ACCORDO TRA
IL GOVERNO DELLA REPUBBLICA ITALIANA
E
IL GOVERNO DEGLI STATI UNITI D'AMERICA
SULLE MISURE DI SICUREZZA PER LA PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE

PREAMBOLO

Il Governo della Repubblica Italiana ("Repubblica Italiana") e il Governo degli Stati Uniti d'America ("Stati Uniti") (singolarmente denominati "Parte" e collettivamente "Parti"),

Considerando che le Parti cooperano in settori che includono, fra gli altri, gli affari esteri, la difesa, la sicurezza, l'ordine pubblico, la scienza, l'industria, la tecnologia, e

Rilevando un mutuo interesse alla protezione delle Informazioni Classificate scambiate in via riservata tra le Parti,

Hanno concordato quanto segue:

ARTICOLO 1 – DEFINIZIONI

Ai fini di questo Accordo si applicano le seguenti definizioni:

1. Informazione Classificata: Informazione fornita da una Parte all'altra Parte, cui è attribuita una classifica dalla Parte trasmittente per ragioni di sicurezza nazionale e, pertanto, necessita di protezione contro la divulgazione non autorizzata. L'informazione può essere in forma orale, visiva, elettronica o scritta, ovvero in forma di materiali, quali attrezzature o apparati tecnologici.

2. Contratto Classificato: Un contratto che richiede, o richiederà, l'accesso a, o la produzione di, Informazioni Classificate da parte di un Contraente o di suo personale nell'esecuzione del Contratto.

3. Contraente: Una persona fisica o giuridica, avente la capacità giuridica di concludere contratti, parte di un Contratto Classificato.

4. Abilitazione di Sicurezza Industriale (di seguito "FSC"): Un certificato rilasciato dall'Autorità Nazionale di Sicurezza di una Parte, così come designata ai sensi dell'Articolo 4, nei confronti della struttura di un Contraente ricadente sotto la giurisdizione della stessa, indicante che tale struttura è abilitata alla trattazione di Informazioni Classificate fino a un determinato livello, e dotata di misure di sicurezza adeguate alla protezione delle stesse. Tale certificato attesta che le Informazioni Classificate di livello RISERVATISSIMO / CONFIDENTIAL o superiore sono protette dal Contraente, cui la FSC è rilasciata, in ottemperanza alle disposizioni del presente Accordo, il cui rispetto è monitorato e garantito dall'Autorità Nazionale di Sicurezza. La FSC non è richiesta a un Contraente per l'esecuzione di contratti che richiedano la ricezione o la produzione di Informazioni Classificate al solo livello RISERVATO.

5. Abilitazione di Sicurezza Personale (di seguito "PSC"):

a. una determinazione dell'Autorità Nazionale di Sicurezza di una Parte, così come designata ai sensi dell'Articolo 4, per cui un individuo impiegato da un ente governativo di tale Parte, ovvero un Contraente sotto la giurisdizione della stessa Parte, è autorizzato ad accedere a Informazioni Classificate fino a un determinato livello; ovvero

b. una determinazione dell'Autorità Nazionale di Sicurezza di una Parte, così come designata ai sensi dell'Articolo 4, per cui un individuo avente cittadinanza di tale Parte, ma in procinto di essere impiegato dall'altra Parte, ovvero da uno dei Contraenti dell'altra Parte, è autorizzato ad accedere a Informazioni Classificate fino a un determinato livello.

6. Necessità di Conoscere: Una determinazione da parte di un soggetto autorizzato alla gestione di Informazioni Classificate attestante la necessità di un potenziale destinatario di Informazioni Classificate di accedere a specifiche Informazioni Classificate, al fine di svolgere o supportare una funzione governativa legittima e autorizzata.

ARTICOLO 2 – LIMITAZIONI ALL'AMBITO APPLICATIVO

Questo Accordo non si applica ad Informazioni Classificate rientranti nella sfera applicativa di altro accordo o intesa tra le Parti, o tra loro agenzie, riguardante la protezione di specifici ambiti o categorie di Informazioni Classificate scambiate tra le Parti o tra agenzie delle stesse, a meno che detto accordo o intesa non renda espressamente applicabili le disposizioni del presente Accordo. Questo Accordo non si applica, altresì, allo scambio di "*Restricted Data*", come definiti nello U.S. Atomic Energy Act del 1954 e successivi emendamenti ("AEA"), ovvero a "*Formerly Restricted Data*", ossia dati rimossi dalla categoria "*Restricted Data*" ai sensi dell'AEA ma ancora considerati dagli Stati Uniti informazioni relative alla difesa.

ARTICOLO 3 – IMPEGNO ALLA PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE

1. Ciascuna Parte protegge le Informazioni Classificate dell'altra Parte secondo i termini stabiliti nel presente Accordo.

2. Le Informazioni Classificate sono protette dalla Parte ricevente con modalità che siano almeno equivalenti a quelle previste per le Informazioni Classificate dalla Parte trasmittente, secondo la tabella di cui all'Articolo 5.

3. Ciascuna Parte notifica tempestivamente all'altra ogni modifica alle proprie leggi e regolamenti che potrebbe avere effetto sulla protezione delle Informazioni Classificate ai sensi del presente Accordo. Gli obblighi stabiliti da questo Accordo sono lasciati impregiudicati da tali modifiche della normativa interna. In tali casi, le Parti si consultano su possibili emendamenti al presente Accordo o altre misure che possono essere idonee al mantenimento della protezione delle Informazioni Classificate scambiate ai sensi del presente Accordo.

ARTICOLO 4 – AUTORITA' NAZIONALI DI SICUREZZA

1. Le Parti si informano reciprocamente circa le Autorità Nazionali di Sicurezza responsabili per l'applicazione di questo Accordo e di ogni successiva modifica relativa a tali Autorità.

2. Ai fini del presente Accordo, le Autorità Nazionali di Sicurezza sono: per la Repubblica Italiana, Presidenza del Consiglio dei Ministri – Dipartimento delle Informazioni per la Sicurezza (DIS) – Ufficio Centrale per la Segretezza (UCSe); per gli Stati Uniti, Assistant Director, International Engagement Directorate, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy, U.S. Department of Defense.

