accès que certains agents, organes ou services compétents de cette Partie peuvent, pour des raisons opérationnelles, n'être adressées et n'être accessibles qu'à certains agents, organes ou services de l'autre Partie spécifiquement désignés comme destinataires, compte tenu de leurs compétences et selon le principe du « besoin de connaître ». En ce qui concerne

l'UE, ces informations sont transmises par l'intermédiaire du Chief Registry Officer du Conseil ou par le Chief Registry Officer de la Direction de la sécurité de la Commission européenne lorsque ces informations sont adressées à la Commission européenne.

*Article 10. Visites des installations et des établissements des Parties*

S'il y a lieu, les Parties confirment les habilitations de sécurité du personnel par le biais de canaux choisis d'un commun accord, lorsque les représentants d'une Partie visitent les installations et les établissements de l'autre Partie.

*Article 11. Visites réciproques de sécurité*

La mise en œuvre des exigences de sécurité définies dans le présent Accord peut être vérifiée par le biais de visites réciproques effectuées par le personnel de sécurité des Parties dans le but d'évaluer l'efficacité des mesures prises en vertu du présent Accord et de l'arrangement technique de sécurité à conclure en vertu de l'article 13, afin de protéger les informations classifiées communiquées ou échangées entre les Parties. En conséquence, les représentants de la sécurité de chacune des Parties peuvent, après consultation préalable, être autorisés à se rendre chez l'autre Partie pour examiner avec elle et pour observer les procédures d'exécution que celle-ci a mises en place. La Partie hôte aide les représentants de la sécurité effectuant la visite à déterminer si les informations classifiées communiquées par la Partie effectuant la visite sont correctement protégées.

*Article 12. Surveillance*

1. En ce qui concerne l'USG, la mise en œuvre du présent Accord est surveillée par le Secrétaire d'État, le Secrétaire à la défense et le Directeur du renseignement national.
2. En ce qui concerne l'UE, la mise en œuvre du présent Accord est surveillée par le Secrétaire général du Conseil et les membres de la Commission chargés des questions de sécurité.

*Article 13. Arrangement technique de sécurité*

1. Aux fins de l'application du présent Accord, un arrangement technique de sécurité est conclu entre les trois autorités désignées aux paragraphes 2 à 4 afin de définir les normes de sécurité pour la protection réciproque des informations classifiées communiquées ou échangées entre les Parties en vertu du présent accord.

2. Le Département d'État des États-Unis, agissant au nom et sous l'autorité de l'USG, est responsable de l'élaboration de l'arrangement technique de sécurité visé au paragraphe 1 pour la protection et la sauvegarde des informations classifiées communiquées ou échangées avec l'USG au titre du présent Accord.

3. Le bureau de sécurité du Secrétariat général du Conseil, sous la direction et pour le compte du Secrétaire général du Conseil, agissant au nom du Conseil et sous son autorité, est responsable de l'élaboration des dispositions techniques de sécurité visées au pa-



ragraphe 1 pour la protection et la sauvegarde des informations classifiées communiquées ou échangées avec le Conseil ou le Secrétariat général du Conseil au titre du présent Accord.

4. La direction de la sécurité de la Commission européenne, agissant sous l'autorité du membre de la Commission chargé des questions de sécurité, est responsable de l'élaboration de l'arrangement technique de sécurité visé au paragraphe 1 pour la protection des informations classifiées communiquées ou échangées avec la Commission européenne au titre du présent Accord.

5. En ce qui concerne l'UE, ces dispositions sont soumises à l'approbation du Comité de sécurité du Conseil.

#### *Article 14. Déclassement et déclassification*

1. Les Parties conviennent que les informations classifiées devraient être déclassées dès qu'elles ne nécessitent plus un niveau de protection aussi élevé et qu'elles devraient être déclassifiées dès lors qu'elles ne doivent plus être protégées contre une divulgation non autorisée.

2. La Partie émettrice a toute latitude pour déclasser ou déclassifier ses propres informations classifiées. La Partie destinataire ne peut, sans l'accord préalable écrit de la Partie émettrice, déclasser la classification de sécurité ou déclassifier les informations classifiées qui lui ont été communiquées par l'autre Partie, indépendamment de toute instruction de déclassification figurant sur le document.

#### *Article 15. Perte ou compromis*

La Partie émettrice est informée de toute perte ou compromission avérée ou présumée de ses informations classifiées, et la Partie destinataire ouvre une enquête pour en déterminer les circonstances. Les résultats de cette enquête ainsi que les informations relatives aux mesures prises pour empêcher le renouvellement d'un tel incident sont communiquées à la Partie émettrice. Les autorités visées à l'article 13 peuvent mettre en place des procédures à cet effet.

#### *Article 16. Règlement des différends*

Tout différend entre les Parties découlant du présent Accord ou y relatif est réglé uniquement par voie de consultation entre les Parties.

#### *Article 17. Coûts*

Chaque Partie supporte les coûts occasionnés par la mise en œuvre du présent Accord qui lui incombent.

*Article 18. Capacité à assurer la protection des informations*

Préalablement à toute communication ou à tout échange d'informations classifiées entre les Parties, les autorités chargées de la sécurité visées à l'article 12 doivent déterminer d'un commun accord que la Partie destinataire est en mesure d'assurer la protection et la sauvegarde des informations visées par le présent Accord dans le respect des dispositions de l'arrangement technique de sécurité qui doit être conclu en application de l'article 13.

*Article 19. Autres accords*

Aucune disposition du présent Accord ne peut modifier les accords ou conventions existant entre les Parties, ni les accords entre l'USG et des États membres de l'Union européenne. Le présent Accord n'empêche pas les Parties de conclure d'autres accords concernant la communication ou l'échange d'informations classifiées visées par le présent Accord, pour autant que lesdits accords ne soient pas incompatibles avec les obligations au titre du présent Accord.

*Article 20. Entrée en vigueur, modification et dénonciation*

1. Le présent Accord entre en vigueur à la date de la dernière signature par les Parties.

2. Chaque Partie notifie à l'autre Partie toute modification apportée à sa législation ou à sa réglementation susceptible de compromettre la protection d'informations classifiées visées dans le présent Accord. Dans un tel cas, les Parties se consultent en vue de modifier, s'il y a lieu, le présent Accord conformément au paragraphe 3.

3. Toute modification du présent Accord doit faire l'objet d'un accord écrit entre les Parties.

4. Chaque Partie peut dénoncer le présent accord par notification écrite adressée à l'autre Partie, quatre-vingt-dix (90) jours avant la date à laquelle elle entend dénoncer l'Accord. Nonobstant la dénonciation du présent Accord, l'ensemble des informations classifiées communiquées en application du présent Accord continue d'être protégé selon les dispositions de celui-ci. Les Parties se consultent immédiatement quant au sort à réserver à ces informations classifiées.

EN FOI DE QUOI, les soussignés, dûment autorisés à cet effet par leurs autorités respectives, ont signé le présent Accord.

FAIT à Washington, le 30 avril 2007, en deux exemplaires, chacun en langue anglaise.

Pour l'Union européenne :

Pour le Gouvernement des États-Unis d'Amérique :