No. 44256

France
and
Italy

General Security Agreement between the Government of the French Republic and the Government of the Italian Republic concerning the protection of classified information exchanged between the two countries. Rome, 25 July 2006

Entry into force: *1 June 2007 by notification, in accordance with article 13*

Authentic texts: *French and Italian*

Registration with the Secretariat of the United Nations: *France, 27 August 2007*

France
et
Italie

Accord général de sécurité entre le Gouvernement de la République française et le Gouvernement de la République italienne relatif à la protection des informations classifiées échangées entre les deux pays. Rome, 25 juillet 2006

Entrée en vigueur : *1er juin 2007 par notification, conformément à l'article 13*

Textes authentiques : *français et italien*

Enregistrement auprès du Secrétariat des Nations Unies : *France, 27 août 2007*

[FRENCH TEXT – TEXTE FRANÇAIS]

ACCORD GÉNÉRAL DE SÉCURITE ENTRE LE GOUVERNEMENT DE LA RÉPUBLIQUE FRANÇAISE ET LE GOUVERNEMENT DE LA REPUBLIQUE ITALIENNE RELATIF À LA PROTECTION DES INFORMATIONS CLASSIFIÉES ÉCHANGÉES ENTRE LES DEUX PAYS

PRÉAMBULE

Le Gouvernement de la République française et le Gouvernement de la République italienne, également dénommés les Parties aux fins du présent Accord, souhaitant garantir la protection des Informations classifiées, dont la responsabilité incombe à leurs Autorités de sécurité compétentes respectives, échangées entre les deux Parties ou transmises entre des organismes commerciaux et industriels de chacune des deux Parties, par des voies approuvées, sont convenus, dans l'intérêt de la sécurité nationale, des dispositions suivantes établies dans le présent Accord Général de Sécurité (AGS).

L'AGS intègre les exigences relatives à la sécurité du chapitre 4 de l'Accord cadre, dénommé « Accord cadre », conclu entre la République française, la République fédérale d'Allemagne, la République italienne, le Royaume d'Espagne, le Royaume de Suède et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord relatif aux mesures visant à faciliter la restructuration et le fonctionnement de l'industrie européenne de défense, fait à Farnborough le 27 juillet 2000.

Article 1. Définitions

Aux fins du présent AGS il faut entendre par :

1.1 « Informations classifiées » tout élément, matériel ou document classifié, quelle qu'en soit la forme, qu'il s'agisse d'une communication orale ou visuelle dont le contenu est classifié ou de la transmission électrique ou électronique d'un message classifié, ou sous une forme quelconque qui nécessite une protection contre une divulgation non autorisée.

1.2 « Contractant » une personne physique ou une personne morale disposant du pouvoir juridique de conclure des contrats.

1.3 « Contrat classé » un contrat qui contient ou implique la connaissance d'Informations classifiées.

1.4 « ANS/ASD » les Autorités nationales de sécurité/Autorités de sécurité désignées qui sont les autorités compétentes en ce qui concerne le contrôle et la mise en œuvre du présent AGS.

1.5 « Partie d'origine » la Partie, y compris tout autre organisme public ou privé placé sous sa juridiction, produisant les Informations classifiées.

1.6 « Partie destinataire » la Partie, y compris tout autre organisme public/privé placé sous sa juridiction, à laquelle les Informations classifiées sont transmises.

Article 2. Tableau d'équivalence

2.1 Aux fins des présentes dispositions, les classifications de sécurité et leurs équivalents dans les deux pays sont :

RÉPUBLIQUE FRANÇAISE	RÉPUBLIQUE ITALIENNE
TRÈS SECRET DÉFENSE	SEGRETISSIMO
SECRET DÉFENSE	SEGRETO
CONFIDENTIEL DÉFENSE	RISERVATISSIMO
voir paragraphe 2.2 ci-dessous	RISERVATO

2.2 Aux fins du présent Accord la République française traite et protège les informations portant la mention "RISERVATO" transmises par l'Italie selon ses lois et réglementations nationales, en accord avec le niveau minimal de sécurité agréé par les Parties.

La République italienne traite et protège les informations revêtues d'une mention de protection telles que "DIFFUSION RESTREINTE" transmises par la France selon ses lois et réglementations nationales, en accord avec le niveau minimal de sécurité agréé par les Parties.

2.3 Des informations exigeant une distribution limitée et des contrôles d'accès sont échangées lorsqu'elles portent de telles indications. Toutefois, dans ce cas, les Parties déterminent mutuellement les mesures de sécurité à appliquer.

Article 3. Autorites de sécurité compétentes

3.1 Les Autorités du gouvernement responsables de garantir la mise en œuvre et le contrôle du présent AGS sont, pour chacune des Parties :

Pour la République française :
Secrétariat Général de la Défense Nationale
51, Boulevard de la Tour-Maubourg
75700 Paris 07SP

Pour la République italienne :
Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
CESlS III REPARTO-UCSI
Via di Santa Susanna ,15
00187 Roma

3.2 Les Autorités susmentionnées s'informent réciproquement des organismes subordonnés responsables des domaines spécifiques, conformément aux dispositions du présent AGS.

Article 4. Restrictions imposées à l'utilisation et la divulgation

4.1 À moins que les Parties n'en soient convenues différemment, la Partie destinataire ne divulgue ni n'utilise, ni ne permet la divulgation ou l'utilisation de toute Information classifiée qui lui est communiquée par l'autre Partie, excepté à des fins et avec les restrictions indiquées par ou au nom de la Partie d'origine.

4.2 La Partie destinataire ne transmet pas à un quelconque État tiers, ou organisation internationale, une quelconque Information classifiée ou matériel, fourni en vertu des dispositions du présent AGS, ni ne divulgue publiquement une quelconque Information classifiée sans l'accord écrit préalable de la Partie d'origine.

Article 5. Protection des informations classifiées

5.1 La Partie d'origine :

a. s'assure que la Partie destinataire est informée de la classification des informations et de toute condition de communication ou restriction imposée à leur utilisation;

b. s'assure que les documents sont dûment marqués;

c. s'assure que la Partie destinataire est informée de tout changement de classification ultérieur.

5.2 La Partie destinataire :

a. conformément à ses lois et réglementations nationales, accorde à toute information et reçue de l'autre Partie le niveau de protection de sécurité qui est attribué à ses propres Informations classifiées bénéficiant d'une classification équivalente;

b. s'assure que les Informations classifiées sont marquées avec leur propre classification nationale équivalente, conformément au paragraphe 2.1 ci-dessus;

c. s'assure que les classifications ne sont pas modifiées, sauf autorisation écrite préalable de la Partie d'origine.

5.3 Afin d'atteindre et de conserver des normes de sécurité comparables, chaque ANS/ASD, sur demande, fournit à l'autre des informations sur ses normes de sécurité,

procédures et pratiques de protection des Informations classifiées et permet, à ces fins, des visites par les Autorités de sécurité compétentes.

Article 6. Accès aux informations classifiées

6.1 L'accès aux Informations classifiées est limité aux personnes qui ont un « besoin d'en connaître » et qui ont été précédemment habilitées par une ANS/ASD des Parties, conformément à leurs normes nationales, au niveau approprié à la classification des informations auxquelles il est souhaité d'accéder.

6.2 L'accès aux Informations classifiées de niveau TRÈS SECRET DÉFENSE/SEGRETISSIMO par une personne ayant exclusivement la nationalité d'une Partie du présent AGS peut être accordé sans l'autorisation préalable de la Partie d'origine.

6.3 L'accès aux Informations classifiées de niveau SECRET DÉFENSE/SEGRETO et de niveau CONFIDENTIEL DÉFENSE/RISERVATISSIMO par une personne ayant exclusivement la nationalité des Parties peut être accordé sans l'autorisation préalable de la Partie d'origine. Cette disposition s'applique également aux ressortissants des Parties signataires de l'« Accord cadre ».

6.4 L'accès aux Informations classifiées de niveau SECRET DÉFENSE/SEGRETO et de niveau CONFIDENTIEL DÉFENSE/RISERVATISSIMO par une personne ayant la double nationalité de l'une des Parties du présent AGS et d'une Partie signataire de l'« Accord cadre » ou d'un État membre de l'Union européenne est accédé sans autorisation préalable de la Partie d'origine. Tout autre accès non couvert par les paragraphes 6.2 à 6.4 doit suivre le processus de consultation décrit au paragraphe 6.5 ci-dessous.

