

**Dohoda**

**medzi**

**vládou Slovenskej republiky**

**a**

**vládou Helénskej republiky**

**o ochrane vymieňaných utajovaných  
skutočností**

Vláda Slovenskej republiky  
a  
vláda Helénskej republiky

(ďalej len „zmluvné strany“),

berúc do úvahy, že efektívna spolupráca si môže vyžadovať výmenu utajovaných skutočností medzi zmluvnými stranami,

berúc do úvahy potrebu stanoviť pravidlá na vzájomnú ochranu utajovaných skutočností použiteľných pre budúce dohody a kontrakty o spolupráci medzi zmluvnými stranami, obsahujúce alebo týkajúce sa utajovaných skutočností,

dohodli sa t a k t o :

### **Článok 1** **Vymedzenie pojmov**

Na účely tejto dohody :

(1) „utajované skutočnosti“ sú informácie alebo materiál, ktoré je potrebné chrániť pred neoprávneným prístupom a ktoré boli za také určené bezpečnostnou klasifikáciou:

a) slovo „materiál“ je dokument a akákoľvek časť stroja alebo zariadenia alebo zbrane, ktorá je už vyrobená alebo jej výroba prebieha,

b) slovo „dokument“ je akýkoľvek záznam, bez ohľadu na jeho fyzikálnu formu alebo charakteristiku, zahŕňajúc, ale nie len, všetko písané alebo tlačené, karty a pásky pre spracovanie údajov, mapy, karty, fotografie, maľby, výkresy, rytiny, škice, pracovné poznámky a papiere, kópie urobené kopírovacím papierom a atramentové pásky alebo reprodukcie akýmikoľvek prostriedkami alebo procesom a hlasové, zvukové, magnetické alebo elektronické alebo optické alebo videozáznamy v akejkoľvek forme a prenosné zariadenie ADP s rezidentným počítačovým pamäťovým médiom,

(2) „Národný bezpečnostný úrad (NSA)/Určený bezpečnostný úrad (DSA)“ je úrad v každej krajine zodpovedný za bezpečnosť utajovaných skutočností prijatých z iných krajín,

(3) „poskytujúca strana“ je zmluvná strana tejto dohody, ktorá poskytuje utajované skutočnosti,

(4) „prijímajúca strana“ je zmluvná strana tejto dohody, ktorej sú odovzdávané utajované skutočnosti,

(5) „návštevníci“ sú osoby zastupujúce štát zmluvnej strany, ktoré majú prístup k utajovaným skutočnostiam podľa tejto dohody na území štátu druhej zmluvnej strany,

(6) „kontrahent“ je fyzická osoba alebo právnická osoba, ktorá je právne spôsobilá uzatvárať kontrakty týkajúce sa výskumu, produkcie a obstarávania,

(7) „kontrakt“ je dohoda medzi dvoma alebo viacerými stranami, v ktorom sú vytvorené a definované ich právne vymáhateľné práva a povinnosti,

(8) „utajovaný kontrakt“ je dohoda medzi dvoma alebo viacerými kontrahentmi, v ktorom sú definované ich právne vymáhateľné práva a povinnosti a ktorého súčasťou sú alebo môžu byť utajované skutočnosti,

(9) „tretia strana“ je štát, medzinárodná organizácia alebo právnická osoba, ktoré nie sú zmluvnou stranou tejto dohody,

(10) „kompetentný orgán“ je orgán, ktorý v súlade s vnútroštátnymi právnymi predpismi je zodpovedný za ochranu utajovaných skutočností a za implementáciu tejto dohody. Takéto orgány sú uvedené v článku 3 tejto dohody.

## **Článok 2** **Bezpečnostné klasifikácie**

Bezpečnostné klasifikácie a ich ekvivalenty pre zmluvné strany sú obmedzené na:

<b>SLOVENSKÁ REPUBLIKA</b>	<b>HELÉNSKA REPUBLIKA</b>	<b>EKVIVALENT V ANGLICKOM JAZYKU</b>
PRÍSNE TAJNÉ	AKROS APORRITO	TOP SECRET
TAJNÉ	APORRITO	SECRET
DÔVERNÉ	EMPISTEYTIKO	CONFIDENTIAL
VYHRADENÉ	CHRISSIS	RESTRICTED

## **Článok 3** **Kompetentné orgány**

(1) Kompetentnými orgánmi štátov zmluvných strán sú:

v Slovenskej republike:

