AGREEMENT

BETWEEN

THE GOVERNMENT OF THE REPUBLIC OF BULGARIA

AND

THE GOVERNMENT OF THE REPUBLIC OF POLAND

ON MUTUAL PROTECTION AND EXCHANGE

OF CLASSIFIED INFORMATION

The Government of the Republic of Bulgaria and the Government of the Republic of Poland, hereinafter referred to as the "Contracting Parties",

aiming to ensure the protection of all the information which has been classified pursuant to the internal legislation of each of the Contracting Parties and transferred to the other Contracting Party

have agreed as follows:

Article 1
Definitions

For the purpose of this Agreement,

(1) **"Classified Information"** means all legally defined information, irrespective of its form, carrier, manner of expression, either generated or in process of generation, which requires protection against unauthorised access;

(2) **"Unauthorised access to Classified Information"** means any form of disclosure of Classified Information, including misuse, damage, submission, destruction and incorrect classification thereof, as well as any other actions, resulting in breach of protection or loss of such information, as well as any actions or inactions that have resulted in making the information known to an unauthorised person;

(3) **"Personnel Security Clearance"** means a document confirming that its holder may be granted access to Classified Information in accordance with the internal legislation of each of the Contracting Parties;

(4) **"Industrial Security Clearance"** means a document confirming that the Contractor may be granted access to Classified Information in connection with a Classified Contract and in accordance with the internal legislation of each of the Contracting Parties;

(5) **"Classified Contract/Subcontract"** means an agreement between two or more persons/legal entities which contains or provides for access to Classified Information;

(6) "**Contractor/Subcontractor**" means a person or a legal entity possessing the legal capacity to conclude contracts or a party to a Classified Contract under the provisions of this Agreement;

(7) "**Competent Security Authority**" means the authority which, in compliance with the internal legislation of each of the Contracting Parties, performs functions regarding the protection of Classified Information, exercises overall control in this sphere as well as conducts the implementation of this Agreement, and is determined as such in Article 3 Paragraph 1 of this Agreement;

(8) "**Organisational Unit**" means an entity which generates, processes, transfers, receives, stores, protects and uses Classified Information in accordance with the internal legislation of each of the Contracting Parties and in compliance with this Agreement;

(9) **"Third Party"** means a state or international organization which is not a Party to this Agreement or any person/legal entity who does not have a Personnel Security Clearance/Industrial Security Clearance, or who was refused such a Clearance after conducting a vetting procedure in accordance with the internal legislation of each of the Contracting Parties and who does not have a need-to-know.

Article 2
Security Classification Levels

(1) The Contracting Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the internal legislation of each of the Contracting Parties.

For the Republic of Bulgaria	For the Republic of Poland	Equivalent in English
СТРОГО СЕКРЕТНО	ŚCIŚLE TAJNE	TOP SECRET
СЕКРЕТНО	TAJNE	SECRET
ПОВЕРИТЕЛНО	POUFNE	CONFIDENTIAL
ЗА СЛУЖЕБНО ПОЛЗВАНЕ	ZASTRZEŻONE	RESTRICTED

(2) The Organisational Units shall inform each other of any case of change or removal of the security classification level of the transferred information.

Article 3
Competent Security Authorities

(1) For the purpose of this Agreement, the Competent Security Authorities shall be:

a. for the Republic of Bulgaria: the State Commission on Information Security.

b. for the Republic of Poland: the Head of the Internal Security Agency (civilian) and the Head of the Military Information Services (military)

(2) The Competent Security Authorities shall inform each other of their internal legislation in force regulating the protection of Classified Information and shall exchange their requisites.

(3) In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall provide each other with information about the security standards, procedures and practices for protection of Classified Information applied by each of the Contracting Parties.

(4) The Competent Security Authorities can sign executive arrangements with regard to the implementation of this Agreement.

Article 4
Principles of the Protection of Classified Information

(1) In compliance with this Agreement and their internal legislation, the Contracting Parties shall implement appropriate measures for protection of Classified Information which is transferred or generated as a result of their mutual activities or in connection with a Classified Contract.