3. Le Parti possono concludere ulteriori intese attuative del presente Accordo, laddove misure di sicurezza aggiuntive siano richieste per proteggere le Informazioni Classificate trasferite alla Parte ricevente attraverso esportazioni in campo militare o programmi di cooperazione per la produzione o lo sviluppo congiunti di prodotti o servizi per la difesa. Tali intese attuative possono includere Accordi di Sicurezza Speciali o Accordi di Sicurezza Industriale.

ARTICOLO 5 – DESIGNAZIONE DELLE INFORMAZIONI CLASSIFICATE

1. Le Informazioni Classificate sono designate, e ove possibile, marcate o contrassegnate dalla Parte trasmittente con uno dei seguenti livelli nazionali di classifica di segretezza. Al fine di assicurare equipollenza di trattamento, le Parti concordano che i seguenti livelli di classifica sono equivalenti:

REPUBBLICA ITALIANA	STATI UNITI
SEGRETISSIMO	TOP SECRET
SEGRETO	SECRET
RISERVATISSIMO	CONFIDENTIAL
RISERVATO	Nessuna equivalenza (vds. Paragrafo 2)

2. Nel corso dell'attuazione del presente Accordo, se la Repubblica Italiana fornisce Informazioni Classificate designate come "RISERVATO", gli Stati Uniti le gestiscono ai sensi dell'Appendice a questo Accordo.

3. Le Informazioni Classificate sono designate e, ove possibile, marcate e contrassegnate, con il nome della Parte trasmittente.

ARTICOLO 6 – RESPONSABILITA' PER LE INFORMAZIONI CLASSIFICATE

La Parte ricevente è responsabile per la protezione di tutte le Informazioni Classificate della Parte trasmittente, nel periodo di tempo in cui tali Informazioni Classificate sono sotto il suo controllo, in modo almeno equivalente a quanto previsto dalla Parte trasmittente per garantire la protezione delle proprie Informazioni Classificate, in linea con la tabella di cui all'Articolo 5. Durante il trasporto, la Parte trasmittente è responsabile per tutte le Informazioni Classificate fino a che la custodia di tali Informazioni Classificate è formalmente trasferita alla Parte ricevente.

ARTICOLO 7 – PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE

1. Nessun individuo è autorizzato ad accedere a Informazioni Classificate unicamente in virtù del grado, posizione, nomina o possesso di una PSC. L'accesso a tali informazioni è consentito esclusivamente a individui che abbiano Necessità di Conoscere e a cui sia stata rilasciata la prevista PSC nel rispetto degli standard prescritti dalla Parte ricevente.

2. Salvo quanto diversamente disposto nel presente Accordo, la Parte ricevente non divulga Informazioni Classificate della Parte trasmittente a nessuna parte terza, ivi inclusi Governi, individui, società, istituzioni, organizzazioni o altri enti di parti terze, senza il previo consenso scritto della stessa Parte trasmittente.

3. La Parte ricevente non utilizza né consente l'utilizzo di Informazioni Classificate della Parte trasmittente per finalità diverse da quelle per cui tali informazioni sono state fornite, senza il previo consenso scritto della stessa Parte trasmittente.

4. La Parte ricevente rispetta ogni diritto di natura privatistica connesso alle Informazioni Classificate della Parte trasmittente, ivi inclusi i diritti relativi a brevetti, diritti d'autore o segreti commerciali, e non cede, utilizza, scambia o divulga tali Informazioni Classificate in modo incompatibile con tali diritti, senza la previa autorizzazione scritta del detentore degli stessi.

5. La Parte ricevente assicura che ogni struttura o stabilimento che tratta Informazioni Classificate ricadenti nel presente Accordo mantenga una lista di persone che, presso tale struttura o stabilimento, sono autorizzate ad accedere a dette informazioni.

6. Ciascuna Parte definisce procedure di controllo e tracciamento per gestire la diffusione e l'accesso a Informazioni Classificate.

7. Ciascuna Parte è tenuta al rispetto di ogni limitazione d'uso, divulgazione, cessione, e accesso alle Informazioni Classificate, così come specificato dalla Parte fornitrice all'atto del rilascio di dette informazioni. Se una Parte non è in grado di ottemperare alle limitazioni specificate, tale Parte si consulta immediatamente con l'altra Parte e pone in essere tutte le misure idonee ad evitare o ridurre al minimo tale uso, divulgazione, cessione o accesso.

ARTICOLO 8 – ABILITAZIONI DI SICUREZZA PERSONALI

1. Le Parti assicurano che tutte le persone che, nello svolgimento delle proprie funzioni ufficiali, abbiano necessità di accedere a Informazioni Classificate, o i cui compiti o funzioni possano consentire l'accesso a tali informazioni ai sensi del presente Accordo, ricevano una PSC al livello adeguato prima che sia loro consentito l'accesso a tali informazioni. La PSC non è richiesta per l'accesso a Informazioni Classificate al livello RISERVATO.

2. La Parte che rilascia la PSC svolge una indagine adeguata e sufficientemente dettagliata al fine di valutare l'idoneità di un individuo ad accedere a Informazioni Classificate. La determinazione relativa al rilascio della PSC è assunta nel rispetto delle leggi e dei regolamenti della Parte che la rilascia.

3. Prima che un funzionario o un rappresentante di una Parte ceda Informazioni Classificate a un funzionario o rappresentante dell'altra Parte, la Parte ricevente fornisce alla Parte trasmittente una garanzia che il proprio funzionario o rappresentante è in possesso della PSC del livello adeguato e della Necessità di Conoscere, e che le Informazioni Classificate saranno protette dalla Parte ricevente in conformità al presente Accordo.