6.5 L'accès aux Informations classifiées de niveau SECRET DÉFENSE/SEGRETO et de niveau CONFIDENTIEL DÉFENSE/RISERVATISSIMO par une personne n'ayant pas la nationalité décrite aux paragraphes 6.2 et 6.3 ci-dessus, fait l'objet d'une consultation préalable avec la Partie d'origine. Le processus de consultation entre les Autorités de sécurité compétentes au sujet de telles personnes est tel que décrit aux alinéas a - d suivants :

a. Le processus est lancé avant le débat ou, si approprié, pendant un projet/programme ou contrat.
b. L'information est limitée à la nationalité des personnes concernées.
c. Une Partie recevant une telle notification détermine si l'accès à ses Informations classifiées est acceptable ou non.
d. De telles consultations sont traitées en priorité, avec pour objectif de parvenir à un consensus. Lorsque ce n'est pas possible, la décision de la Partie d'origine est acceptée.

6.6 Afin de simplifier l'accès à ces Informations classifiées, les Parties s'efforcent de se mettre d'accord, dans les Instructions de sécurité du programme (ISP) ou dans toute autre documentation appropriée approuvée par les Autorités de sécurité compétentes, pour que ces restrictions d'accès soient moins rigoureuses ou ne soient pas exigées.

6. 7 Pour des raisons de sécurité particulières, lorsque la Partie d'origine exige que l'accès à des Informations classifiées de niveau SECRET DÉFENSE/SEGRETO ou de niveau CONFIDENTIEL DÉFENSE/RISERVATISSIMO soit limité aux seules person-

nes ayant exclusivement la nationalité des Parties, ces informations portent la mention de leur classification et un avertissement supplémentaire « Spécial - Italie/France ».

Article 7. Transmission des informations classifiées

7.1 Les Informations classifiées de niveau TRÈS SECRET DÉFENSE/SEGRETISSIMO sont uniquement transmises entre les Parties par la valise diplomatique de Gouvernement à Gouvernement.

7.2 Les Informations classifiées de niveau SECRET DÉFENSE/SEGRETO et de niveau CONFIDENTIEL DÉFENSE/RISERVATISSIMO sont transmises par la voie officielle entre les Parties conformément aux réglementations nationales relatives à la sécurité de la Partie d'origine. Mais d'autres dispositions peuvent être établies en cas d'urgence, sous réserve d'approbation mutuelle par les Parties.

7.3 En cas d'urgence, c'est-à-dire uniquement lorsque l'utilisation de la voie officielle ne peut pas répondre aux exigences, les Informations classifiées de niveau CONFIDENTIEL DÉFENSE/RISERVATISSIMO peuvent être transmises via des sociétés commerciales de messagerie, aux conditions suivantes :

a. La société de messagerie est située sur le territoire des Parties et a mis en place un programme de sécurité et de protection approuvé par l'ANS/ASD concernée pour la prise en charge d'articles de valeur avec un service de signature, incluant notamment une surveillance et un enregistrement permanents permettant de déterminer à tout moment qui en a la charge, soit par un système de registre de signatures et de pointage, soit par un système électronique de suivi et d'enregistrement.

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

c. La société de messagerie doit garantir que l'expédition sera livrée au destinataire avant une date et une heure données dans un délai de 24 heures.

d. La société de messagerie peut confier une tâche à un délégué ou à un sous-traitant, cependant, la responsabilité de l'exécution des obligations ci-dessus incombe toujours à la société de messagerie.

7.4 Les Informations classifiées de niveau DIFFUSION RESTREINTE/RISERVATO sont transmises conformément aux réglementations nationales relatives à la sécurité de la Partie d'origine, à condition qu'ils soient moins restrictifs que ceux mentionnés aux paragraphes 7.1 et 7.2 ci-dessus.

7.5 Les Informations classifiées de niveau SECRET DÉFENSE/SEGRETO et de niveau CONFIDENTIEL DÉFENSE/RISERVATISSIMO peuvent être transmises entre les deux Parties par des voies électroniques et électromagnétiques sécurisées,

7.6 Les Informations classifiées de niveau SECRET DÉFENSE/SEGRETO et de niveau CONFIDENTIEL DÉFENSE/RISERVATISSIMO ne doivent pas être transmises en clair par des moyens électroniques. Seuls des systèmes cryptographiques approuvés par les Autorités de sécurité compétentes des Parties doivent être utilisés pour le cryptage d'Informations classifiées de niveau SECRET DÉFENSE/SEGRETO et de niveau CONFIDENTIEL DÉFENSE/RISERVATISSIMO, quel que soit le mode de transmis-

sion. Dans un tel cas, un « arrangement » séparé est conclu entre les Autorités de sécurité compétentes.

7.7 Les Informations classifiées de niveau DIFFUSION RESTREINTE/RISERVATO doivent être transmises ou récupérées par des moyens électroniques (par exemple des liaisons informatiques point à point), via un réseau public comme Internet, en utilisant des dispositifs de cryptage gouvernementaux ou commerciaux mutuellement acceptés par les Autorités de sécurité nationale compétentes. Cependant, si les Parties l'acceptent, les conversations téléphoniques, les vidéoconférences ou les transmissions par télécopie contenant des Informations classifiées de niveau DIFFUSION RESTREINTE/RISERVATO peuvent être en clair, en l'absence de système de cryptage approuvé.

7.8 Lorsque d'importants volumes d'Informations classifiées doivent être transmis, les moyens de transport, le trajet et l'escorte, le cas échant, sont conjointement déterminés et évalués au cas par cas par l'ANS/ASD des Parties.

Article 8. Visites

8.1 Chaque Partie permet des visites impliquant l'accès aux Informations classifiées de ses établissements, agences et laboratoires publics ainsi que des établissements industriels des contractants, par des représentants civils ou militaires de l'autre Partie ou par les employés de leurs contractants à condition que le visiteur dispose d'une habilitation de sécurité individuelle et d'un « besoin d'en connaître ». Pour les visites effectuées dans le contexte des Informations classifiées aux établissements de l'autre Partie ou aux établissements d'un contractant pour lesquelles l'accès à des Informations classifiées de niveau TRÈS SECRET DÉFENSE/SEGRETISSIMO est requis, il convient de présenter une demande formelle de visite par la voie diplomatique.

8.2 Tous les visiteurs se conforment aux règles de sécurité en vigueur sur le territoire de la Partie d'accueil. Toutes les Informations classifiées communiquées ou mises à la disposition des visiteurs doivent être traitées comme si elles étaient fournies à la Partie à laquelle appartiennent les visiteurs, et doivent être protégées en conséquence.

8.3.1Pour les visites effectuées dans le contexte des Informations classifiées aux établissements de l'autre Partie ou aux établissements d'un Contractant pour lesquelles l'accès à des Informations classifiées est requis, la procédure suivante est applicable :

a. Sous réserve des dispositions suivantes, une telle visite est préparée directement entre l'établissement d'envoi et l'établissement d'accueil.

b. Ces visites sont également soumises aux conditions suivantes :

1) la visite a un but officiel;

2) tout établissement d'accueil dispose d'une habilitation de sécurité d'établissement appropriée;

3) avant l'arrivée, une confirmation de l'habilitation de sécurité individuelle du visiteur est donnée directement à l'établissement d'accueil par le responsable de la sécurité de l'établissement d'envoi. Pour confirmer son identité, le visiteur doit être en possession d'une carte d'identité ou d'un passeport à présenter aux autorités de sécurité de l'établissement d'accueil.

8.3.2 Les visites relatives à des informations classifIées de niveau DIFFUSION RESTREINTE/RISERVATO sont également organisées directement entre l'établissement d'envoi et l'établissement d'accueil.

8.4 II appartient au responsable de la sécurité :

a. de l'établissement d'envoi de vérifier auprès de son Autorité de sécurité compétente que la société/l'établissement d'accueil est en possession d'une habilitation de sécurité d'établissement adéquate;

b. des établissements d'envoi et d'accueil de se mettre d'accord sur la nécessité de la visite.