Národný bezpečnostný úrad (NSA)  
Budatínska 30  
850 07 Bratislava  
Slovenská republika

v Helénskej republike:

a) Národný bezpečnostný úrad (NSA)

NATIONAL SECURITY AUTHORITY (NSA)  
Hellenic National Defence General Staff

Military Intelligence Joint Directorate  
Security Counterintelligence Department  
(HNDGS/MIJD/SCID)  
Mesogion Ave STG 1020  
Athens, Greece

b) Určený priemyselný bezpečnostný úrad (DSA)

Hellenic Ministry of National Defence (Ministerstvo národnej bezpečnosti HR)  
General Secretariat/General Directorate for Defence Industry and Research  
(Generálny sekretariát/Generálne riaditeľstvo pre obranný priemysel a výskum)  
Stratopedo „FAKINO“ STG 1020  
Athens, Greece

(2) Kompetentné orgány si navzájom vybavujú oficiálne žiadosti.

(3) Kompetentné orgány sa navzájom informujú o platných predpisoch platných na území ich štátov, ktoré upravujú ochranu utajovaných skutočností.

(4) Kompetentné orgány môžu na požiadanie jedného z nich mať konzultácie s cieľom zabezpečenia úzkej spolupráce pri implementácii tejto dohody.

(5) S cieľom získania a udržania porovnateľných štandardov bezpečnosti si kompetentné orgány, na základe žiadosti, poskytnú informácie o bezpečnostných štandardoch, postupoch a praxi pri ochrane utajovaných skutočností, ktoré využíva príslušná zmluvná strana.

(6) Kompetentné orgány môžu uzatvárať vykonávacie protokoly k tejto dohode. Iné určené bezpečnostné úrady štátov zmluvných strán môžu uzatvárať vykonávacie protokoly k tejto dohode po predchádzajúcej konzultácii s príslušnými kompetentnými orgánmi.

#### **Článok 4**

#### **Ochrana utajovaných skutočností**

(1) Zmluvné strany si navzájom uznávajú osvedčenia o personálnych bezpečnostných preverkách a potvrdenia o priemyselných bezpečnostných preverkách druhého štátu v súlade s ich vnútroštátnymi právnymi predpismi.

(2) Prístup k utajovaným skutočnostiam je obmedzený len na tie osoby, ktoré ich potrebujú poznať (princíp need to know) a u ktorých bola vykonaná bezpečnostná preverka NSA/DSA alebo kompetentným orgánom prijímajúcej strany, v súlade s ich vnútroštátnymi právnymi predpismi, zodpovedajúca stupňu utajenia sprístupňovanej informácie.

(3) Poskytujúca strana zabezpečí, že prijímajúca strana je informovaná o:

a) bezpečnostnej klasifikácii utajovanej skutočnosti a o podmienkach poskytnutia alebo obmedzeniach jej použitia a o tom, že utajované dokumenty sú takto označené,

b) akejkoľvek následnej zmene v bezpečnostnej klasifikácii.

(4) Prijímajúca strana:

a) v súlade s jej vnútroštátnymi právnymi predpismi udelí utajovaným skutočnostiam taký stupeň bezpečnostnej ochrany, aké majú jej vlastné utajované skutočnosti rovnakého stupňa podľa článku 2,

b) zabezpečí, že bezpečnostné klasifikácie nie sú zmenené a utajované skutočnosti nie sú odtajnené, ak nie je na to písomné oprávnenie poskytovajúcej strany alebo v jej mene.

## **Článok 5**

### **Obmedzenia pri používaní a poskytnutí**

(1) Prijímajúca strana neposkytne, nepoužije, ani nepovolí poskytnutie ani použitie utajovaných skutočností okrem účelov a obmedzenia daného poskytovajúcou stranou alebo v jej mene, ak nie je daný výslovný písomný súhlas v opačnom zmysle.

(2) Poskytnuté utajované skutočnosti sa nesprístupnia tretej strane bez predchádzajúceho písomného súhlasu poskytovajúcej strany.

## **Článok 6**

### **Prenos utajovaných skutočností**

(1) Utajované skutočnosti sa vymieňajú medzi oboma zmluvnými stranami diplomatickou cestou.

(2) Iné schválené spôsoby prenosu alebo výmeny utajovaných skutočností vrátane elektromagnetických spôsobov môžu byť použité, ak sa na tom dohodnú kompetentné orgány.

