LAW No. 273 of 22 December 2010
on the ratification of the Security Agreement between Romania and the Kingdom of Spain on the Mutual Protection of Classified Information, signed in Madrid on 14 May 2010

ISSUER: The PARLIAMENT
PUBLISHED IN: The Official Journal no.14 of 6 January 2011

The Parliament of Romania adopts this law.

SINGLE ARTICLE
The Security Agreement between Romania and the Kingdom of Spain on the Mutual Protection of Classified Information, signed in Madrid on 14 May 2010 is ratified.

This law was adopted by the Parliament of Romania, with the observance of the provisions of Article 75 and Article 76 paragraph (2) of the Constitution of Romania, republished.

PRESIDENT OF THE CHAMBER OF DEPUTIES
ROBERTA ALMA ANASTASE

p. PRESIDENT OF THE SENATE
TEODOR VIOREL MELESCANU

Bucharest, 22 December 2010
No. 273

SECURITY AGREEMENT BETWEEN ROMANIA AND THE KINGDOM OF SPAIN ON THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

Romania and the Kingdom of Spain, hereinafter called the Parties, in order to safeguard the Classified Information exchanged between them, have agreed on the following:

ARTICLE 1
APPLICABILITY

1. This Security Agreement (hereinafter referred to as Agreement) shall form the basis of any activity, involving, in compliance with national legislation, the exchange of Classified Information between the Parties, concerning cases such as:

a) co-operation between the Parties concerning the national defence and any other issue related to national security;

b) co-operation, joint ventures, contracts or any other relation between state bodies or other public or private entities of the Parties in the field of national defence and any other issue related to national security;

c) sales of equipment, products and know-how.

2. This Agreement shall not affect the commitments of both Parties which stem from other international agreements and shall not be used against the interests, security and territorial integrity of other states.

ARTICLE 2
DEFINITIONS

For the purpose of this Agreement:

a. **Classified Information** means:
any information, document or material, regardless of its physical form to which a Security Classification has been assigned in compliance with national legislation and which shall be protected accordingly;

b. **Classified Document** means:
any sort of record containing Classified Information regardless of its form or physical characteristic, including, without limitation, written or printed matters, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions produced by any means or processes, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable automated data processing equipment with resident computer storage media, and removable computer storage media;

c. **Classified Material** means:
any object or item of machinery, prototype, equipment, weapon etc., mechanically or hand made, manufactured or in process of manufacture, to which a Security Classification has been assigned;

d. **Security Classification** means:
the assignment of a national classification in accordance with the legislations of the Parties;

e. **Classified Contract** means:
an agreement between two or more Contractors establishing and defining their rights and obligations and containing or implying Classified Information;

f. **Contractor or Subcontractor** means:
an individual or legal entity possessing the legal capacity to conclude Classified Contracts;

g. **Breach of Security** means:
an act or omission contrary to national legislation, that results in an actual or possible Compromise of Classified Information;

h. **Compromise of Classified Information** means:
a situation when – due to a Breach of Security or adverse activity (such as espionage, act of terrorism or theft) – Classified Information has lost its confidentiality, integrity or availability, or when supporting services and resources have lost their integrity or availability. This includes loss, partial or total disclosure, unauthorized modification and destruction or denial of service;

i. **Security Aspects Letter** means:
a document issued by the appropriate authority as a part of any Classified Contract or subcontract, identifying the security requirements or those elements of the contract requiring security protection;

j. **Security Classification Guide** means:
a listing of Classified Information, materials and activities related to a Classified Contract and their classification levels, included in the Security Aspects Letter;

k. **Personnel Security Clearance** means:
the determination by the National Security Authority/Designated Security Authority that an individual is eligible to have access to Classified Information, in accordance with the respective national legislation;

l. **Facility Security Clearance/Industrial Security Authorization** means:
the determination by the National Security Authority/Designated Security Authority that, from a security point of view, a facility has the physical and organisational capability to use and deposit Classified Information, in accordance with the national legislation;