8.5 Le responsable de la sécurité de l'établissement d'accueil d'une société ou, le cas échéant, d'un établissement gouvernemental, doit s'assurer que tous les visiteurs sont inscrits sur un registre, avec indication de leur nom, de l'organisation qu'ils représentent, de la date d'expiration de l'habilitation de sécurité individuelle, de la/des date(s) de la/des visite(s) et du/des nom(s) de la/des personne(s) visitée(s). Ces registres doivent être conservés pendant au moins cinq ans.

8.6 L'Autorité de sécurité compétente de la Partie d'accueil a le droit d'exiger de ses établissements d'accueil d'être préalablement informée d'une visite si celle-ci doit durer plus de 21 jours. Cette Autorité de sécurité compétente peut alors donner son accord, mais en cas de problème de sécurité, elle consulte l'Autorité de sécurité compétente du visiteur.

8.7 Chacune des Parties assure la protection des données personnelles transmises par l'autre Partie en accord avec ses lois et réglementations nationales.

Article 9. Contrats

9.1 Une Partie concluant, ou autorisant un contractant installé sur son territoire à conclure, un Contrat classé avec un Contractant de l'autre Partie, doit obtenir l'assurance préalable de l'ANS/ASD de l'autre Partie, que le Contractant proposé dispose d'une habilitation de sécurité du niveau approprié, ainsi que de mesures de sécurité appropriées pour garantir une protection adéquate des Informations classifiées. Cette assurance implique que le Contractant autorisé respecte les lois et réglementations nationales relatives à la sécurité.

9.2 L'Autorité de sécurité compétente de la Partie d'origine communique toute information nécessaire sur le Contrat classé à l'Autorité de sécurité compétente de la Partie destinataire, pour permettre un contrôle de la sécurité approprié.

9.3 Chaque contrat comprend un supplément ou une annexe avec des dispositions sur les exigences en matière de sécurité et sur la classification de chaque aspect/élément ou sur le niveau de classification de chaque aspect du Contrat. Les dispositions figurent dans des clauses de sécurité spécifiques ou dans une Lettre sur les aspects de sécurité. Ces dispositions doivent identifier chaque aspect classifié du Contrat, ou tout aspect classifié devant être généré par le contrat, et lui attribuer une classification de sécurité spécifique. Les changements apportés aux exigences ou aux aspects/éléments sont notifiés le cas échéant. La Partie d'origine informe la Partie destinataire lorsque la totalité ou une partie des Informations classifiées a été déclassifiée.

Article 10. Arrangements réciproques relatifs à la sécurité industrielle

10.1 Chaque ANS/ASD notifie l'état de sécurité du site d'une société installée dans son pays, lorsque l'autre Partie le lui demande. Chaque ANS/ASD doit également notifier l'état d'habilitation de sécurité d'un individu lorsque l'autre Partie le lui demande. Ces notifications sont appelées respectivement habilitation de sécurité d'établissement et habilitation de sécurité individuelle.

10.2 En cas de demande, l'ANS/ASD établit l'état d'habilitation de sécurité de la personne morale/physique objet de la demande et transmet un certificat d'habilitation de sécurité si la personne morale/physique est déjà habilitée. Si la personne morale/physique ne dispose pas d'une habilitation de sécurité, ou si l'habilitation est établie à un niveau de sécurité inférieur au niveau demandé, une notification est envoyée pour indiquer que le certificat d'habilitation de sécurité ne peut pas être immédiatement délivré, mais que si l'autre ANS/ASD le souhaite, cette demande sera traitée. À la fin du processus, la notification de la décision prise est transmise à l'Autorité ayant formulé la demande.

10.3 Si une ANS/ASD suspend ou prend des mesures pour abroger une habilitation de sécurité individuelle, ou suspend ou prend des mesures pour annuler l'accès accordé à un ressortissant de l'autre Partie basé sur un certificat d'habilitation de sécurité individuelle, l'autre Partie est informée de la situation et des raisons justifiant ces mesures.

10.4 À la demande de l'autre Partie, toute ANS/ASD coopère aux examens et investigations concernant les habilitations de sécurité.

10.5 Chaque ANS/ASD a le droit de demander à l'autre de réviser une habilitation de sécurité d'établissement à condition que cette demande soit accompagnée des raisons la motivant. Suite à la demande de révision, l'ANS/ASD l'ayant formulée est informée des résultats et des raisons justifiant la décision prise.

Article 11. Perte ou Compromission

11.1 En cas de violation de la sécurité impliquant la perte d'Informations classifiées ou s'il est possible que de telles informations aient été compromises, l'ANS/ASD d'une Partie doit immédiatement informer l'ANS/ASD de l'autre Partie.

11.2 Une enquête immédiate est menée à bien par la Partie destinataire (avec l'aide de la Partie d'origine si requis), conformément aux réglementations applicables sur son territoire pour la protection des Informations classifiées. La Partie destinataire informe, dès que possible, la Partie d'origine des circonstances, du résultat de l'enquête, des mesures adoptées et des mesures correctrices prises.

Article 12. Mise en œuvre

12.1 La mise en œuvre du présent AGS n'implique normalement aucun coût spécifique.

12.2 Chaque Partie et les autorités de son État assistent le personnel effectuant des missions et/ou exerçant des droits, conformément aux dispositions du présent AGS, sur le territoire de l'autre Partie.

12.3 Si besoin, les Autorités de sécurité compétentes des Parties se consultent sur des aspects techniques spécifiques concernant la mise en œuvre du présent AGS et peuvent mutuellement se mettre d'accord sur la conclusion de protocoles de sécurité supplémentaires, de nature spécifique, complétant le présent AGS au cas par cas.

Article 13. Dispositions finales

13.1 Le présent AGS remplace l'Accord de sécurité conclu le 1er février 1978 entre le Gouvernement de la République italienne et le Gouvernement de la République française, au sujet de la Protection des Informations classifiées.

13.2 Le présent AGS est conclu pour une durée indéterminée. Le présent AGS entre en vigueur le premier jour du deuxième mois suivant la réception de la dernière notification entre les Parties spécifiant que les procédures nationales permettant l'entrée en vigueur du présent AGS ont été accomplies.

13.3 Le présent AGS peut être dénoncé par consentement mutuel ou unilatéralement. Ladite dénonciation prend effet six mois après la date d'envoi de l'avis écrit. Les Parties restent responsables de la protection de toutes les Informations classifiées échangées en vertu des dispositions du présent AGS.

13.4 En vertu du présent AGS chaque Partie doit rapidement informer l'autre Partie de tout changement qu'elle envisage d'apporter à ses lois et réglementations nationales affectant la protection des Informations classifiées. Dans un tel cas, les Parties se consultent pour envisager des éventuels amendements à apporter au présent AGS.

13.5 Les dispositions du présent AGS peuvent être modifiées et complétées avec l'accord mutuel écrit des deux Parties. De telles modifications et compléments entrent en vigueur suivant les mêmes modalités que le présent AGS.

13.6 Tout différend concernant l'interprétation ou l'application des dispositions du présent AGS est résolu exclusivement par consultation entre les Parties.

En foi de quoi, les soussignés dûment autorisés à ces fins par leur Gouvernement respectif, ont signé le présent AGS en double exemplaire en langues italienne et française, les deux textes faisant également foi.

Fait à Rome, le 25 juillet 2006.

Pour le Gouvernement de la République française :

YVES AUBAIN DE LA MESSUZIÈRE
Ambassadeur de France

Pour le Gouvernement de la République italienne :

EMILIO DEL MESE
Préfet, Directeur de l'Autorité nationale de Sécurité

[ITALIAN TEXT – TEXTE ITALIEN]

ACCORDO GENERALE DI SICUREZZA

tra

IL GOVERNO DELLA REPUBBLICA FRANCESE

e

IL GOVERNO DELLA REPUBBLICA ITALIANA

RELATIVO ALLA

PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE SCAMBIATE TRA I DUE PAESI

PREAMBOLO

Il Governo della Repubblica francese ed il Governo della Repubblica italiana, di seguito denominati le Parti, ai fini del presente Accordo, desiderando assicurare la protezione delle Informazioni classificate, che ricadono sotto la responsabilità delle rispettive competenti Autorità di Sicurezza, scambiate tra le due Parti o tra organizzazioni commerciali ed industriali in ciascuna delle due Parti, attraverso canali approvati, hanno stabilito, nell'interesse della sicurezza nazionale, le seguenti disposizioni che sono riportate nel presente Accordo Generale di Sicurezza (AGS).