## **Článok 7**

### **Preklady a rozmnožovanie**

(1) Preklady utajovaných skutočností môžu vykonávať len osoby, u ktorých bola vykonaná bezpečnostná preverka zodpovedajúca stupňu utajenia originálneho dokumentu. Preklad musí byť označený rovnakým stupňom utajenia ako originál a vyjadrovať, že preklad obsahuje utajované skutočnosti štátu poskytovajúcej strany.

(2) V prípade rozmnožovania utajovaných skutočností musia byť všetky kópie označené rovnakým stupňom utajenia ako pôvodný dokument. Počet kópií utajovaných skutočností je obmedzený len na počet potrebný na služobné účely.

(3) Preklad a kópie utajovaných skutočností označených ako PRÍSNE TAJNÉ a TAJNÉ je možné vykonať len na základe písomného povolenia príslušného orgánu štátu poskytujúcej strany.

## **Článok 8 Likvidácia**

(1) Utajované skutočnosti a ich nosiče musia byť zničené alebo modifikované tak, aby sa zabránilo akejkoľvek možnosti ich obnovy.

(2) Utajované skutočnosti označené ako PRÍSNE TAJNÉ a TAJNÉ nesmú byť prijímajúcou stranou zničené bez písomného súhlasu poskytujúcej strany. Kópia záznamu o zničení týchto utajovaných skutočností sa doručí príslušnému orgánu poskytujúcej strany.

(3) V prípade výnimočnej situácie ako je kríza, konflikty alebo vojnové stavy, prijímajúca strana môže zničiť utajované skutočnosti označené ako PRÍSNE TAJNÉ a TAJNÉ bez písomného súhlasu poskytujúcej strany a doručí kópiu záznamu o zničení týchto utajovaných skutočností kompetentnému orgánu poskytujúcej strany v čo najkratšom čase.

## **Článok 9 Utajované kontrakty**

(1) V prípade, že jedna zmluvná strana zamýšľa uzavrieť utajovaný kontrakt s kontrahentom, ktorý má bydlisko alebo sídlo na území štátu druhej zmluvnej strany, potom kompetentný orgán prijímajúcej strany vydá ubezpečenie, že navrhovaný kontrahent má bezpečnostnú previerku zodpovedajúcu stupňu utajenia poskytovaných utajovaných skutočností v rámci navrhovaného utajovaného kontraktu a implementoval príslušné bezpečnostné opatrenia na zabezpečenie ochrany utajovaných skutočností. Toto ubezpečenie taktiež obsahuje povinnosť zabezpečiť, že bezpečnostné opatrenia prevereného kontrahenta korešpondujú s vnútroštátnymi právnymi predpismi o ochrane utajovaných skutočností a že kompetentný orgán dozerá na tieto opatrenia.

(2) Kompetentný orgán alebo určený bezpečnostný úrad kontrahenta je zodpovedný za zabezpečenie, aby každá utajovaná skutočnosť, ktorá bola poskytnutá alebo vytvorená v súvislosti s utajovaným kontraktom, mala udelenú príslušnú bezpečnostnú klasifikáciu.

(3) Kompetentný orgán alebo určený bezpečnostný úrad jednej zmluvnej strany môže zaslať kompetentnému orgánu alebo určenému bezpečnostnému úradu kontrahenta zoznam bezpečnostných požiadaviek. Prijímajúca strana písomne potvrdí prijatie požadovaného zoznamu bezpečnostných požiadaviek a zašle ho kontrahentovi.

(4) Určený bezpečnostný úrad alebo kompetentný orgán kontrahenta zabezpečí, že kontrahent bude narábať s utajovanými skutočnosťami kontraktu

rovnakým spôsobom ako s utajovanými skutočnosťami štátu kontrahenta v súlade so stupňom utajenia stanoveným v zozname bezpečnostných požiadaviek.

(5) V prípade, že kompetentný orgán alebo určený bezpečnostný úrad schváli utajovaný subkontrakt, primerane sa uplatnia odseky (2) a (4) tohto článku.

(6) Kompetentné orgány alebo určené bezpečnostné úrady zmluvných strán zabezpečia, že utajovaný kontrakt je uzavretý, alebo prípadne, že práca na utajovanej časti začne po tom, ako kontrahent implementuje bezpečnostné opatrenia.

## **Článok 10**

### **Návštevy**

(1) Bezpečnostní experti určených bezpečnostných úradov alebo kompetentných orgánov sa môžu pravidelne navštevovať, aby prediskutovali postupy na ochranu utajovaných skutočností.