m. **Need to Know** means:
a principle by which access to Classified Information may be granted individually, only to those persons who, in performing their duties, need to work with or have access to such information;

n. **National Security Authority** means:
an institution empowered with authority at national level which, in compliance with the legislations of the Parties, ensures the unitary implementation of the protective measures for Classified Information. Such authorities are listed in Article 7;

o. **Designated Security Authority** means:
a national authority with specific competences in the field of protection of Classified Information, responsible for implementing the security requirements covered by this Agreement;

p. **Third Party** means:
any individual, institution, national or international organization, private or public entity which is not part to this Agreement.

ARTICLE 3
PROTECTION OF CLASSIFIED INFORMATION

1. In accordance with their legislation, the Parties shall take appropriate measures to protect Classified Information which is transmitted, received, produced or developed as a result of any agreement or relation between them. The Parties shall afford to all the exchanged, received Classified Information the same degree of security protection, according to the equivalence of Security Classification mentioned in Article 4.

2. The receiving Party shall neither use a lower Security Classification for the received Classified Information nor declassify this information without the prior written consent of the National Security Authority of the originating Party. The National Security Authority of the originating Party shall inform the National Security Authority of the receiving Party of any changes in Security Classification of the exchanged information.

3. Reproduction or translation, by any means, of the received Classified Documents shall be made only with the written consent of the originator. All the reproductions of the Classified Documents shall be marked with the same Security Classification as the original copy and shall be protected in the same way as the original information. The number of copies shall limit to that number necessary for official purposes.

4. Classified Documents and materials shall be destroyed only with the written consent or at the request of the originating Party, in accordance with the legislations of the Parties, in such a manner that any reconstruction of Classified Information in whole or in part be impossible. If the originating Party does not agree on the destruction, the Classified Documents or materials shall be returned to it.

5. The receiving Party shall inform the originating Party of the destruction of Classified Information. The STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ/ SECRETO/ TOP SECRET documents or materials shall not be destroyed but returned to the originating Party.

6. Access to locations and facilities where activities involving Classified Information are performed or where Classified Information is stored, shall be allowed only to those individuals having a Personnel Security Clearance corresponding to the Security Classification of the information, with the observance of the Need-to-Know principle.

7. Access to Classified Information is allowed, with the observance of the Need-to-Know principle, only to those individuals having a Personnel Security Clearance valid for the Security Classification of the information for which the access is required.

8. None of the Parties shall release received Classified Information to a Third Party without prior written authorization of the National Security Authority of the Party which releases the information.
This Agreement shall not be invoked by either Party to obtain Classified Information that the other Party has received from a Third Party.

9. Each Party shall supervise the observance of national legislation at the public and/or private entities that hold, develop, produce and/or use Classified Information of the other Party.

10. Before a representative of a Party provides Classified Information to a representative of the other Party, the receiving Party shall notify the originating Party that the former representative has a Personnel Security Clearance of the highest Security Classification for the information to which he/she is to have access, and that the Classified Information is protected in accordance with the provisions of this Agreement.

ARTICLE 4
SECURITY CLASSIFICATIONS

1. The Security Classifications applicable to information exchanged within the framework of this Agreement shall be:

a) For Romania: SECRET DE SERVICIU, SECRET, STRICT SECRET and STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ;
b) For the Kingdom of Spain: DIFUSIÓN LIMITADA, CONFIDENCIAL, RESERVADO and SECRETO.

2. The Parties have determined that the equivalence of the national Security Classifications is as follows:

Romania	The Kingdom of Spain	English language Equivalent
STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ	SECRETO	TOP SECRET
STRICT SECRET	RESERVADO	SECRET
SECRET	CONFIDENCIAL	CONFIDENTIAL
SECRET DE SERVICIU	DIFUSIÓN LIMITADA	RESTRICTED

ARTICLE 5
PERSONNEL SECURITY CLEARANCE

1. Each Party shall guarantee that any individual, who, due to his/her employment or functions needs access to Classified Information, shall have a Personnel Security Clearance corresponding to the appropriate Security Classification performed by the National Security Authority/Designated Security Authority in accordance with the respective national legislation.