L'AGS comprende i requisiti di sicurezza del capitolo 4 dell'Accordo quadro, definito come "Accordo Quadro" tra la Repubblica Francese, la Repubblica Federale di Germania, la Repubblica Italiana, il Regno di Spagna, il Regno di Svezia, il Regno Unito della Gran Bretagna e dell' Irlanda del Nord, concernente le misure per facilitare la ristrutturazione e le attività dell'industria europea per la difesa, fatto a Farnborough il 27 luglio 2000.

Articolo 1

DEFINIZIONI

Ai fini del presente AGS si intende per:

1.1 **"Informazione classificata"**ogni elemento, materiale o documento classificato, quale che ne sia la forma, sia essa una comunicazione orale o visiva di contenuto classificato o la trasmissione elettrica o elettronica di un messaggio classificato, sotto qualsiasi forma, che debba essere protetta contro divulgazioni non autorizzate.

1.2 **"Contraente"** ogni persona fisica o giuridica in possesso della capacità legale di sottoscrivere contratti.

1.3 **"Contratto classificato"** un contratto che contiene o implica la conoscenza di Informazioni classificate.

1.4 **"ANS/ASD"** Le Autorità Nazionali per la Sicurezza/Autorità di Sicurezza Designate che sono le competenti Autorità per il controllo e l'applicazione di questo AGS.

1.5 **"Parte originatrice"** la Parte, ed ogni altro Ente pubblico o privato posto sotto la sua giurisdizione che ha prodotto l'Informazione classificata.

1.6 **"Parte ricevente"** la Parte, ed ogni altro Ente pubblico o privato posto sotto la sua giurisdizione a cui l'Informazione classificata è trasmessa.

Articolo 2

TAVOLA DELLE EQUIVALENZE

2.1 Ai fini delle presenti disposizioni le classifiche di segretezza e loro equivalenze nei due Paesi sono:

REPUBBLICA FRANCESE	REPUBBLICA ITALIANA
TRES SECRET DEFENSE	**SEGRETISSIMO**
SECRET DEFENSE	**SEGRETO**
CONFIDENTIEL DEFENSE	**RISERVATISSIMO**
vedi sottoparagrafo 2.2	**RISERVATO**

2.2 Ai fini del presente accordo la Repubblica francese tratta e protegge le informazioni contrassegnate "RISERVATO" trasmesse dall'Italia in accordo alle proprie leggi e regolamenti nazionali, in accordo con il livello minimo di sicurezza concordato tra le Parti.
La Repubblica italiana tratta e protegge le informazioni contrassegnate in forma protettiva come "DIFFUSION RESTREINTE", trasmesse dalla Francia, in accordo con le proprie leggi e regolamenti nazionali, in accordo con il livello minimo di sicurezza concordato tra le Parti.

2.3 Le informazioni che richiedono diffusione limitata e controlli di accesso sono scambiate con tali indicazioni. In questi casi, le Parti concordano reciprocamente le misure di sicurezza da applicare.

Articolo 3

AUTORITA' DI SICUREZZA COMPETENTI

3.1 Le Autorità di Governo responsabili per assicurare il controllo e l'applicazione del presente AGS in ciascuna Parte sono:

PER LA REPUBBLICA FRANCESE:
SEGRETARIAT GENERAL DE LA DEFENSE NATIONALE
51, Boulevard de la Tour – Maubourg
75700 Paris 07SP

PER LA REPUBBLICA ITALIANA:
Presidenza del Consiglio dei Ministri
Autorita' Nazionale per la Sicurezza
CESIS III REPARTO-UCSI
Via di Santa Susanna, 15
00187 Roma

3.2 Le suddette Autorità si informeranno reciprocamente su ogni ente subordinato responsabile per specifiche aree disciplinate dalle disposizioni del presente AGS.

Articolo 4

RESTRIZIONI SULL'USO E DIFFUSIONE

4.1 Salvo se diversamente convenuto tra le Parti, la Parte ricevente non diffonde o usa o permette la diffusione o l'uso di qualsiasi Informazione classificata ad essa comunicata dall'altra Parte eccetto per gli scopi e nei limiti stabiliti da o per conto della Parte originatrice.

4.2 La Parte ricevente non trasmette a nessun Stato terzo, o Organizzazione internazionale, alcuna Informazione classificata o materiale, fornito sulla base del presente AGS, né dà pubblica diffusione di qualsiasi Informazione classificata senza il preventivo permesso scritto della Parte originatrice.

Articolo 5

PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE

5.1 La Parte originatrice:

a. Verifica che la Parte ricevente sia informata della classifica delle informazioni e di ogni altra condizione sul rilascio o limitazioni sull'uso delle stesse.

b. Verifica che i documenti siano debitamente contrassegnati in tal senso.

c. Verifica che la Parte ricevente sia informata di qualsiasi cambiamento successivo nella classifica.

5.2 La Parte ricevente:

a. Conformemente alle proprie leggi e regolamenti nazionali, garantisce ad ogni informazione ricevuta dall'altra Parte una protezione di sicurezza di misura pari a quella garantita alle proprie Informazioni classificate di classifica equivalente.

b. Verifica che le Informazioni classificate siano contrassegnate con l'equivalente classificazione nazionale in accordo con il precedente para 2.1.

c. Verifica che le classifiche non siano modificate, salvo autorizzazione scritta della Parte originatrice.

5.3 Allo scopo di poter acquisire e mantenere standard di sicurezza equivalenti, ogni ANS/ASD fornisce all'altra Parte, su richiesta, informazioni riguardanti i propri livelli di sicurezza, procedure e prassi per la protezione delle Informazioni classificate e facilita, a tale scopo, visite da parte delle competenti Autorità di Sicurezza.

Articolo 6

ACCESSO AD INFORMAZIONI CLASSIFICATE

6.1 L'accesso alle Informazioni classificate è limitato a coloro che hanno "necessità di conoscere" ed ai quali sia stata preventivamente concessa una abilitazione di sicurezza da parte dell'ANS/ASD delle Parti, in accordo con le proprie norme nazionali, ad un livello adeguato alla classifica delle informazioni alle quali si può aver accesso.

6.2 L'accesso a Informazioni classificate a livello TRES SECRET DEFENSE/SEGRETISSIMO da parte di persone in possesso della sola cittadinanza di una delle Parti di questo AGS può essere concesso senza la previa autorizzazione della Parte originatrice.

6.3 L'accesso a Informazioni classificate a livello SECRET DEFENSE/SEGRETO e CONFIDENTIEL DEFENSE/RISERVATISSIMO da parte di una persona in possesso della sola cittadinanza delle Parti può essere concesso senza la previa autorizzazione della Parte originatrice. Questa disposizione si applica anche ai cittadini delle Parti firmatarie "l'Accordo Quadro".

6.4 L'accesso a Informazioni classificate a livelli SECRET DEFENSE/SEGRETO e CONFIDENTIEL DEFENSE/RISERVATISSIMO da parte di persone in possesso di doppia cittadinanza di una delle Parti del presente AGS e di una Parte firmataria dell'"Accordo Quadro" o di uno Stato membro dell'Unione Europea è concesso senza preventiva autorizzazione della Parte originatrice. Per qualsiasi altro accesso non previsto dai paragrafi 6.2 a 6.4 si attua la procedura di consultazione descritta nel paragrafo 6.5 successivo.

6.5 L'accesso a Informazioni classificate a livello SECRET DEFENSE/SEGRETO e CONFIDENTIEL DEFENSE/RISERVATISSIMO da parte di persona senza la cittadinanza descritta nei paragrafi 6.2 e 6.3 precedenti è soggetto alla preventiva consultazione con la Parte originatrice. Il processo di consultazione tra le competenti Autorità di Sicurezza concernente tali persone avviene come descritto nei sub-paragrafi a - d seguenti:

a. Il procedimento è avviato prima dell'inizio o, a seconda dei casi, nel corso di un progetto/programma o contratto.

b. Le informazioni sono limitate alla cittadinanza delle persone interessate.

c. Una Parte che riceve tale notifica valuta se l'accesso alle proprie Informazioni classificate sia accettabile o meno.

d. A tali consultazioni è data priorità al fine di raggiungere un consenso. Ove ciò non sia possibile, si accetta la decisione della Parte originatrice.