(2) V prípade, že je potrebný prístup k utajovaným skutočnostiam alebo do priestorov, kde sa utajované skutočnosti pripravujú, nakladá sa s nimi alebo sú uchovávané, vyžaduje sa pre návštevy predchádzajúci súhlas určeného bezpečnostného úradu alebo kompetentného orgánu hostiteľského štátu.

(3) Žiadosť o povolenie návštevy je potrebné zaslať kompetentnému orgánu alebo príslušnému štátnemu orgánu hostiteľského štátu najmenej pätnásť pracovných dní pred plánovaným realizovaním návštevy.

(4) Žiadosť musí obsahovať tieto údaje:

a) meno a priezvisko návštevníka, dátum a miesto narodenia a číslo cestovného dokladu,

b) štátnu príslušnosť,

c) funkciu návštevníka a názov subjektu, ktorý zastupuje a ak je možné názov a ďalšiu bližšiu identifikáciu utajovaného kontraktu, na ktorom sa podieľa,

d) informáciu o stupni bezpečnostnej previerky návštevníka,

d) účel návštevy a predpokladaný dátum príchodu a odchodu,

e) názov inštitúcie alebo spoločnosti, ktorá má byť navštívená.

(5) Všetci návštevníci sa riadia vnútroštátnymi právnymi predpismi o ochrane utajovaných skutočností hostiteľskej zmluvnej strany.

(6) Zoznamy návštevníkov je možné vytvoriť za podmienky, že obe zmluvné strany súhlasia. Tieto zoznamy budú platné na dobu nepresahujúcu dvanásť (12) mesiacov po predchádzajúcom schválení oboch kompetentných orgánov a budú predložené hostiteľskej zmluvnej strane. Keď je zoznam schválený,

príprava návštevy sa môže uskutočniť priamo medzi organizáciami alebo spoločnosťami s ohľadom na zoznam osôb.

(7) Každá zmluvná strana zaručí ochranu osobných údajov návštevníkov v súlade s príslušnými vnútroštátnymi právnymi predpismi.

## **Článok 11 Porušenie bezpečnosti**

(1) Ak došlo k porušeniu bezpečnosti, ktorého výsledkom je isté alebo predpokladané ohrozenie utajovanej skutočnosti, poskytnutej alebo prijatej od druhej zmluvnej strany, kompetentný orgán štátu, v ktorom k ohrozeniu došlo, o tom v čo najkratšom čase informuje kompetentný orgán druhej zmluvnej strany a vykoná náležité vyšetrenie. Druhá zmluvná strana bude, ak to bude požadované, spolupracovať pri vyšetrení.

(2) V prípade, že ohrozenie skutočnosti, ktorá bola poskytnutá podľa článku 5, nastalo v krajine inej, ako sú zmluvné strany, kompetentný orgán odosielajúcej zmluvnej strany prijme opatrenia ako v odseku (1).

(3) V každom prípade bude druhá zmluvná strana informovaná o výsledkoch vyšetrenia a obdrží konečnú správu o príčinách udalosti a rozsahu škôd.

## **Článok 12 Náklady**

Náklady vzniknuté pri vykonávaní tejto dohody sú hradené zmluvnou stranou poskytujúcou služby.

## **Článok 13 Riešenie sporov**

Spory týkajúce sa výkladu alebo vykonávania tejto dohody budú predmetom priamych konzultácií kompetentných orgánov.

## **Článok 14 Záverečné ustanovenia**

(1) Táto dohoda podlieha schváleniu v súlade s vnútroštátnymi právnymi predpismi oboch zmluvných strán a nadobudne platnosť prvým dňom druhého (2.) mesiaca nasledujúceho po dni doručenia neskoršej nóty, ktorou sa zmluvné strany navzájom informujú o tom, že boli splnené podmienky ustanovené vnútroštátnymi právnymi predpismi na nadobudnutie platnosti tejto dohody.

(2) Táto dohoda zostane v platnosti desať (10) rokov. Pokiaľ žiadna zo zmluvných strán neinformuje druhú zmluvnú stranu o úmysle dohodu vypovedať



najmenej šesť (6) mesiacov pred uplynutím doby jej platnosti, predlžuje sa táto dohoda vždy na obdobie ďalších päť (5) rokov.