ARTICOLO 9 – CESSIONE DI INFORMAZIONI CLASSIFICATE AI CONTRAENTI

1. Le Informazioni Classificate ricevute da una Parte ricevente possono essere fornite dalla stessa a un Contraente o potenziale Contraente le cui funzioni richiedano l'accesso a tali informazioni, con il previo consenso scritto della Parte trasmittente. Prima di cedere qualunque Informazione Classificata a un Contraente o potenziale Contraente, la Parte ricevente:

a. Conferma che tale Contraente o potenziale Contraente e le strutture di esso abbiano la capacità di tutelare le informazioni in conformità con le condizioni stabilite dal presente Accordo;

b. Conferma che tale Contraente o potenziale Contraente e le strutture di esso siano in possesso delle adeguate PSC e FSC, ove richiesto;

c. Conferma che tale Contraente o potenziale Contraente abbia posto in essere procedure atte a garantire che tutti gli individui che hanno accesso alle informazioni siano consapevoli delle proprie responsabilità in merito alla protezione di tali informazioni in conformità con le leggi e i regolamenti nazionali applicabili;

d. Svolge periodicamente ispezioni di sicurezza delle strutture abilitate, al fine di garantire che le informazioni siano protette come stabilito dal presente Accordo;

e. Conferma che il Contraente o potenziale Contraente abbia posto in essere procedure atte ad assicurare che l'accesso alle informazioni sia limitato a quegli individui che hanno una Necessità di Conoscere.

ARTICOLO 10 – CONTRATTI CLASSIFICATI

1. Quando una Parte propone di stipulare, o autorizza un Contraente nel proprio territorio a stipulare, un Contratto Classificato al livello RISERVATISSIMO / CONFIDENTIAL o superiore con un Contraente nel territorio dell'altra Parte, la Parte che stipula o autorizza il Contraente a stipulare tale Contratto Classificato richiede una garanzia che una FSC è stata rilasciata dall'Autorità Nazionale di Sicurezza dell'altra Parte. L'Autorità Nazionale di Sicurezza della Parte che riceve la richiesta monitora e svolge tutte le azioni necessarie per garantire che la condotta del Contraente per gli aspetti di sicurezza sia conforme alle leggi e ai regolamenti applicabili.

2. L'Autorità Nazionale di Sicurezza di una Parte che negozia un Contratto Classificato la cui esecuzione avverrà nel territorio dell'altra Parte inserirà nel Contratto Classificato, nell'invito a presentare l'offerta, ovvero nel subcontratto, idonee clausole di sicurezza e ulteriori disposizioni rilevanti, anche in relazione ai costi per la sicurezza. Tali disposizioni includono la necessità che ogni Contraente preveda idonee clausole di sicurezza nella propria documentazione contrattuale.

ARTICOLO 11 – RESPONSABILITA' SULLE STRUTTURE

Ciascuna Parte è responsabile per la sicurezza di tutte le strutture governative, private e degli stabilimenti presso i quali sono custodite Informazioni Classificate dell'altra Parte, e garantisce che tali strutture o stabilimenti abbiano attribuito a persone qualificate e adeguatamente abilitate la responsabilità e l'autorità per il controllo e la protezione di tali informazioni.

ARTICOLO 12 – CUSTODIA DELLE INFORMAZIONI CLASSIFICATE

Le Informazioni Classificate scambiate tra le Parti sono custodite in modo da consentire l'accesso esclusivamente da parte di individui autorizzati ad accedervi.

ARTICOLO 13 - TRASMISSIONE

1. Le Informazioni Classificate sono trasmesse tra le Parti attraverso canali governativi ovvero attraverso altri canali reciprocamente e previamente approvati per iscritto.

2. I requisiti minimi per la sicurezza delle Informazioni Classificate durante la trasmissione sono i seguenti:

a. Documenti o altri supporti:

(1) Documenti o altri supporti contenenti Informazioni Classificate sono trasmessi in doppia busta sigillata. La busta interna reca la sola indicazione della classifica dei documenti o altri supporti e dell'indirizzo dell'organizzazione del destinatario. La busta esterna indica l'indirizzo dell'organizzazione del destinatario, l'indirizzo dell'organizzazione del mittente, e il numero di controllo del documento, se del caso.

(2) Nessuna indicazione della classifica dei documenti o dei supporti contenuti nella busta è recata sulla busta esterna. La doppia busta sigillata è trasmessa secondo le procedure prescritte dalle Parti.

(3) Per spedizioni trasmesse tra le Parti, contenenti documenti o supporti recanti Informazioni Classificate, le ricevute sono predisposte dal mittente. Tali ricevute sono firmate dal destinatario finale e restituite al mittente.

b. Materiali:

(1) I materiali, comprese le attrezzature, che contengono Informazioni Classificate sono trasportati con veicoli coperti e chiusi, o, in alternativa, sono imballati in modo sicuro, ovvero protetti e tenuti sotto controllo continuo al fine di evitare la loro perdita o la divulgazione non autorizzata.

(2) I materiali, comprese le attrezzature, che contengono Informazioni Classificate che devono essere depositati temporaneamente in attesa della spedizione sono collocati in aree di stoccaggio protette. Tali aree sono protette attraverso sistemi di rilevamento di intrusioni, ovvero da guardie munite di PSC che ne garantiscono la continua sorveglianza. Solo personale autorizzato, munito di adeguata PSC, può accedere alle aree di stoccaggio protette.

(3) Ogni qual volta i materiali che contengono Informazioni Classificate, comprese le attrezzature, sono oggetto di passaggio di consegne durante il trasporto, è necessario l'ottenimento di una ricevuta, la quale deve essere firmata dal destinatario finale e restituita al mittente.

c. Trasmissione elettronica:

(1) Le Informazioni Classificate al livello RISERVATISSIMO / CONFIDENTIAL e superiore oggetto di trasmissione elettronica sono trasmesse utilizzando mezzi sicuri, approvati dalle Autorità Nazionali di Sicurezza di ciascuna Parte.

ARTICOLO 14 – VISITE A STRUTTURE E STABILIMENTI DELLE PARTI

1. Le visite di rappresentanti di una Parte alle strutture e agli stabilimenti dell'altra Parte, che comportino l'accesso a Informazioni Classificate, ovvero visite per cui sia richiesta una PSC ai fini dell'accesso, sono limitate a quelle necessarie per scopi ufficiali. L'autorizzazione è rilasciata esclusivamente a rappresentanti in possesso di PSC in corso di validità.