2. On request, the National Security Authorities of the Parties, taking into account the respective national legislation, shall assist each other in performing the vetting procedures related to the Personnel Security Clearance and to the Facility Security Clearance/Industrial Security Authorisation. To this purpose specific arrangements may be agreed between the National Security Authorities of the Parties.

3. The Parties shall mutually recognize the Personnel Security Clearance certificates and Facility Security Clearance/Industrial Security Authorisation certificates issued in accordance with the legislation of the respective Party.

4. The National Security Authorities shall inform each other of any changes in the capacity of an individual or a legal entity to have access to or to handle Classified Information.

ARTICLE 6
RELEASE OF CLASSIFIED INFORMATION

1. Within the scope of its legislation, the receiving Party shall take all steps reasonably available to keep Classified Information transmitted to it by the originating Party free from disclosure under any legislative provision or other rule of law, unless the originating Party consents to such disclosure. If there is any request to declassify or disclose any Classified Information transmitted under the provisions of this Agreement, the receiving Party shall immediately notify the originating Party and both Parties shall consult each other before any decision is taken.

2. Subject to the provisions of paragraph (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 the purposes and within any limitations stated by or on behalf of the originating Party.

3. Subject to the provisions of paragraph (1), the receiving Party shall not release, disclose or permit the release or disclosure of the Classified Information transmitted under the provisions of this Agreement to any Third Party without the prior written consent of the originating Party.

ARTICLE 7
NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities responsible, at national level, for the implementation and the control of the measures undertaken in the implementation of this Agreement are:

In Romania	**In the Kingdom of Spain**
Guvernul României Oficiul Registrului Naţional al Informaţiilor Secrete de Stat Bucureşti Str. Mureş nr.4 sector 1 ROMANIA	Secretario de Estado Director del Centro Nacional de Inteligencia Oficina Nacional de Seguridad Avda Padre Huidobro s/n Madrid 28023 SPAIN

2. In order to keep the same security standards each National Security Authority shall provide, upon request, to the other National Security Authority information about its security organization and procedures. To this purpose, the National Security Authorities shall also agree on mutual visits in both countries by certified officials.

ARTICLE 8
VISITS

1. Visits entailing access to Classified Information by nationals from one Party to the other Party are subject to prior written authorisation given by the National Security Authority/Designated Security Authority of the host Party.

2. Visits entailing access to Classified Information by a national of a Third Party shall only be authorised upon the written consent of the originating Party.

3. The National Security Authority/Designated Security Authority of the sending Party shall notify the National Security Authority/Designated Security Authority of the host Party of expected visitors in accordance with the procedures defined in paragraphs below.

4. Visits entailing access to Classified Information shall be allowed by one Party to visitors from the other Party only if they have been:

a. granted appropriate Personnel Security Clearance by the National Security Authority/Designated Security Authority of the sending Party; and

b. authorised to receive or to have access to Classified Information in accordance with the legislation of their Party.

5. The National Security Authority/Designated Security Authority of the sending Party shall notify the National Security Authority / Designated Security Authority of the host Party of the planned visit through a request for visit, which has to be received at least twenty (20) working days before the visit or visits take place.

6. In urgent cases, the request for visit could be transmitted at least five (5) working days before.

7. The request for visit shall include:

a. Visitor's first and last name, place and date of birth, nationality, passport or ID card number;

b. Name of the establishment, company or organisation he/she represents or to which he/she belongs;

c. Name and address of the establishment, company or organisation to be visited;

d. Certification of the visitor's Personnel Security Clearance;

e. Object and purpose of the visit or visits;

f. Expected date and duration of the requested visit or visits. In case of recurring visits the total period covered by the visits should be stated;

g. Name and phone number of the point of contact at the establishment/facility to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;

h. The date, signature and stamping of the official seal of the National Security Authority or of the appropriate Designated Security Authority.