(3) Zmeny a doplnky tejto dohody nadobudnú platnosť v súlade s ustanovením odseku 1 tohto článku.

(4) V prípade vypovedania tejto dohody všetky utajované skutočnosti vytvorené alebo vymenené medzi zmluvnými stranami na jej základe budú chránené v súlade s ustanoveniami tejto dohody, dokiaľ to ich povaha a klasifikácia bude vyžadovať.

Dané v .....dňa ....., v dvoch pôvodných vyhotoveniach, každé v slovenskom, gréckom a anglickom jazyku, pričom všetky texty sú rovnako autentické.

V prípade rozdielnosti výkladu ustanovení tejto dohody je rozhodujúce znenie textu v anglickom jazyku.

**Za vládu  
Slovenskej republiky**

**Aurel Ugor  
riaditeľ  
Národného bezpečnostného úradu**

**Za vládu  
Helénskej republiky**

**Vassilios Michaloliakos  
námestník  
ministra národnej obrany**

**AGREEMENT**

**Between**

**THE GOVERNMENT OF THE SLOVAK  
REPUBLIC**

**And**

**THE GOVERNMENT OF THE HELLENIC  
REPUBLIC**

**ON THE PROTECTION**

**OF EXCHANGED CLASSIFIED  
INFORMATION**

The Government of the Slovak Republic  
And  
The Government of the Hellenic Republic

Hereinafter referred to as Parties,

Considering that effective co-operation may require exchange of classified information, between the Parties,

Considering the need to set rules regulating the mutual protection of classified information applicable to any future co-operation agreements and contracts between the Parties containing or involving classified information,

Have agreed as follows:

## **Article 1 DEFINITIONS**

For the purpose of the present Agreement:

1.1 "Classified Information", means information or material determined to require protection against unauthorized disclosure which has been so designated by security classification:

the word "material" includes documents and any item of machinery or equipment or weapons either manufactured or in process of manufacture.

the word "document" means any recorded information regardless of its physical form or characteristics, including but not limited to, written or printed matter, data processing cards or tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media.

1.2 "National Security Authority (NSA)/ Designated Security Authority (DSA)" means the Authority in each country responsible for the security of classified information received from other countries.

1.3 "Originating Party" means the party to the present Agreement, which transmits classified information.

1.4 "Receiving Party" means the party to the present Agreement, which classified information is transmitted to.

1.5 "Visitors" means individuals being representatives of the State of a Party who have access to classified information under the present Agreement on the territory of the State of other Party.

1.6 “Contractor” means an individual or legal entity possessing the legal capability to undertake contracts, engaged matters of research, production and procurement.

1.7 “Contract” means an agreement between two or more parties creating and defining enforceable rights and obligations.

1.8 “Classified Contract” is an agreement between two or more contractors defining their enforceable rights and obligations and the part of which shall be or may be classified information.

1.9 “Third Party” means States, International Organizations and legal entity which are not defined as Parties in the Present Agreement.

1.10 “Competent Authority” means the authority which in compliance with national laws and regulations is responsible for the protection of classified information and for the implementation of the present Agreement. Such authorities are stated in Article 3 of this Agreement.

## **Article 2 SECURITY CLASSIFICATIONS**

The security classifications and their equivalents for the Parties will be limited to:

IN THE SLOVAK REPUBLIC	IN THE HELLENIC REPUBLIC	EQUIVALENT IN ENGLISH
PRÍSNE TAJNÉ	AKROS APORRITO	TOP SECRET
TAJNÉ	APORRITO	SECRET
DÔVERNÉ	EMPISTEYTIKO	CONFIDENTIAL
VYHRADENÉ	PERIORISMENIS CHRISIS	RESTRICTED

## **Article 3 COMPETENT AUTHORITIES**

3.1 The Competent Authorities of the States of the Parties are:

For the Slovak Republic

NATIONAL SECURITY AUTHORITY (NSA)  
Budatínska 30  
850 07 Bratislava  
Slovak Republic

For the Hellenic Republic.

a. NATIONAL SECURITY AUTHORITY (NSA)  
Hellenic National Defence General Staff

Military Intelligence Joint Directorate  
Security Counterintelligence Department.  
(HNDGS/MIJD/SCID)  
Mesogion Ave STG 1020  
Athens, Greece

- b. DESIGNATED INDUSTRIAL SECURITY AUTHORITY (DSA)  
Hellenic Ministry of National Defence  
General Secretariat/General Directorate for Defence Industry and  
Research  
Stratopedo "FAKINO" STG 1020  
Athens, Greece

3.2 The Competent Authorities shall provide each other with their official requisites.

3.3 The Competent Authorities shall inform each other of the regulations in force on the territories of their States regulating the protection of classified information.