(2) The Receiving Organisational Unit shall afford Classified Information a security classification level equivalent to that

provided by the Originating Organisational Unit in accordance with the principle set forth in Article 2 of this Agreement;

(3) The Competent Security Authorities shall inform each other about any changes in the internal legislation affecting the protection of Classified Information.

(4) In the case referred to in Paragraph 3, the Contracting Parties shall undertake measures aimed at the introduction of appropriate changes to this Agreement. Meanwhile, the Classified Information shall be protected according to the provisions of this Agreement, unless otherwise agreed in writing.

(5) Access to Classified Information transferred or generated in accordance with this Agreement shall be granted only to persons who have a Personnel Security Clearance, issued after conducting an appropriate vetting procedure in accordance to the internal legislation of each of the Contracting Parties and who have a need – to – know.

(6) The Receiving Organisational Unit shall not allow access to the Classified Information to a Third Party without a prior consent of the Originating Organisational Unit who imposed the security classification.

(7) The Receiving Organisational Unit shall not use the Classified Information for purposes other than those for which it was transferred or generated.

Article 5
Transfer of Classified Information

(1) Classified Information shall be transferred by means of diplomatic or military couriers or by other means in accordance with the internal legislations of each of the Contracting Parties. The Receiving Organisational Unit shall confirm in writing the receipt of the Classified Information.

(2) Classified Information shall be transmitted via protected telecommunication systems, networks or electromagnetic means

which have been granted a certificate issued pursuant to the internal legislation of each of the Contracting Parties.

(3) Other means of transfer of Classified Information may also be used if mutually approved by the Competent Security Authorities.

Article 6
Translation, reproduction, destruction

(1) Classified Information marked with a classification level СТРОГО СЕКРЕТНО/ ŚCIŚLE TAJNE/TOP SECRET shall be translated or copied only by written permission of the Competent Security Authority of the Originating Contracting Party.

(2) All translations of Classified Information shall be made by persons who have appropriate Personnel Security Clearance. Such translation shall bear an appropriate security classification marking and a suitable annotation in the language of translation indicating that the translation contains Classified Information of the Originating Organisational Unit.

(3) When Classified Information is reproduced, all original security markings thereon shall also be reproduced or marked on each copy. Such reproduced Classified Information shall be placed under the same control as the original information. The number of copies shall be limited to that required for official purposes.

(4) The Originating Organisational Unit may expressly prohibit reproduction, alteration or destruction of Classified Information by marking the relevant carrier or sending subsequent written notice. In such case, the Classified Information subject to destruction shall be returned to the Originating Organisational Unit.

(5) Classified Information shall be destroyed or modified insofar as to forestall its reconstruction in whole or in part. Classified Information marked as СТРОГО СЕКРЕТНО/ŚCIŚLE TAJNE/TOP SECRET shall not be destroyed or modified. Instead it shall be returned to the Originating Organisational Unit or to the Competent Security Authority in case of liquidation of the Originating Organisational Unit.

Article 7
Classified Contracts

(1) In case a Classified Contract with a potential Contractor residing or having its seat or registered in the territory of the State of the other Contracting Party is to be concluded, the Competent Security Authority for the potential Contractor shall issue a document certifying that it has been granted the Industrial Security Clearance corresponding to the required security classification level and that all of its personnel whose positions and duties require access to Classified Information have been granted the appropriate Personnel Security Clearance.

(2) If the potential Contractor does not meet the requirements referred to in Paragraph 1, the Competent Security Authority which is to issue the certifying document, shall immediately inform the Competent Security Authority of the other Contracting Party that, upon its request, necessary actions shall be taken to start the vetting procedures for issuance of Industrial Security Clearance and Personnel Security Clearances.

(3) Each Classified Contract shall be accompanied by a security instruction. This instruction shall specify the Classified Information released to or generated by the Contractor, the classification level assigned to this information and the different phases of the execution of the Classified Contract. A copy of this document shall be submitted to the Competent Security Authority of each of the Contracting Parties.