6.6 Al fine di semplificare l'accesso a tali Informazioni classificate, le Parti cercano di concordare, nelle Istruzioni di Sicurezza del Programma (ISP) o in altri appositi documenti approvati dalle competenti Autorità per la Sicurezza, che tali limitazioni all'accesso possano essere meno restrittive o non necessarie

6.7 Per particolari motivi di sicurezza, se la Parte originatrice chiede che l'accesso a Informazioni classificate a livello SECRET DEFENSE/SEGRETO e CONFIDENTIEL DEFENSE/RISERVATISSIMO sia limitato solamente a chi ha la sola cittadinanza delle Parti in questione, tali informazioni devono essere

contrassegnate con la propria classifica ed una ulteriore avvertenza indicante: "Speciale- Italia/Francia ".

Articolo 7

TRASMISSIONE DI INFORMAZIONI CLASSIFICATE

7.1 Le Informazioni classificate a livello TRES SECRET DEFENSE/SEGRETISSIMO sono trasmesse tra le Parti solamente attraverso bolgetta diplomatica da Governo a Governo.

7.2 Le Informazioni classificate a livello SECRET DEFENSE/SEGRETO e RISERVATISSIMO/CONFIDENTIEL DEFENSE sono trasmesse tramite i canali ufficiali delle Parti secondo le norme nazionali di sicurezza della Parte originatrice. Ma altre disposizioni potranno essere stabilite in caso di emergenza, se approvate dalle Parti.

7.3 In caso di urgenza, cioè solo quando l'uso di canali ufficiali non soddisfi le necessità, le Informazioni classificate a livello CONFIDENTIEL DEFENSE/RISERVATISSIMO possono essere trasmesse a mezzo società di corrieri privati, a condizione che:

a. La società di corrieri sia situata entro il territorio delle Parti e abbia a disposizione un programma di sicurezza e di protezione, approvato dalla rispettiva ANS/ASD, per la movimentazione di materiale di valore, supportato da un servizio di consegna contro firma, comprendente in particolare la sorveglianza e la registrazione continuativa che permetta di determinare in ogni momento chi ne ha la custodia, sia tramite un sistema di registrazione delle firme e dei contrassegni, sia tramite un sistema elettronico di ricerca/ritrovamento.

b. La società di corrieri acquisisca e fornisca al mittente prova dell'effettuata consegna contro firma del destinatario a presentazione dei contrassegni, o acquisisca ricevuta con il numero dei colli.

c. La società di corrieri garantisca che la consegna sia effettuata al consegnatario entro un preciso orario e data, in un periodo di 24 ore.

d. La società di corrieri deleghi un incaricato o un subappaltatore. Tuttavia, la responsabilità per l'adempimento dei suddetti requisiti ricade sulla società di corrieri.

7.4 Le Informazioni classificate a livello DIFFUSION RESTREINTE/RISERVATO, sono trasmesse nell'osservanza delle norme nazionali di sicurezza della Parte originatrice, con il presupposto che esse siano meno restrittive di quelle di cui ai para 7.1. e 7.2. suddetti.

7.5 Le Informazioni classificate ai livelli SECRET DEFENSE/SEGRETO e CONFIDENTIEL DEFENSE/RISERVATISSIMO possono essere trasmesse, tra le due Parti, a mezzo canali elettronici ed elettro-magnetici protetti.

7.6 Le Informazioni classificate a livello SECRET DEFENSE/SEGRETO e CONFIDENTIEL DEFENSE/RISERVATISSIMO non devono essere trasmesse elettronicamente sotto forma di testo in chiaro. Si useranno sistemi crittografici, approvati dalle competenti Autorità per la Sicurezza delle Parti, per la cifratura di Informazioni classificate SECRET DEFENSE/SEGRETO e CONFIDENTIEL DEFENSE/RISERVATISSIMO, indipendentemente dal metodo di trasmissione. In tali circostanze dovrà essere stipulato un "Accordo" separato tra le competenti Autorità di Sicurezza.

7.7 Le Informazioni classificate a livello DIFFUSION RESTREINTE/RISERVATO devono essere trasmesse o vi si deve accedere elettronicamente (per esempio a mezzo collegamenti computerizzati punto a punto) attraverso rete pubblica quale Internet, usando dispositivi governativi o commerciali di cifratura reciprocamente accettati dalle competenti Autorità per la Sicurezza delle Parti. Tuttavia, se accettato dalle Parti, le conversazioni telefoniche, le conferenze video o trasmissioni per facsimile contenenti Informazioni classificate a livello DIFFUSION RESTREINTE/RISERVATO possono essere in chiaro ove non sia disponibile un sistema approvato di cifratura.

7.8 Nel caso debba essere trasmessa una notevole quantità di Informazioni classificate, i mezzi di trasporto, il percorso e la scorta, ove necessaria, devono essere congiuntamente determinati e valutati caso per caso dalle ANS/ASD delle Parti.

Articolo 8

VISITE

8.1. Ciascuna Parte consente visite che comportino l'accesso a Informazioni classificate alle sue infrastrutture pubbliche, agenzie, laboratori e società industriali contraenti, da rappresentanti civili o militari dell' altra Parte o da parte dei dipendenti dei loro contraenti, ammesso che il visitatore abbia una adeguata abilitazione di sicurezza personale e la "necessità di conoscere". In

caso di visite classificate a infrastrutture dell'altra Parte o a ditte di un contraente in cui sia richiesto l'accesso ad Informazioni classificate a livello TRES SECRET DEFENSE/ SEGRETISSIMO verrà inviata formale richiesta di visita attraverso canali diplomatici.

8.2 Tutto il personale in visita si attiene alle norme di sicurezza vigenti nel Paese ospitante. Ogni Informazione classificata comunicata o resa disponibile ai visitatori viene trattata come se fosse stata fornita alla Parte a cui appartiene il personale in visita e viene protetta di conseguenza.

8.3.1 Per visite a infrastrutture governative dell'altra Parte od a ditte di un contraente ove sia richiesto l'accesso a Informazioni classificate, si applicherà la seguente procedura:

a. Subordinatamente alle seguenti direttive, tali visite saranno organizzate direttamente tra la ditta richiedente e la ditta da visitare.

b. Per tali visite si devono avere anche i seguenti prerequisiti:

1) le visite devono avere uno scopo ufficiale;

2) ogni ditta da visitare deve essere in possesso di adeguata abilitazione di sicurezza societaria;

3) prima dell'arrivo, l'incaricato alla sicurezza della struttura che invia il personale in visita deve fornire conferma della abilitazione di sicurezza personale del visitatore direttamente alla struttura ricevente. A conferma della propria identità, il visitatore deve essere in possesso di una carta d'identità o di un passaporto da presentare alla autorità preposta alla sicurezza della struttura da visitare.

8.3.2 Le visite aventi per oggetto Informazioni classificate a livello DIFFUSION RESTREINTE/RISERVATO sono del pari organizzate direttamente tra la ditta richiedente e la ditta da visitare.

8.4 E' responsabilità dell'Incaricato alla sicurezza:

a. della ditta che deve effettuare la visita di assicurarsi con la propria competente Autorità per la Sicurezza che ogni Società/Sito da visitare sia in possesso di adeguata certificazione di sicurezza;

b. delle ditte visitanti e da visitare di accordarsi sulla necessità della visita.

8.5 L'incaricato alla sicurezza di una società/sito da visitare o, ove del caso, di una infrastruttura governativa, deve assicurare che si tengano registrazioni di tutti i visitatori, dei loro nomi, delle organizzazioni che rappresentano, della data di scadenza delle abilitazioni di sicurezza personale, della data della visita e del nome della persona visitata. Tali registrazioni devono essere conservate per un periodo non inferiore a cinque anni.

8.6 La competente Autorità per la Sicurezza della Parte ricevente ha il diritto di richiedere una preventiva notifica da parte delle proprie ditte che devono essere visitate, per visite della durata di più di 21 giorni. Tale Autorità competente per la Sicurezza può quindi rilasciare l'approvazione, ma se dovesse insorgere un problema di sicurezza, si consulterà con la competente Autorità di Sicurezza del visitatore.