2. L'autorizzazione alla visita di tali strutture e stabilimenti è rilasciata esclusivamente dalla Parte nel cui territorio sono collocate le strutture o stabilimenti oggetto della visita. La Parte visitata, o i sui funzionari designati, hanno la responsabilità di informare la struttura o lo stabilimento della visita proposta, nonché l'oggetto e il massimo livello di Informazioni Classificate che possono essere fornite ai visitatori.

3. Le richieste di visita da parte di rappresentanti delle Parti sono presentate dall'Ambasciata d'Italia a Washington, D.C., in caso di visitatori italiani, e dall'Ambasciata degli Stati Uniti a Roma in caso di visitatori statunitensi.

ARTICOLO 15 – VISITE DI SICUREZZA

L'attuazione dei requisiti di sicurezza stabiliti in questo Accordo può essere verificata attraverso visite reciproche di esperti di sicurezza delle Parti. Agli esperti di sicurezza di ciascuna Parte, previa consultazione, è permesso di visitare l'altra Parte per discutere e osservare le procedure attuative della stessa, al fine di conseguire un soddisfacente livello di comparabilità tra sistemi di sicurezza. La Parte ospitante assiste gli esperti di sicurezza nell'attività di valutazione dell'adeguatezza delle misure di protezione accordate alle Informazioni Classificate ricevute dall'altra Parte.

ARTICOLO 16 – STANDARD DI SICUREZZA

Su richiesta, ciascuna Parte fornisce all'altra Parte informazioni sui propri standard, pratiche e procedure di sicurezza per la tutela delle Informazioni Classificate.

ARTICOLO 17 – RIPRODUZIONE DELLE INFORMAZIONI CLASSIFICATE

Quando le Informazioni Classificate sono riprodotte, tutti i contrassegni di sicurezza originali apposti su di esse sono parimenti riprodotti, marcati o applicati su ciascuna riproduzione di tali informazioni. Tali riproduzioni sono soggette agli stessi controlli previsti per le informazioni originali. Il numero delle riproduzioni è limitato al minimo richiesto per i fini ufficiali.

ARTICOLO 18 – DISTRUZIONE DELLE INFORMAZIONI CLASSIFICATE

1. I documenti e gli altri supporti contenenti Informazioni Classificate sono distrutti attraverso l'incenerimento, la tritatura, la macerazione, ovvero altri mezzi che prevengano la ricostruzione delle Informazioni Classificate ivi contenute.

2. I materiali, compresc le attrezzature, che contengono Informazioni Classificate sono distrutti mediante strumenti che li rendano non più riconoscibili al fine di impedire la ricostruzione delle Informazioni Classificate per intero o in parte.

ARTICOLO 19 – RIDUZIONE DI CLASSIFICA E DECLASSIFICA

1. Le Parti convengono che il livello di classifica delle Informazioni Classificate possa essere ridotto non appena tali informazioni cessino di richiedere tale più elevato livello di protezione, ovvero che le informazioni possano essere declassificate non appena le stesse non richiedano più alcuna protezione dalla divulgazione non autorizzata.

2. La Parte trasmittente ha il potere di ridurre il livello di classifica delle proprie Informazioni Classificate, ovvero di declassificarle, in conformità con le leggi, i regolamenti e i protocolli nazionali applicabili. La Parte ricevente non riduce né rimuove il livello di classifica dell'Informazione Classificata ricevuta dalla Parte trasmittente senza il previo consenso scritto della stessa, anche in presenza di apparenti istruzioni di declassifica presenti sul documento.

ARTICOLO 20 – PERDITA O COMPROMISSIONE

All'atto della scoperta la Parte ricevente informa immediatamente la Parte trasmittente di ogni perdita o compromissione di Informazioni Classificate, così come di ogni possibile perdita o compromissione di tali informazioni fornite dalla Parte trasmittente. In caso di perdita o compromissione, effettiva o potenziale di tali informazioni, la Parte ricevente avvia tempestivamente una indagine volta a determinare le circostanze della effettiva o potenziale perdita o compromissione. Le risultanze dell'indagine e un'informativa riguardante le misure adottate per prevenire il ripetersi di tali eventi sono trasmesse alla Parte trasmittente.

ARTICOLO 21 - CONTROVERSIE

Divergenze tra le Parti derivanti da o relative al presente Accordo sono risolte esclusivamente attraverso consultazioni tra le Parti e non sono sottoposte a corti nazionali, tribunali internazionali, ovvero altre persone o enti ai fini della risoluzione.

ARTICOLO 22 - COSTI

1. Ciascuna Parte è responsabile del sostenimento dei costi da essa affrontati per l'attuazione del presente Accordo.

2. Tutti gli obblighi assunti dalle Parti ai sensi del presente Accordo sono soggetti alle leggi di bilancio applicabili delle Parti. Le Parti intendono coprire i propri costi sostenuti per l'attuazione del presente Accordo senza superare le loro ordinarie disponibilità di bilancio. Indipendentemente dalla disponibilità di fondi, ciascuna Parte continua a proteggere, nel rispetto delle leggi e dei regolamenti applicabili, le Informazioni Classificate in modalità almeno equivalente al livello di protezione riconosciuto alle Informazioni Classificate dalla Parte trasmittente.

ARTICOLO 23 – DISPOSIZIONI FINALI

1. Il presente Accordo entra in vigore alla data della ricezione dell'ultima delle due notifiche scritte con cui le Parti si sono informate, tramite canali diplomatici, che le procedure interne per l'entrata in vigore di esso sono state completate.

2. Il presente Accordo è attuato nel rispetto delle normative nazionali delle Parti.

3. Ciascuna Parte può denunciare questo Accordo dando notifica all'altra Parte per iscritto, attraverso canali diplomatici, della propria intenzione in tal senso, novanta giorni prima della data in cui intende terminare l'efficacia dell'Accordo.

4. Anche in caso di cessazione del presente Accordo, tutte le Informazioni Classificate scambiate o in altro modo fornite ai sensi di esso continuano a essere protette in conformità con le disposizioni in esso contenute.