8. The validity of visit authorisation shall not exceed twelve months.

9. The National Security Authority/Designated Security Authority of the host Party shall inform the security officers of the establishment, facility or organisation to be visited of data of those persons approved for a visit.

10. In cases involving a specific project or a particular contract it may, subject to the approval of both Parties, be possible to establish recurring visitors' lists. These lists shall be valid for an initial period not exceeding twelve (12) months and may be extended for an equal period of time, subject to the prior approval of both Parties' National Security Authority/Designated Security Authority. Once a list has been approved, visit arrangements may be made directly between the establishments or companies involved in respect of listed individuals.

11. All visitors shall comply with the national legislation on the protection of Classified Information of the host Party.

12. Each Party shall guarantee the protection of personal data of the visitors according to the respective national legislation.

Representatives of either National Security Authority/Designated Security Authorities may visit each other in order to:

a) analyse the procedures for the protection of Classified Information;

b) analyse the efficiency of the measures adopted by Contractors for the implementation of this Agreement.

In this case, the date of visit shall be agree upon by the Parties, giving notice of this fact thirty (30) days in advance.

14. The Parties shall inform each other in writing of the authorities to be responsible for the procedure, control and supervision of the requests for visit.

ARTICLE 9
INDUSTRIAL SECURITY

1. In the event that either Party intends to award a Classified Contract to be performed within the territory of the other Party, the Party of the country in which the performance is taking place, will assume responsibility for the protection of Classified Information related to the contract in accordance with its legislation.

2. Prior to releasing to Contractors/Subcontractors or to prospective Contractors/Subcontractors any Classified Information received from the other Party, the receiving Party through the National Security Authority/Designated Security Authority, shall:

a. grant appropriate Facility Security Clearance/Industrial Security Authorisation certificates to the Contractors/Subcontractors or to prospective Contractors/Subcontractors, on condition they have met the requirements for their issue;

b. grant appropriate Personnel Security Clearance certificates to all personnel whose duties require access to Classified Information on condition they have met the requirements for their issue.

3. The Parties shall ensure that every Classified Contract includes an appropriate Security Aspects Letter containing:

a. Security Classification Guide;

b. Procedure for the communication of changes in the Security Classification of Classified Information;

c. Communication channels and means for electromagnetic transmission;

d. Transportation procedure;

e. Official inspections;

f. Competent authorities responsible for the co-ordination of the security envisaged in the Classified Contract;

g. An obligation to notify any actual or suspected Compromise of the Classified Information.

4. The procedures related to Classified Contracts shall be developed and agreed between the National Security Authorities/Designated Security Authorities of the Parties.

5. The Parties shall ensure protection of copyrights, industrial property rights – patents included – and any other rights connected with the Classified Information exchanged between them, according to their legislations.

6. Each Party's National Security Authority/Designated Security Authorities shall notify the security status of an establishment or Contractor on its territory when requested by the other Party's National Security

Authority/Designated Security Authorities. Each Party's National Security Authority/Designated Security Authorities shall also notify the security clearance status of one of its nationals when so requested. These notifications shall be considered as Facility Security Clearance and Personnel Security Clearance assurance respectively.

7. When a Contractor/individual does not have a Facility/Personnel Security Clearance, or the clearance level is lower than required, any National Security Authority/Designated Security Authority shall request the other National Security Authority/Designated Security Authority to start the process for the granting or upgrading, according to its national security laws and regulations. Following successful enquires a Facility/Personnel Security Clearance Information Sheet shall be provided. If not, the requesting National Security Authority/Designated Security Authority shall be informed.