8.7 Ciascuna Parte assicura la protezione dei dati personali trasmessi dall'altra Parte in conformità alle leggi e regolamenti nazionali che regolano la materia.

Articolo 9

CONTRATTI

9.1 Una Parte che stipula un contratto o che autorizza un contraente nel suo Paese a eseguire un contratto che include Informazioni classificate con un contraente dell'altra Parte dovrà ottenere preventiva assicurazione, dalla ANS/ASD dell'altra Parte, che il contraente proposto sia in possesso di una abilitazione di sicurezza di livello adeguato e sia anche in possesso di requisiti di sicurezza adeguati per fornire protezione alle Informazioni classificate. Tale assicurazione implica che il contraente autorizzato rispetti le leggi ed i regolamenti di sicurezza nazionali.

9.2 La competente Autorità di Sicurezza della Parte originatrice trasmette le necessarie informazioni, relative al contratto classificato, alla competente Autorità per la Sicurezza della Parte ricevente, per consentire un adeguato controllo di sicurezza.

9.3 Ogni contratto contiene un supplemento o annesso con le disposizioni sui requisiti per la sicurezza e sulla classifica di ogni aspetto/elemento o livello di classifica di ogni aspetto del contratto. Tali disposizioni sono contenute in specifiche clausole di sicurezza o in una Lettera sugli aspetti di sicurezza. Le stesse disposizioni indicano ogni aspetto classificato del contratto, oppure ogni aspetto classificato che possa originare dal contratto ed attribuire ad esso una sua specifica classifica di sicurezza. Cambiamenti nei requisiti o negli aspetti/elementi sono notificati, quando necessario. La Parte originatrice

comunica alla Parte ricevente quando l'Informazione classificata o parte di essa sia stata declassificata.

Articolo 10

RECIPROCI ACCORDI PER LA SICUREZZA INDUSTRIALE

10.1 Ciascuna ANS/ASD notifica lo status di sicurezza del sito di una società che ha sede nel suo Paese, quando richiesto dall'altra Parte. Ciascuna ANS/ASD notifica altresì lo status della abilitazione di sicurezza di una persona fisica quando richiesto in tal senso dall'altra Parte. Queste notifiche sono rispettivamente note come abilitazione di sicurezza industriale e abilitazione di sicurezza personale.

10.2 Quando richiesto, la ANS/ASD stabilisce lo status dell'abilitazione di sicurezza di una persona fisica/giuridica che è soggetto della domanda ed inoltra comunicazione riguardante l'abilitazione di sicurezza se la persona fisica/giuridica sono già abilitate. Se la persona fisica/giuridica non possiede una abilitazione di sicurezza, o se la abilitazione è di un livello inferiore a quello richiesto, ne è data comunicazione alla Parte richiedente, specificando che il certificato di abilitazione di sicurezza non viene immediatamente rilasciato, ma se richiesto dall'altra ANS/ASD tale domanda viene istruita. Al termine di tale processo sarà fornita una notificazione della decisione presa all'Autorità richiedente.

10.3 Se una delle ANS/ASD sospende o intraprende azioni per revocare una abilitazione di sicurezza personale, o sospende o intraprende azioni per revocare l'accesso concesso a un cittadino dell'altra Parte basato su una abilitazione di sicurezza personale, l'altra Parte è informata del fatto e le sono rese note le ragioni che giustificano tale decisione.

10.4 Se richiesto dall'altra Parte, ciascuna ANS/ASD coopera nella revisione e negli accertamenti concernenti le abilitazioni di sicurezza.

10.5 Ogni ANS/ASD si riserva il diritto di chiedere all'altra la revisione delle abilitazioni di Sicurezza del sito purchè tale richiesta sia accompagnata dalle opportune motivazioni. Al termine della revisione l'ANS/ASD richiedente è informata sui risultati e sulle motivazioni relative alle decisioni prese.

Articolo 11

PERDITA O COMPROMISSIONE

11.1 Nel caso di una violazione di sicurezza che comporti perdita di Informazioni classificate o di sospetto che tali Informazioni classificate siano state compromesse, l'ANS/ASD di una Parte informa subito l'ANS/ASD dell'altra Parte.

11.2 Una immediata indagine è condotta dalla Parte ricevente (con l'ausilio della Parte originatrice, se richiesto) nell'osservanza delle norme in vigore in quel Paese sulla protezione delle Informazioni classificate. La Parte ricevente informa, al più presto possibile, la Parte originatrice sulle circostanze, sull'esito delle indagini e le misure adottate e le azioni di rimedio intraprese.

Art. 12

MODALITA DI ATTUAZIONE

12.1 L'applicazione del presente AGS non comporta di norma alcun costo specifico.

12.2 Ciascuna Parte e le autorità del proprio Stato assistono il personale che svolge attività e/o esercita diritti, nel Paese della controparte, nell'osservanza del presente AGS.

12.3 In caso di necessità, le competenti Autorità di Sicurezza delle Parti si consultano su specifici aspetti tecnici concernenti l'applicazione del presente AGS e possono, di comune accordo, stipulare protocolli di sicurezza supplementari al presente AGS di specifica natura, sulla base di ogni singolo caso.

Articolo 13

DISPOSIZIONI FINALI

13.1 Il presente AGS sostituisce l'Accordo di Sicurezza stipulato il 1° febbraio 1978 tra il Governo della Repubblica italiana e il governo della Repubblica francese, sulla protezione delle Informazioni classificate.

13.2 Il presente AGS è valido per un periodo di tempo indeterminato. Il presente AGS entrerà in vigore il primo giorno del secondo mese successivo alla ricezione dell'ultima notifica tra le Parti che i necessari adempimenti, stabiliti dalle norme giuridiche nazionali per l'entrata in vigore del presente AGS, siano stati espletati.

13.3 Il presente AGS può essere denunciato per mutuo consenso tra le Parti o unilateralmente. Detta denuncia avrà effetto 6 mesi dopo la data di invio della comunicazione scritta. Le Parti rimarranno responsabili della protezione di tutte le Informazioni classificate scambiate sulla base del presente AGS.

13.4 In virtù del presente AGS, ciascuna Parte notificherà prontamente all'altra Parte qualsiasi cambiamento delle proprie leggi e regolamenti nazionali che potrebbe incidere sulla protezione delle Informazioni classificate. In tal caso, le Parti si consultano per esaminare possibili cambiamenti al presente AGS.

13.5 Le disposizioni di questo AGS possono essere emendate ed integrate sulla base di un mutuo consenso scritto delle Parti. Tali emendamenti e integrazioni entrano in vigore con le stesse modalità del presente AGS.

13.6 Ogni controversia riguardante l'interpretazione o l'applicazione delle disposizioni contenute in questo AGS è risolta esclusivamente attraverso consultazioni tra le Parti.

In fede di che, i sottoscritti, debitamente autorizzati dai rispettivi Governi, hanno firmato il presente AGS, in due esemplari, in lingua italiana e francese, entrambi i testi facenti egualmente fede.

Fatto a Roma il 25/07/2006

Per il Governo della Repubblica Francese

Per il Governo della Repubblica Italiana

[TRANSLATION – TRADUCTION]

GENERAL SECURITY AGREEMENT BETWEEN THE GOVERNMENT OF THE FRENCH REPUBLIC AND THE GOVERNMENT OF THE ITALIAN REPUBLIC CONCERNING THE PROTECTION OF CLASSIFIED INFORMATION EXCHANGED BETWEEN THE TWO COUNTRIES

PREAMBLE

The Government of the French Republic and the Government of the Italian Republic, also referred to as the Parties for the purposes of this Agreement, desiring to ensure the protection of classified information being exchanged between the two Parties or transmitted between commercial or industrial entities of the two Parties via approved channels, and noting that responsibility for such protection lies with their respective competent security authorities, have agreed, in the interest of national security, to the following provisions as part of this General Security Agreement (GSA).

The General Security Agreement incorporates the security requirements specified in Part 4 of the "Framework Agreement between the French Republic, the Federal Republic of Germany, the Italian Republic, the Kingdom of Spain, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland concerning measures to facilitate the restructuring and operation of the European defence industry", done at Farnborough on 27 July 2000, also referred to as the Framework Agreement.