5. L'Accordo tra il Governo della Repubblica Italiana e il Governo degli Stati Uniti concernente la Tutela delle Informazioni Classificate, con relativo annesso, concluso mediante scambio di note a Washington il 4 agosto 1964 ed entrato in vigore il 4 Agosto 1964, e l'emendamento dello stesso, effettuato mediante scambio di lettere il 15 aprile e il 2 settembre 1982, ed entrato in vigore il 2 settembre 1982 (collettivamente denominati l' "Accordo di Sicurezza"), cessano di avere efficacia alla data di entrata in vigore del presente Accordo.

6. Qualunque riferimento all'Accordo di Sicurezza contenuto in altri accordi o intese esistenti tra le Parti è da ritenersi quale riferimento al presente Accordo.

IN FEDE DI CHE i sottoscritti, debitamente autorizzati dai rispettivi Governi, hanno firmato il presente Accordo.

Fatto a ROMA il 25 LUGLIO 2024 in due originali, ognuno in lingua italiana e inglese, entrambe le versioni facendo egualmente fede.

PER IL GOVERNO DELLA REPUBBLICA ITALIANA:	**PER IL GOVERNO DEGLI STATI UNITI D'AMERICA:**
Direttore Generale del Dipartimento delle Informazioni per la Sicurezza	**Ambasciatore degli Stati Uniti d'America in Italia**

APPENDICE

PROCEDURE PER LA PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE ITALIANE RECANTI LIVELLO RISERVATO FORNITE AGLI STATI UNITI

1. A seguito di ricezione, le Informazioni Classificate italiane trasmesse agli Stati Uniti e contrassegnate come "RISERVATO" sono protette dagli Stati Uniti nel rispetto delle procedure che seguono.

2. Le informazioni contrassegnate come "RISERVATO" sono custodite in contenitori chiusi a chiave posti all'interno di aree chiaramente delimitate e dotate di misure di protezione minime tali da impedire l'accesso di personale non autorizzato.

3. Le informazioni a livello "RISERVATO" non sono divulgate a persone o enti non autorizzati senza il previo consenso scritto del Governo Italiano, a meno che ciò non sia richiesto dalla legislazione degli Stati Uniti, ivi incluso il *Freedom of Information Act*.

4. Le informazioni a livello "RISERVATO" sono, a seconda dei casi, custodite, trattate e trasmesse elettronicamente utilizzando sistemi accreditati. In particolare, ogni sistema, prima di essere impiegato per la custodia, trattazione o trasmissione di informazioni a livello "RISERVATO", deve ricevere un'approvazione di sicurezza, denominata Accreditamento. Un Accreditamento è una dichiarazione formale, da parte della competente autorità di accreditamento, attestante che l'uso di un sistema soddisfa adeguati requisiti di sicurezza e non presenta rischi non accettabili. Le Procedure Operative per gli Standard di Sicurezza sono procedure tecniche per l'attuazione di protocolli e requisiti di sicurezza, valide esclusivamente per una specifica struttura, per la protezione di sistemi automatizzati che trattano Informazioni Classificate. Per sistemi di informazione automatizzati stand-alone, quali computer fissi e portatili, utilizzati nelle strutture del Governo statunitense, il documento di registrazione al sistema e le Procedure Operative per gli Standard di Sicurezza devono soddisfare i requisiti di Accreditamento. Una guida all'uso di sistemi di informazione e comunicazione per i Contraenti viene integrata nella *Restricted Conditions Requirements Clause* del Contratto.

5. Le informazioni "RISERVATO" sono trasmesse all'interno degli Stati Uniti con posta prioritaria in busta chiusa, a condizione che la trasmissione sia tracciabile. La trasmissione al di fuori degli Stati Uniti avviene in doppia busta chiusa, con la busta interna recante il contrassegno "RISERVATO". La trasmissione al di fuori degli Stati Uniti avviene mediante mezzi tracciabili, quali corrieri commerciali o altri strumenti concordati tra le Parti.

6. I documenti redatti dagli Stati Uniti che contengono informazioni a livello "RISERVATO" recano sulla copertina e sulla prima pagina il contrassegno "RISERVATO". Le sezioni del documento contenenti informazioni "RISERVATO" sono identificate mediante lo stesso contrassegno.

7. L'accesso a o la trasmissione elettronica di informazioni a livello "RISERVATO" può avvenire attraverso reti pubbliche, quale internet, utilizzando sistemi di cifratura reciprocamente accettati dalle Parti. Le conversazioni telefoniche, le video conferenze o le trasmissioni di fax contenenti

informazioni "RISERVATO" possono essere effettuate in circostanze eccezionali, laddove un sistema di cifratura non sia disponibile, e a condizione che l'Autorità Nazionale di Sicurezza della Parte trasmittente acconsenta.

8. Per l'esecuzione di contratti che richiedono solamente la ricezione o la produzione di Informazioni Classificate al livello "RISERVATO" non è necessaria la FSC.

9. L'Accesso alle informazioni a livello "RISERVATO" è consentito esclusivamente agli individui che hanno la Necessità di Conoscere. Il possesso di una PSC non è necessario per accedere a informazioni a livello "RISERVATO".

AGREEMENT BETWEEN
THE GOVERNMENT OF THE ITALIAN REPUBLIC
AND
THE GOVERNMENT OF THE UNITED STATES OF AMERICA
CONCERNING SECURITY MEASURES FOR THE PROTECTION OF CLASSIFIED INFORMATION

PREAMBLE

The Government of the Italian Republic ("Italian Republic") and the Government of the United States of America (the "United States") (each a "Party," and collectively the "Parties"),

Considering that the Parties cooperate in matters including, but not limited to, foreign affairs, defense, security, law enforcement, science, industry, and technology, and

Having a mutual interest in the protection of Classified Information exchanged in confidence between the Parties,

Have agreed as follows:

ARTICLE 1 – DEFINITIONS

For the purpose of this Agreement the following definitions apply:

1. Classified Information: Information provided by one Party to the other Party that is designated as classified by the releasing Party for national security purposes and therefore requires protection against unauthorized disclosure. The information may be in oral, visual, electronic, or documentary form, or in the form of material, including equipment or technology.

2. Classified Contract: A contract that requires, or will require, access to, or production of, Classified Information by a Contractor or by its employees in the performance of the contract.

3. Contractor: An individual or a legal entity, possessing the legal capacity to conclude contracts, who is a party to a Classified Contract.