8. If either National Security Authority/Designated Security Authority learns about any incident regarding the protection of Classified Information then immediately inform the other National Security Authority/Designated Security Authority about these facts, will analyse them and will notify the results of this review to the other National Security Authority/Designated Security Authority.

9. If required by the other Party each National Security Authority/Designated Security Authority will co-operate in reviews of the incidents regarding the protection of Classified Information.

ARTICLE 10
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information shall be transmitted by diplomatic or military channels or other means agreed upon by the National Security Authorities. The receiving National Security Authority/Designed Security Authority shall confirm the receipt of Classified Information.

2. If a large consignment containing Classified Information is to be transmitted, the National Security Authorities shall mutually agree on and approve the means of transportation, the route and security measures for each such case.

3. Other approved means of transmission or exchange of Classified Information may be used, if agreed on, by the National Security Authorities.

4. The exchange of Classified Information through information and communications systems, shall take place in accordance with the security procedures established through mutual arrangements by the National Security Authorities.

ARTICLE 11
BREACHES OF SECURITY AND COMPROMISE OF CLASSIFIED INFORMATION

1. In case of a Breach of Security that results in a Compromise or possible Compromise of Classified Information, the National Security Authority of the Party where the security breach occurred shall promptly inform the National Security Authority of the other Party, ensure proper security investigation of such event and take the necessary measures to limit the consequences, in accordance with its national legislation. If required, the National Security Authorities shall cooperate in the investigation.

2. In case the compromise does not occur on the territory of either Party, the National Security Authority of the dispatching Party shall take action as of paragraph 1.

3. After completion of the investigation, the National Security Authority of the Party where the Compromise or possible Compromise of Classified Information occurred shall immediately inform in writing, to the National Security Authority of the other Party on the findings and conclusions of the investigation.

ARTICLE 12
SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or implementation of this Agreement shall be settled by consultation between the National Security Authorities of the Parties or, should an acceptable settlement be impossible to reach, between the designated representatives of the Parties.

ARTICLE 13
COSTS

Each Party shall bear the eventual costs related to the implementation of this Agreement in accordance with its legislation. Under no circumstances such costs incurred by one Party shall be imposed to the other Party.

ARTICLE 14
MUTUAL ASSISTANCE

1. Each Party shall assist to the personnel from the other Party in the implementation and interpretation of the provisions of this Agreement.

2. Should the need arise the National Security Authorities of the Parties will consult each other on specific technical aspects concerning the implementation of this Agreement and can mutually approve the conclusion of supplementary security protocols of specific nature to this Agreement on a case by case basis.

ARTICLE 15
FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time and it is subject to approval in accordance with the legislation of each Party.

2. This Agreement shall enter into force on the first day of the second month following the receipt of the last of the notifications between the Parties that the necessary requirements set by national legislation for this Agreement to enter into force have been met.

3. Each Party has the right to denounce this Agreement at any time. In such case the validity of the Agreement will terminate after 6 (six) months following the day on which the notification of termination notice was served to the other Party.

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

5. This Agreement may be amended on the basis of the mutual consent of the Parties. Such amendments shall enter into force in accordance with the provisions of paragraph 2.

6. Each Party shall promptly notify the other Party of any changes to its legislation that would affect the protection of Classified Information under this Agreement. In such case, the Parties shall consult to consider possible changes to this Agreement. In the meantime, Classified Information shall continue to be protected as described herein, unless requested otherwise in writing by the originating Party.

7. When this Agreement enters into force, the Agreement between Romania and the Kingdom of Spain on the Protection of Defence Classified Information, signed at Bucharest, on the 3rd of March, 2004 shall be terminated.

Signed in Madrid on 14th of May 2010 in two original copies, each one in the Romanian and Spanish languages, both texts having equal validity.

FOR
ROMANIA

MARIUS PETRESCU
Secretary of State
Director General
of the National Registry Office for Classified Information

FOR
THE KINGDOM OF SPAIN