(4) The Classified Contract must contain minimum measures for protection of Classified Information regarding generation, transfer and usage of the Classified Information, visits procedures and access to such information. It must be in full conformity with this Agreement and the imperative provisions of the internal legislation of each of the Contracting Parties.

(5) The requirements set forth in this Article shall also fully apply respectively to Subcontracts and Subcontractors.

Article 8
Visits

(1) Experts on Classified Information protection of the Competent Security Authorities shall hold regular meetings to discuss the measures for protection of Classified Information.

(2) Persons arriving on a visit from the territory of one of the Contracting Parties to the territory of the other Contracting Party shall be allowed access to Classified Information to the necessary extent, as well as to the premises where Classified Information is generated, handled or stored, only after prior receipt a written permit issued by the Competent Security Authority of the respective Contracting Party.

(3) The permit referred to in Paragraph 2, shall be granted exclusively to persons granted a Personnel Security Clearance pursuant to their internal legislation.

(4) Requests for visits shall include information concerning:

a. purpose, date and programme of the visit;
b. issues relating to Classified Information that are to be discussed and level of their security classification;
c. name and surname of the proposed visitor, date and place of birth, nationality and passport number or identity card number;
d. position of the visitor together with the name of the institution or facility which he or she represents;
e. certification of the level of Personnel Security Clearance held by the visitor;
f. name and address of the facility to be visited;
g. name, surname and position(s) of the person(s) to be visited, if known.

(5) Each Contracting Party shall guarantee the protection of personal data of the visitors, according to its internal legislation.

Article 9
Breach of Security Regulations

(1) In case of a breach of security regulations resulting from unauthorized access or a risk of unauthorized access to Classified Information generated or transferred in accordance with this Agreement, the Competent Security Authority of the Contracting Party on whose territory such event occurred shall immediately inform the Competent Security Authority of the other Contracting Party and it shall take necessary measures aimed at minimizing effects of such breach.

(2) In case of a breach of security regulations which might affect the protection of Classified Information generated or transferred in accordance with this Agreement, the Contracting Party on whose territory such breach occurred, shall take up appropriate investigation in compliance with its internal legislation.

(3) The Competent Security Authority of the Contracting Party on whose territory the breach of security regulations occurred shall immediately inform the Competent Security Authority of the other Contracting Party of the result of the investigation referred to in Paragraph 2.

Article 10
Expenses

Each Contracting Party shall cover its expenses incurred in the course of implementing its obligations under this Agreement.

Article 11
Settlement of Disputes

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by way of negotiations between the Contracting Parties, if the prior consultations between Competent Security Authorities turn out to be ineffective.

Article 12
Final Provisions

(1) This Agreement shall enter into force fourteen days after the receipt of the last diplomatic note confirming the fulfilment of all the procedures provided for by the internal legislation of each of the Contracting Parties.

(2) This Agreement is concluded for an indefinite period of time.

(3) Each of the Contracting Parties may denounce this Agreement by diplomatic note forwarded to the other Contracting Party. The denunciation shall enter into force six months after the date of receipt of such diplomatic note. Notwithstanding the termination of this Agreement, all Classified Information transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until one of the Contracting Parties dispenses the other Contracting Party from this obligation.

(4) This Agreement may be amended on the basis of mutual written consent by both Contracting Parties. Such amendments shall enter into force in accordance with the provisions of Paragraph 1.

Done at Warsaw on 7-th April 2005 in two original copies, each in the Bulgarian, Polish and English languages, all texts being equally authentic. In case of divergences of interpretation, the English text shall prevail.

FOR THE GOVERNMENT OF THE REPUBLIC OF BULGARIA

TSVETA MARKOVA
Chairperson of the State Commission on Information Security

FOR THE GOVERNMENT OF THE REPUBLIC OF POLAND

ZBIGNIEW GOSZCZYŃSKI
Deputy Head of the Internal Security Agency