3.4 In order to ensure close co-operation in the implementation of the present Agreement, the Competent Authorities may hold consultations at the request made by one of them.

3.5 In order to achieve and maintain comparable standards of security, the respective Competent Authorities shall, on request, provide each other with information about the security standards, procedures and practices for protection of classified information employed by the respective Party.

3.6 The Competent Authorities can conclude executive documents to this Agreement. Subject to prior consultation with the respective Competent Authorities, other Designated Security Authorities of the States of the Parties are also allowed to conclude executive documents to this Agreement.

#### **Article 4**

### **PROTECTION OF CLASSIFIED INFORMATION**

4.1 The Parties shall mutually recognize the certificates on Personnel Security Clearances and Facility Security Clearances of the other State issued in accordance with its own national legislation.

4.2 Access to classified information shall be limited to those persons who have a need to know and who have been security cleared by the NSA/DSA or the Competent Authority of the Receiving Party, in accordance with its national laws and regulations, corresponding to the required classification level of the information to be accessed.

4.3 The Originating Party shall ensure that the Receiving Party is informed of:

4.3.1 the security classification of the classified Information and of any conditions of release or limitations on its use, and that the classified documents are so marked.

4.3.2 any subsequent change in security classification.

4.4 The Receiving Party shall:

4.4.1 in accordance with its national law and regulations, afford a level of security protection to classified information as it is afforded to its own classified information of equivalent classification as shown in Article 2.

4.4.2 ensure that security classifications are not amended and classified information is not declassified unless authorized in writing by or on behalf of the Originating Party.

## **Article 5**

### **RESTRICTIONS ON USE AND DISCLOSURE**

5.1 Unless express written consent is given to the contrary, the Receiving Party shall not disclose or use, or permit the disclosure or use of any classified information except for purposes and within any limitation stated by or on behalf of the Originating Party.

5.2 Provided classified information shall not be disclosed to third party without the prior written approval of the Originating Party.

## **Article 6**

### **TRANSMISSION OF CLASSIFIED INFORMATION**

6.1 Classified information will be exchanged between the two Parties by diplomatic channels.

6.2 Other approved means of transmission or exchange of classified information, including electromagnetic means, may be used if agreed upon by the Competent Authorities.

## **Article 7**

### **TRANSLATION AND REPRODUCTION**

7.1 Translation of classified information may be done only by persons having the security clearance corresponding to the classification level of the original document. The translation shall be marked with the same classification level as the original document, indicating that the translation contains classified information of the State of the Originating Party.

7.2 In case of reproduction of the classified information their original classification level shall be reproduced or marked on each copy. The number of copies shall be limited to that required for official use only.

7.3 Translation and copies of classified information marked TOP SECRET and SECRET may be done only on the basis of a written approval of the Competent Authority of the State of the Originating Party.

## **Article 8 DESTRUCTION**

8.1 Classified information and their carriers shall be destroyed or modified in a way to prevent any possibility of their reproduction.

8.2 Classified information marked as TOP SECRET and SECRET shall not be destroyed by the receiving Party without the written consent of the Originating Party. The copy of the report on destruction of this classified information shall be delivered to the Competent Authority of the Originating Party.

8.3 Under exceptional circumstances, as crisis, conflicts or war situations, the Receiving Party may destroy classified information marked as TOP SECRET and SECRET without the written consent of the Originating Party and shall deliver the copy of the report on destruction of this classified information to the Competent Authority of the Originating Party as soon as possible.

## **Article 9 CLASSIFIED CONTRACTS**

9.1 Should a Party consider concluding a classified contract with a Contractor residing in the territory of the State of the other Party, then the Competent Authority of the Receiving party shall issue an assurance that the proposed Contractor has a security clearance corresponding to the required classification level of the provided classified information within the proposed classified contract and has implemented appropriate security arrangement to ensure the protection of classified information. This assurance also involves the obligation to ensure that the security arrangements of the security cleared contractor correspond to national legislation on protection of classified information and that these arrangements are supervised by the Competent Authority.

9.2 The Competent Authority or the Designated Security Authority of the contractor is responsible for ensuring that each piece of classified information, which has been either released or generated in connection with a classified contract, has been assigned relevant security classification.