Article 1. Definitions

For the purposes of this General Security Agreement:

1.1 "Classified information" means classified items, materials and documents, irrespective of their form, which may involve oral or visual communications whose contents have been classified, or electrical or electronic transmissions of classified messages, or communications in whatever form requiring protection against unauthorized disclosure.

1.2 "Contractor" means any individual or legal entity with the legal capacity to conclude contracts.

1. 3 "Classified contract" means a contract that contains or implies the knowledge of classified information.

1.4 "NSA/DSA" means the national security authorities/designated security authorities that are the competent authorities with regard to the monitoring and implementation of this General Security Agreement.

1.5 "Originating Party" means the Party, including any other public or private entity subject to its national laws and regulations, which produced the classified information.

1.6 "Receiving Party" means the Party, including any other public or private entity subject to its national laws and regulations, to which the classified information is transmitted.

Article 2. Table of equivalences

2.1 For the purposes of this Agreement, the security classifications and their equivalents in the two countries are as follows:

FOR THE FRENCH REPUBLIC	FOR THE ITALIAN REPUBLIC
TRÈS SECRET DÉFENSE	SEGRETISSIMO
SECRET DÉFENSE	SEGRETO
CONFIDENTIEL DÉFENSE	RISERVATISSIMO
See para. 2.2 below	RISERVATO

2.2 For the purposes of this Agreement, the French Republic shall handle and protect information marked "RISERVATO" transmitted by Italy, pursuant to its national laws and regulations, in accordance with the minimum level of security agreed by the Parties.

The Italian Republic shall handle and protect information marked with a protection level such as "DIFFUSION RESTREINTE" and transmitted to it by France, pursuant to its national laws and regulations, in accordance with the minimum level of security agreed by the Parties.

2.3 Information that is exchanged and requires restrictions on distribution and access shall be so marked during its exchange. However, in such situations the Parties shall determine jointly the security measures to be applied.

Article 3. Competent Security Authorities

3.1 The Government authorities responsible for ensuring implementing and monitoring of this General Security Agreement for each of the parties are:

For the French Republic:
The General Secretariat for National Defence
51, boulevard de La Tour-Maubourg
75700 Paris 07SP

For the Italian Republic:
The Presidency of the Council of Ministers
National Security Authority
CESIS III REPARTO-UCSI
Via de Santa Susanna, 15
00187 Rome

3.2 The above-mentioned authorities shall inform each other of any subordinate bodies responsible for specific areas in accordance with the provisions of this General Security Agreement.

Article 4. Restrictions on use and disclosure

4.1 Unless the Parties have agreed otherwise, the receiving Party shall not disclose nor use nor allow the disclosure or use of any classified information transmitted to it by the other Party, except for the purposes and subject to the restrictions indicated by or on behalf of the originating Party.

4.2 The receiving Party shall not transmit any classified information or material it has received under the provisions of this General Security Agreement to any third State or international organization, nor disclose publicly any classified information without the prior written consent of the originating Party.

Article 5. Protection of classified information

5.1 The originating Party shall:

(a) ensure that the receiving Party has been informed of the classification applicable to information and of any conditions with regard to communication or restrictions on its use;

(b) ensure that documents have been properly marked;

(c) ensure that the receiving Party is informed of any subsequent change in classification.

5.2 The receiving Party shall:

(a) in conformity with its national laws and regulations, afford the classified information received from the other Party the degree of protection and security that is afforded to its own national classified information with the equivalent classification;

(b) ensure that classified information is marked with its own equivalent national classification, as specified in paragraph 2.1 of article 2 above;

(c) ensure that the classifications are not changed without the prior written consent of the originating Party.

5.3 In order to achieve and maintain comparable security standards, each NSA/DSA shall, upon request, furnish the other with information on its security standards, procedures and practices with regard to the protection of classified information and shall, to that end, allow visits by the competent security authorities.

Article 6. Access to classified information

6.1 Access to classified information shall be restricted to individuals who have a need to know and have received prior clearance from an NSA/DSA of the Parties, in ac-

cordance with their national standards, of a level appropriate to the classification of the information to which they desire access.

6.2 Access to information classified TRÈS SECRET DÉFENSE/SEGRETISSIMO by an individual who is exclusively a national of one of the Parties of this General Security Agreement may be granted without the prior authorization of the originating Party.

6.3 Access to information classified SECRET DÉFENSE/SEGRETO and CONFIDENTIEL DÉFENSE/RISERVATISSIMO by an individual who is exclusively a national of one of the Parties of this General Security Agreement may be granted without the prior authorization of the originating Party. This provision shall also apply to nationals of parties to the Framework Agreement.

6.4 Access to information classified SECRET DÉFENSE/SEGRETO by an individual who holds dual nationality in one of the Parties of this General Security Agreement and in a party to the Framework Agreement or in a member State of the European Union shall be granted without the prior authorization of the originating Party. Any other access not covered under paragraphs 6.2 – 6.4 above shall be subject to the consultation process described in paragraph 6.5 below.

6.5 Access to information classified SECRET DÉFENSE/SEGRETO and CONFIDENTIEL DÉFENSE/RISERVATISSIMO by an individual holding a nationality not covered by paragraphs 6.2 and 6.3 above shall be decided through prior consultations with the originating Party. The consultation process between the competent security authorities with regard to such individuals shall be governed by subparagraphs (a)-(d) below:

(a) The process shall be launched before or, if appropriate, during a project/programme or contract.

(b) The information in question shall be restricted to the nationality of the individuals concerned.

(c) A Party receiving such notification shall decide whether access to its classified information is acceptable or not.

(d) Such consultations shall be handled on a priority basis with the goal of reaching a consensus. Where that is not possible, the decision of the originating Party shall be accepted.

6.6 In order to simplify access to classified information, the Parties shall endeavour to reach agreement in programme security instructions (PSIs) or any other appropriate documentation approved by the competent security authorities, so that such access restrictions can be made less rigorous or not required at all.

6.7 For particular security reasons, when an originating Party insists that access to information classified SECRET DÉFENSE/SEGRETO or CONFIDENTIEL DÉFENSE/RISERVATISSIMO be restricted to individuals who are exclusively nationals of the Parties, such information shall be marked with its classification and a supplementary warning "Spécial-Italie/France".

Article 7. Transmission of classified information

7.1 Information that has been classified TRÈS SECRET DÉFENSE/SEGRETISSIMO shall be transmitted solely between the Parties, using the diplomatic pouch from Government to Government.

7.2 Information that has been classified SECRET DÉFENSE/SEGRETO and CONFIDENTIEL DÉFENSE/RISERVATISSIMO shall be transmitted between the Parties through official channels pursuant to the security regulations of the originating Party. However, other provisions may be agreed in the event of an emergency, subject to mutual approval by the Parties.

7.3 In the event of an emergency, i.e. only when the official channel is unable to meet the requirements, information classified CONFIDENTIEL DÉFENSE/ RISERVATISSIMO may be transmitted via a commercial courier service, subject to the following conditions:

(a) The courier service must be situated in the territory of the Parties and shall have instituted a security and protection programme approved by the NSA/DSA concerned for handling valuable items, including a certification service that involves in particular continuous monitoring and registration and makes it possible to determine at any time who has possession of the item, using either a system with a signature register and a log book or an electronic monitoring and registration system.

(b) The courier company must obtain and furnish to the sender a copy of the certificate of receipt based on the signature register and logs or must obtain a receipt with the package numbers.

(c) The courier company must guarantee that the shipment will be delivered to the receiving party by a certain date and time within 24 hours.

(d) The courier company may delegate a task to a representative or a subcontractor; however, responsibility for meeting the obligations specified above shall always rest with the courier company.

7.4 Information classified DIFFUSION RESTREINT/RISERVATO shall be transmitted in accordance with the national security regulations of the originating Party, provided that they are less restrictive than those mentioned in paragraphs 7.1 and 7.2 above.

7.5 Information classified SECRET DÉFENSE/SEGRETO and CONFIDENTIEL DÉFENSE/RISERVATISSIMO may be transmitted between the two Parties via secured electronic or electromagnetic channels.