4. Facility Security Clearance (hereinafter "FSC"): A certification provided by the National Security Authority of a Party, as designated in Article 4, for a Contractor facility under the Party's jurisdiction that indicates the facility is cleared to a specified level and also has suitable security safeguards in place at a specified level to safeguard Classified Information. Such a certification shall signify that Classified Information at the RISERVATISSIMO / CONFIDENTIAL level or above shall be protected by the Contractor for which the FSC is provided in accordance with the provisions of this Agreement and that compliance shall be monitored and enforced by the relevant National Security Authority. An FSC is not required for a Contractor to undertake contracts that only require the receipt or production of Classified Information at the RISERVATO level.

5. Personnel Security Clearance (hereinafter "PSC"):

a. a determination by the National Security Authority of a Party, as designated in Article 4, that an individual who is employed by a government agency of that Party or a Contractor under the jurisdiction of that Party is authorized to access Classified Information up to a specified level; or

b. a determination by the National Security Authority of a Party, as designated in Article 4, that an individual who is a citizen of such Party but is to be employed by the other Party or by one of the other Party's Contractors is authorized access to Classified Information up to a specified level.

6. Need to Know: A determination made by an authorized holder of Classified Information that a prospective recipient of Classified Information requires access to specific Classified Information in order to perform or assist in a lawful and authorized governmental function.

ARTICLE 2 – LIMITATIONS ON SCOPE OF THE AGREEMENT

This Agreement shall not apply to Classified Information within the scope of the terms of another agreement or arrangement between the Parties or agencies thereof providing for the protection of a particular item or category of Classified Information exchanged between the Parties or agencies thereof, except to the extent that such other agreement or arrangement expressly makes this Agreement's terms applicable. This Agreement also shall not apply to the exchange of Restricted Data, as defined in the U.S. Atomic Energy Act of 1954, as amended (the "AEA"), or to Formerly Restricted Data, which is data removed from the Restricted Data category in accordance with the AEA but still considered to be defense information by the United States.

ARTICLE 3 – COMMITMENT TO THE PROTECTION OF CLASSIFIED INFORMATION

1. Each Party shall protect Classified Information of the other Party according to the terms set forth herein.

2. Classified Information shall be protected by the recipient Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party in accordance with the table in Article 5.

3. Each Party shall promptly notify the other of any changes to its laws and regulations that would affect the protection of Classified Information under this Agreement. The obligations in this Agreement shall not be affected by such changes in domestic law. In such cases, the Parties shall consult regarding possible amendments to this Agreement or other measures that may be appropriate to maintain protection of Classified Information exchanged under this Agreement.

ARTICLE 4 – NATIONAL SECURITY AUTHORITIES

1. The Parties shall inform each other of the National Security Authorities responsible for implementation of this Agreement and any subsequent changes to these Authorities.

2. For the purpose of this Agreement, the National Security Authorities shall be: for the Italian Republic, Presidency of the Council of Ministers – Security Intelligence Department (DIS) – Central

Secrecy Office (UCSe); for the United States, Assistant Director, International Engagement Directorate, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy, U.S. Department of Defense.

3. The Parties may conclude supplemental implementing arrangements to this Agreement where additional security measures may be required to protect Classified Information transferred to the recipient Party through foreign military sales or cooperative programs for co-production or co-development of defense articles or services. Such implementing arrangements may include Special Security Agreements or Industrial Security Agreements.

ARTICLE 5 – DESIGNATION OF CLASSIFIED INFORMATION

1. Classified Information shall be designated, and stamped or marked where possible, by the releasing Party as classified at one of the following national security classification levels. For purposes of ensuring equivalent treatment, the Parties agree that the following security classification levels are equivalent:

ITALIAN REPUBLIC	UNITED STATES
SEGRETISSIMO	TOP SECRET
SEGRETO	SECRET
RISERVATISSIMO	CONFIDENTIAL
RISERVATO	No equivalent (see para. 2 below)

2. During the implementation of this Agreement, if the Italian Republic provides Classified Information designated as "RISERVATO," the United States shall handle it in accordance with the Appendix to this Agreement.

3. Classified Information shall be designated, and stamped or marked where possible, with the name of the releasing Party.

ARTICLE 6 – RESPONSIBILITY FOR CLASSIFIED INFORMATION

The recipient Party shall be responsible for the protection of all Classified Information of the releasing Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party in accordance with the table in Article 5, while the Classified Information is under its control. While in transit, the releasing Party shall be responsible for all Classified Information until custody of the Classified Information is formally transferred to the recipient Party.

ARTICLE 7 – PROTECTION OF CLASSIFIED INFORMATION

1. No individual shall be entitled to have access to Classified Information solely by virtue of rank, position, appointment, or PSC. Access to such information shall be granted only to individuals who have a Need to Know and who have been granted the requisite PSC in accordance with the prescribed standards of the recipient Party.

2. Except as otherwise provided in this Agreement, the recipient Party shall not release Classified Information of the releasing Party to any third party, including any third-party government, individual, firm, institution, organization, or other entity, without the prior written consent of the releasing Party.

3. The recipient Party shall not use or permit the use of Classified Information of the releasing Party for any other purpose than that for which it was provided without the prior written consent of the releasing Party.

4. The recipient Party shall respect any private rights that are associated with Classified Information of the releasing Party, including those rights with respect to patents, copyrights, or trade secrets, and shall not release, use, exchange, or disclose such Classified Information in a manner inconsistent with those rights without the prior written authorization of the owner of those rights.

5. The recipient Party shall ensure that each facility or establishment that handles Classified Information covered by this Agreement maintains a list of individuals at the facility or establishment who are authorized to have access to such information.

6. Each Party shall develop accountability and control procedures to manage the dissemination of, and access to, Classified Information.

7. Each Party shall comply with any and all limitations on use, disclosure, release, and access to Classified Information as may be specified by the releasing Party when it discloses such Classified Information. If a Party is unable to comply with the specified limitations, that Party shall immediately consult with the other Party and shall undertake all lawful measures to prevent or minimize any such use, disclosure, release, or access.