9.3 The Competent Authority or the Designated Security Authority of one Party may send the Competent Authority or the Designated Security of the

contractor security requirement list. The Receiving Party shall confirm in writing the receipt of the requested security requirements list and forward it to the contractor.

9.4 The Designated Security Authority or the Competent Authority of the contractor shall ensure that the contractor will handle the classified information of a contract in the same manner as the classified information of the State of the contractor, in compliance with the classification level referred in the security requirement list.

9.5 Should the Competent Authority or the Designated Security Authority approve a classified subcontract, the paragraphs (2) and (4) of this Article shall apply accordingly.

9.6 The Competent Authorities or the Designated Security Authorities of the Parties shall ensure that a classified contract is concluded or, eventually, work on classified parts begins, only after the Contractor has implemented security measures.

## **Article 10**

### **VISITS**

10.1 Security experts of the Designated Security Authorities or the Competent Authorities may periodically visit each other in order to discuss the procedures for the protection of classified information.

10.2 The prior approval of the Designated Security Authority or the Competent Authority of the host State shall be required in respect of visitors if access to classified information or to premises where classified information is developed, handled or stored is necessary.

10.3 A request for visit shall be sent to the Competent Authorities or other relevant State bodies of the host State, at least fifteen (15) working days before the planned realization of the visit.

10.4 Request shall include the following information:

10.4.1 Name and surname of visitor, date and place of birth, passport number.

10.4.2 Nationality

10.4.3 Position of visitor and name of institution or company (s)he is representative of, or name and closer identification of classified contract (s)he takes part in.

10.4.4 Information on the level of security clearance of visitor.

10.4.5 Purpose of visit and estimated date of arrival and departure.



10.4.6 Name of institution or company to be visited.

10.4.7 All visitors will comply with the national laws and regulations on protection of classified information of the host Party.

10.5 Subject to the approval of both Parties, it may be possible to establish Visitors Lists. These Lists will be valid for an initial period not exceeding twelve (12) months subject to the prior approval of both Competent Authorities. They should be submitted to the host Party. Once a list has been approved, visit arrangements may be made directly between the establishments or companies involved in respect of listed individuals.

10.6 Each Party shall guarantee the protection of personal data of the visitors according to the respective national laws and regulations.

## **Article 11 BREACH OF SECURITY**

11.1 In case of a breach of security that results in a certain or suspect compromise of classified information, originated or received from the other Party, the Competent Authority of the State where the compromise occurred shall inform the Competent Authority of the other party as soon as possible and carry out the appropriate investigation. The other Party shall, if required, cooperate in the investigation.

11.2 In case the compromise of information which has been disclosed according to Article 5, occurs in a country different from the Parties, the Competent Authority of the dispatching Party shall take the actions as of Paragraph (1)

11.3 In any case, the other party shall be informed of the results of the investigation and shall receive the final statement as to the reasons of the event and the extent of the damage.

## **Article 12 COSTS**

Any cost incurred in the application of the present Agreement shall be borne by the Party providing the services.

## **Article 13 DISPUTES**

Any dispute concerning the interpretation or implementation of the present Agreement shall be resolved by direct consultation between the Competent Authorities.

## **Article 14**

### **FINAL CLAUSES**

14.1 The present Agreement shall be subject to approval in accordance with national laws and regulations of both Parties and shall enter into force on the first day of the second (2) month following the receipt of the last written notification of the Parties informing each other of the completion of their national legal procedures that are necessary for its entering into force.

14.2 The present Agreement shall remain in force for ten (10) years and shall be automatically extended for a further five (5) year period unless by notification sent to the other Party at least six (6) months before the expiration period, either Party informs the other of its intention to terminate the Agreement.

14.3 Any amendments or changes to the Agreement shall enter into force according to the procedures of paragraph 1 of this Article.

14.4 All classified information that have been exchanged or arouse in compliance with this Agreement, shall be protected according to the provisions of this Agreement even after termination of the Agreement, until their nature and classification require so.

Done in ..... on ..... in two original copies, each in the Slovak, Greek and English languages, all texts being equally authentic.

In case of different interpretations of the provisions of this Agreement the English text shall prevail.

For the Government  
of the Slovak Republic

For the Government  
of the Hellenic Republic

Aurel Ugor  
Director of NSA

Vassilios Michaloliakos  
Deputy Minister of National Defense