7.6 Information classified SECRET DÉFENSE/RISERVATISSIMO or CONFIDENTIEL DÉFENSE/RISERVATISSIMO must not be transmitted electronically in clear text. Only cryptographic systems that have been approved by the competent security authorities of the Parties may be used in encrypting information classified SECRET DÉFENSE/RISERVATISSIMO and CONFIDENTIEL DÉFENSE/ RISERVATISSIMO, whatever the means of transmission. In such situations a separate "arrangement" shall be concluded between the competent security authorities.

7.7 Where information classified DIFFUSION RESTREINTE/RISERVATO is transmitted and received electronically via a public network such as the Internet (such as via point-to-point data links), government or public encryption techniques jointly accept-

able to the national competent security authorities must be used. However, if the Parties agree, telephone conversations, video conferences and fax transmissions containing information classified DIFFUSION RESTREINTE/RISERVATO may be carried out in unencrypted mode in the absence of an approved encryption system.

7.8 Where large amounts of classified information need to be transmitted, the means of transportation, the route and, if necessary, the escort shall be determined jointly and evaluated on a case by case basis by the NSA/DSAs of the Parties.

Article 8. Visits

8.1 Each Party shall permit visits by civilian or military representatives of the other Party or by employees of their contractors, involving access to classified information in its facilities, agencies and public laboratories, as well as in the industrial sites of contractors, provided that such visitors hold a personal security clearance and have a need to know. Where such visits to establishments of the other Party or to sites of contractors involve access to information classified TRÈS SECRET DÉFENSE/SEGRETISSIMO, a formal request for the visit shall be submitted through the diplomatic channel.

8.2 All visitors shall respect the security regulations in force in the territory of the host Party. All classified information that is communicated to or made available to the visitors must be treated as if it had been furnished to the Party to which the visitors belong and must be protected accordingly.

8.3.1 In the case of visits to establishments of the other Party or to sites of contractors that require access to classified information, the following procedures shall apply:

(a) Subject to the provisions below, such visits shall be prepared directly by the sending establishment and the host establishment.

(b) Such visits shall also be subject to the following conditions:

1. The visit must have an official purpose.

2. The host establishment must have the appropriate facility security clearance.

3. Before arrival, the official in charge of security at the sending establishment shall provide a confirmation of the personal security clearance of the visitor directly to the host establishment. In order to confirm his identity, the visitor shall have in his possession an identity card or passport for presentation to the security authorities of the host establishment.

8.3.2 Visits involving information classified DIFFUSION RESTREINT/RISERVATO shall also be organized directly between the sending establishment and the host establishment.

8.4 The official in charge of security:

(a) at the sending establishment shall verify with his competent security authorities that the host company or establishment has the appropriate facility security clearance;

(b) at the sending and host establishments shall reach agreement on the need for the visit.

8.5 The official in charge of security at the host establishment of a company or, as the case may be, of a government entity must ensure that all visitors are registered, with

their name, their organization, the expiration date of their personal security clearance, the date(s) of their visit(s) and the name(s) of the person(s) visited. Such registers must be kept for at least five years.

8.6 The competent security authorities of the host Party shall have the right to require of its host establishments that they inform it in advance of any visit expected to last more than 21 days. The competent security authority may agree thereto, but when security concerns arise, it shall consult the competent security authority of the visiting Party.

8.7 Each Party shall ensure the protection of personal data transmitted by the other Party in accordance with its national laws and regulations.

Article 9. Contracts

9.1 Before concluding a classified contract or authorizing a contractor established in its territory to conclude a classified contract with a contractor from the other Party, a Party shall obtain prior assurance from the NSA/DSA of the other Party that the proposed contractor has been granted the appropriate level of clearance and has taken the appropriate security measures to ensure the protection of classified information. This assurance shall imply that the authorized contractor will respect the national security laws and regulations.

9.2 The competent security authorities of the originating Party shall communicate all necessary information about the classified contract to the competent security authorities of the receiving Party in order to ensure appropriate security controls.

9.3 Each contract shall include a supplement or annex with provisions on the security requirements and the classification relating to each part of the contract or on the level of classification of each part of the contract. These provisions shall be contained in specific clauses on security or in a letter on security aspects. These provisions must identify each classified part of the contract or any classified outputs that the contract is expected to generate and assign a specific classification to such parts or outputs. Notification shall be given concerning any changes with regard to requirements or to such parts. The originating Party shall notify the receiving Party if all or part of the classified information has been declassified.

Article 10. Reciprocal arrangements regarding industrial security

10.1 Each NSA/DSA shall, if the other Party requests it, provide information on the security status of a company facility in its territory. Each NSA/DSA shall also, if the other Party requests it, provide information on the status of an individual's security clearance. These notifications shall be referred to as a facility security clearance and a personal security clearance respectively.

10.2 Upon request, the NSA/DSA shall determine the security clearance status of the company or individual that is the object of the query and, if the company or person already has a security clearance, shall transmit a security clearance certificate. If the company or individual has no security clearance or if the security clearance is at a lower level than required, notice shall be sent indicating that the security clearance certificate cannot be sent immediately and that the request will be processed if the other NSA/DSA so

wishes. Upon completion of the process, notice of the decision taken shall be sent to the authorities submitting the request.

10.3 If a NSA/DSA suspends or takes action to revoke a personal security clearance, or suspends or takes action to revoke the access granted to a national of the other Party based upon a personal security clearance, the other Party shall be informed of the situation and of the reasons for taking such action.

10.4 If requested by the other Party, each NSA/DSA shall cooperate in investigations into security clearances.

10.5 An NSA/DSA shall have the right to request of the other Party that it review a facility security clearance, provided that the request is accompanied by the grounds for the request. Subsequent to the request for review, the NSA/DSA submitting it shall be informed of the outcome and the grounds for the decision taken.

Article 11. Loss or compromise

11.1 In the event of violation of security implying the loss of classified information or if there is a possibility that such information has been compromised, the NSA/DSA of one Party must immediately notify the NSA/DSA of the other Party.

11.2 An investigation shall immediately be carried out by the receiving Party (with the assistance of the originating Party if requested), in accordance with the regulations in force in its territory concerning the protection of classified information. The receiving Party shall notify the originating Party as soon as possible of the circumstances, the outcome of the investigation, the steps taken and any corrective measures adopted.

Article 12. Implementation

12.1 Implementation of this General Security Agreement shall not generally involve any specific costs.

12.2 Each Party and the authorities of its State shall assist its staff in carrying out missions and/or in exercising rights, in accordance with this General Security Agreement, in the territory of the other Party.

12.3 If necessary, the competent security authorities of the Parties shall hold consultations on specific technical aspects of the implementation of this General Security Agreement and may come to joint agreement on the conclusion of supplementary security protocols of specific nature, complementing this General Security Agreement on a case by case basis.

Article 13. Final provisions

13.1 This General Security Agreement shall replace the Security Agreement between the Government of the French Republic and the Government of the Italian Republic on the protection of classified information, signed on 1 February 1978.

13.2 This General Security Agreement is concluded for an indefinite period. The Agreement shall enter into force on the first day of the second month following the date

of receipt of the last notification between the Parties stating that the national procedures for the entry into force of the Agreement have been completed.

13.3 This General Security Agreement may be denounced unilaterally or by mutual agreement. The denunciation shall enter into force six months after the date on which the written notice was sent. The Parties shall remain responsible for protecting all classified information exchanged under the provisions of this General Security Agreement.

13.4 Under this General Security Agreement each Party shall quickly notify the other Party of any changes it intends to make in its national laws and regulations regarding the protection of classified information. In such a situation, the Parties shall hold consultations to plan possible amendments to this Agreement.

13.5 The provisions of this General Security Agreement may be modified and added to by mutual agreement on the part of the two Parties. Such modifications and extensions shall enter into force via the same modalities as the present Agreement.

13.6 Any dispute concerning the interpretation or implementation of the provisions of this General Security Agreement shall be resolved exclusively through consultations between the Parties.

In witness whereof, the signatories, duly authorized for that purpose by their respective Governments, have signed this General Security Agreement in duplicate, in the French and Italian languages, both texts being equally authentic.

Done at Rome on 25 July 2006.

For the Government of the French Republic:

YVES AUBIN DE LA MESSUZIÈRE
Ambassador of France

For the Government of the Italian Republic:

EMILIO DEL MESE
Prefect, Director of the National Security Authority