ARTICLE 8 – PERSONNEL SECURITY CLEARANCES

1. The Parties shall ensure that all individuals who in the conduct of their official duties require access or whose duties or functions may afford access to Classified Information pursuant to this Agreement receive an appropriate PSC before they are granted access to such information. A PSC is not required to access Classified Information at the RISERVATO level.

2. The Party granting the PSC shall conduct an appropriate investigation in sufficient detail to determine an individual's suitability for access to Classified Information. The determination to grant a PSC will be made in accordance with the national laws and regulations of the granting Party.

3. Before an official or representative of one Party releases Classified Information to an official or representative of the other Party, the recipient Party shall provide to the releasing Party an assurance

that the official or representative has the necessary PSC level and a Need to Know and that the Classified Information will be protected by the recipient Party in accordance with this Agreement.

ARTICLE 9 – RELEASE OF CLASSIFIED INFORMATION TO CONTRACTORS

1. Classified Information received by a recipient Party may be provided by the recipient Party to a Contractor or prospective Contractor whose duties require access to such information with the prior written consent of the releasing Party. Prior to releasing any Classified Information to a Contractor or prospective Contractor, the recipient Party shall:

a. Confirm that such Contractor or prospective Contractor and the Contractor's facility have the capability to safeguard the information in accordance with the terms of this Agreement;

b. Confirm that such Contractor or prospective Contractor and the Contractor's facility have been granted appropriate PSCs and FSCs, as applicable;

c. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that all individuals having access to the information are informed of their responsibilities to protect the information in accordance with applicable laws and regulations;

d. Carry out periodic security inspections of cleared facilities to ensure that the information is protected as required by this Agreement; and,

e. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that access to the information is limited to those individuals who have a Need to Know.

ARTICLE 10 – CLASSIFIED CONTRACTS

1. When a Party proposes to place, or authorizes a Contractor in its territory to place, a Classified Contract that is classified at the RISERVATISSIMO / CONFIDENTIAL level or above, with a Contractor in the territory of the other Party, the Party that is to place or authorize the Contractor to place such Classified Contract shall request an assurance that an FSC has been issued from the National Security Authority of the other Party. The National Security Authority of the requested Party shall monitor and take all appropriate steps to ensure the security conduct by the Contractor will be in accordance with applicable laws and regulations.

2. The National Security Authority of a Party negotiating a Classified Contract to be performed in the country of the other Party shall incorporate in the Classified Contract, request for proposal, or subcontract document appropriate security clauses and other relevant provisions, including costs for security. This includes provisions requiring any Contractors to include appropriate security clauses in their contract documents.

ARTICLE 11 – RESPONSIBILITY FOR FACILITIES

Each Party shall be responsible for the security of all government and private facilities and establishments where it stores Classified Information of the other Party and shall ensure that such facilities or establishments have qualified and appropriately cleared individuals appointed with the responsibility and authority for the control and protection of such information.

ARTICLE 12 – STORAGE OF CLASSIFIED INFORMATION

Classified Information exchanged between the Parties shall be stored in a manner that ensures access only by those individuals who have been authorized access.

ARTICLE 13 – TRANSMISSION

1. Classified Information shall be transmitted between the Parties through government-to-government channels or other channels mutually approved in advance in writing.

2. The minimum requirements for the security of Classified Information during transmission shall be as follows:

a. Documents or other media:

(1) Documents or other media containing Classified Information shall be transmitted in double, sealed envelopes. The inner envelope shall indicate only the classification of the documents or other media and the organizational address of the intended recipient. The outer envelope shall indicate the organizational address of the intended recipient, the organizational address of the sender, and the document control number, if applicable.

(2) No indication of the classification of the enclosed documents or other media shall be made on the outer envelope. The double sealed envelope shall be transmitted according to the prescribed procedures of the Parties.

(3) Receipts shall be prepared by the sender for packages containing documents or other media containing Classified Information that are transmitted between the Parties, and such receipts shall be signed by the final recipient and returned to the sender.

b. Material:

(1) Material, including equipment, that contains Classified Information shall be transported in sealed, covered vehicles, or shall otherwise be securely packaged or protected and kept under continuous control in order to prevent unauthorized disclosure or loss.

(2) Material, including equipment that contains Classified Information that must be stored temporarily awaiting shipment shall be placed in protected storage areas. Such areas shall be protected by intrusion detection equipment or guards with requisite PSCs who shall maintain continuous surveillance of those areas. Only authorized personnel with the requisite PSC shall have access to the protected storage areas.

(3) Receipts shall be obtained whenever material that contains Classified Information, including equipment, changes hands during transit, and a receipt for such material shall be signed by the final recipient and returned to the sender.

c. Electronic transmissions:

(1) Classified Information that is classified at the RISERVATISSIMO / CONFIDENTIAL level or above that is to be transferred electronically shall be transmitted using secure means that have been approved by each Party's National Security Authority.

ARTICLE 14 – VISITS TO FACILITIES AND ESTABLISHMENTS OF THE PARTIES

1. Visits by representatives of one Party to facilities and establishments of the other Party that require access to Classified Information, or visits for which a PSC is required to permit access, shall be limited to those necessary for official purposes. Authorization shall only be granted to representatives who possess a valid PSC.

2. Authorization to visit such facilities and establishments shall be granted only by the Party in whose territory the facility or establishment to be visited is located. The visited Party, or its designated officials, shall be responsible for advising the facility or establishment of the proposed visit, and the scope and highest level of Classified Information that may be furnished to the visitor.

3. Requests for visits by representatives of the Parties shall be submitted by the Embassy of the Italian Republic in Washington, D.C. in the case of Italian visitors, and by the Embassy of the United States in Rome in the case of U.S. visitors.

ARTICLE 15 – SECURITY VISITS

Implementation of security requirements set out in this Agreement may be verified through reciprocal visits by security experts of the Parties. The security experts of each Party, after prior consultation, shall be permitted to visit the other Party to discuss and observe the implementing procedures of the other Party in the interest of achieving reasonable comparability of security systems. The host Party shall assist the visiting security experts in determining whether Classified Information received from the other Party is being adequately protected.

ARTICLE 16 – SECURITY STANDARDS

On request, each Party shall provide the other Party with information about its security standards, practices, and procedures for safeguarding of Classified Information.

ARTICLE 17 – REPRODUCTION OF CLASSIFIED INFORMATION

When Classified Information is reproduced, all of the original security markings thereon shall also be reproduced, stamped, or marked on each reproduction of such information. Such reproductions shall be subject to the same controls as the original information. The number of reproductions shall be limited to the minimum number required for official purposes.

ARTICLE 18 – DESTRUCTION OF CLASSIFIED INFORMATION

1. Documents and other media containing Classified Information shall be destroyed by burning, shredding, pulping, or other means that prevent reconstruction of the Classified Information contained therein.

2. Material, including equipment, containing Classified Information shall be destroyed through means that render it no longer recognizable so as to preclude reconstruction of the Classified Information in whole or in part.

ARTICLE 19 – DOWNGRADING AND DECLASSIFICATION

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

2. The releasing Party has authority to downgrade or declassify its own Classified Information in accordance with its applicable national laws, regulations, and policies. The recipient Party shall not downgrade the security classification or declassify Classified Information received from the releasing Party, notwithstanding any apparent declassification instructions on the document, without the prior written consent of the releasing Party.

ARTICLE 20 – LOSS OR COMPROMISE

The recipient Party shall inform the releasing Party immediately upon discovery of all losses or compromises, as well as possible losses or compromises, of Classified Information transmitted by the releasing Party. In the event of an actual or possible loss or compromise of such information, the recipient Party shall initiate an investigation immediately to determine the circumstances of the actual or possible loss or compromise. The results of the investigation and information regarding measures taken to prevent recurrence shall be provided to the releasing Party.

ARTICLE 21 – DISPUTES

Disagreements between the Parties arising under or relating to this Agreement shall be settled solely through consultations between the Parties and shall not be referred to a national court, an international tribunal, or any other person or entity for settlement.

ARTICLE 22 – COSTS

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

2. All obligations of the Parties under this Agreement shall be subject to the relevant appropriations laws of the Parties. The Parties intend to cover their own costs incurred in implementing this Agreement without exceeding their ordinary budget availability. Notwithstanding the availability of funds, each Party shall, in accordance with applicable laws and regulations, continue to protect Classified Information in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party.

ARTICLE 23 – FINAL PROVISIONS

1. This Agreement shall enter into force on the date of receipt of the later note in an exchange of notes between the Parties, through diplomatic channels, indicating that each Party has completed its internal procedures required for entry into force of this Agreement.

2. This Agreement shall be implemented in accordance with the national laws of the Parties.

3. Either Party may terminate this Agreement by notifying the other Party in writing through diplomatic channels of its intention to terminate the Agreement ninety days prior to the intended date of termination.

4. Notwithstanding the termination of this Agreement, all Classified Information exchanged or otherwise provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

5. The Agreement Between the Government of the Italian Republic and the Government of the United States Relating to the Safeguarding of Classified Information, with annex, effected by exchange of notes at Washington on August 4, 1964, and entered into force on August 4, 1964, and its amendment, effected by exchange of letters on April 15 and September 2, 1982, and entered into force on September 2, 1982 (collectively, the "Security Agreement"), shall terminate on the date that this Agreement enters into force.

6. Any reference in any other existing agreement or arrangement between the Parties to the Security Agreement shall be considered to be a reference to this Agreement.

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

Done at ROME... this 25 day of JULY 2024., in duplicate, each in the Italian and English languages, both language versions being equally authentic.

FOR THE GOVERNMENT OF THE ITALIAN REPUBLIC:	**FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA:**
Director General of the Security Intelligence Department	**U.S. Ambassador to Italy**

APPENDIX

PROCEDURES FOR PROTECTING ITALIAN RISERVATO CLASSIFIED INFORMATION PROVIDED TO THE UNITED STATES

1.Upon receipt, Italian Classified Information provided to the United States and designated as "RISERVATO" shall be protected by the United States in accordance with the following procedures.

2. Information designated as "RISERVATO" shall be stored in locked containers within clearly delimited areas equipped with minimum protection measures so as to prevent access by unauthorized personnel.

3. "RISERVATO" information shall not be disclosed to unauthorized persons or entities without the prior written approval of the Italian Republic except as required by U.S. law, including the Freedom of Information Act.

4. "RISERVATO" information shall, as applicable, be stored, processed, or transmitted electronically using accredited systems. In particular, before any system is used to store, process, or transmit "RISERVATO" information, it must receive security approval, known as Accreditation. An Accreditation is a formal statement by the appropriate accrediting authority confirming that the use of a system meets the appropriate security requirements and does not present an unacceptable risk. Security Standard Operating Procedures are technical procedures to implement security policies and requirements unique to a specific facility to protect automated information systems processing Classified Information. For stand-alone automated information systems such as desktop and laptop computers utilized in U.S. Government establishments, the system registration document together with the Security Standard Operating Procedures shall fulfill Accreditation. For Contractors, guidance on the use of communications and information systems shall be incorporated into the Restricted Conditions Requirements Clause in the Contract.

5. "RISERVATO" information shall be transmitted by first class mail within the United States in one sealed envelope, provided that the transmission can be tracked. Transmission outside the United States shall be in double, sealed envelopes, with the inner envelope marked "RISERVATO." Transmission outside the United States shall be by traceable means such as commercial courier or other means agreed upon by the Parties in writing.

6. U.S. documents that contain "RISERVATO" information shall bear on the cover and the first page the marking "RISERVATO." The portion of the documents containing "RISERVATO" information also shall be identified with the same marking.

7. "RISERVATO" information may be transmitted or accessed electronically via a public network like the Internet using encryption devices mutually accepted by the Parties. Telephone conversations, video conferencing, or facsimile transmissions containing "RISERVATO" information may be conducted in exceptional circumstances if an encryption system is not available and subject to the approval of the releasing Party's National Security Authority.

8. An FSC is not required for a Contractor to undertake contracts that require only the receipt or production of Classified Information at the "RISERVATO" level.

9. Access to such "RISERVATO" information shall be granted only to those individuals who have a Need to Know. A PSC is not required to access "RISERVATO" information.