No. 56455*

Spain
and
South Africa

Security Agreement between the Kingdom of Spain and the Government of the Republic of South Africa concerning the protection of classified information exchanged between them within the framework of defence cooperation (with annex). Madrid, 4 October 2017

Entry into force: *26 November 2020 by notification, in accordance with article 15(1)*

Authentic texts: *English and Spanish*

Registration with the Secretariat of the United Nations: *Spain, 29 January 2021*

*No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.

Espagne
et
Afrique du Sud

Accord de sécurité entre le Royaume d'Espagne et le Gouvernement de la République sud-africaine concernant la protection des informations classifiées échangées entre eux dans le cadre de la coopération en matière de défense (avec annexe). Madrid, 4 octobre 2017

Entrée en vigueur : *26 novembre 2020 par notification, conformément au paragraphe 1 de l'article 15*

Textes authentiques : *anglais et espagnol*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Espagne, 29 janvier 2021*

*Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.

[ENGLISH TEXT – TEXTE ANGLAIS]

SECURITY AGREEMENT

BETWEEN

THE KINGDOM OF SPAIN

AND

THE GOVERNMENT OF THE REPUBLIC OF SOUTH AFRICA

CONCERNING

THE PROTECTION OF CLASSIFIED INFORMATION EXCHANGED BETWEEN THEM WITHIN THE FRAMEWORK OF DEFENCE COOPERATION

The Kingdom of Spain and the Government of the Republic of South Africa, hereinafter jointly referred to as the "Parties" and separately as a "Party");

WISHING to ensure adequate protection of classified information exchanged between them within the framework of defence cooperation;

HEREBY AGREE as follows:

ARTICLE 1
DEFINITIONS

In this Security Agreement (hereinafter referred to as "this Agreement"), unless the context indicates otherwise:

"Classified Information" means any item in any form, including written, oral or visual, and any material to which the Originating Party has, in accordance with its national security laws and regulations, assigned a security classification;

"classified contract" means any contract or sub-contract between the Parties or with or between contractors or potential contractors, which contains Classified Information, or the performance of which requires, access to Classified Information of either Party;

"contractor" means an individual or a legal entity possessing the legal capacity to conclude contracts;

"document" means any letter, note, minute, report, memorandum, signal, message, sketch, photograph, film, map, chart, plan, notebook, stencil, carbon, typewritten ribbon, or any form of recorded information (eg tape-recording, magnetic recording, punched card, or tape);

"Facility Security Clearance" means the determination by the National Security Authority or other competent 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 laws and regulations;

"material" means any document and any part of machinery, equipment or weapon, either manufactured or in the process of being manufactured;

"National Security Authority" means the authority designated by a Party responsible for the formulation of the applicable security policy and supervision of this Agreement;

"Originating Party" means that Party which generates and provides Classified Information and accords it a national security classification, and which transmits Classified Information to the other Party;

"Personnel Security Clearance" means the determination by the National Security Authority that an individual has been security cleared to access and handle Classified Information up to and including a specified security classification level in accordance with the national laws and regulations.

"Project Security Instructions" means a compilation of security regulations and procedures which are applied to a specific project or programme in order to standardise security procedures;

"Receiving Party" means that Party which receives the Classified Information from the Originating Party;

"sub-contractor" means a contractor to whom a prime contractor lets a sub-contract.

"third party" means any State, including legal entities and individuals under its jurisdiction, or International Organisation, which is not a party to this Agreement.

ARTICLE 2
NATIONAL SECURITY AUTHORITIES

1. The National Security Authority responsible for this Agreement shall be:

    a) in the case of the Kingdom of Spain, the Secretary of State Director of the National Intelligence Centre, National Office of Security, on behalf of the Kingdom of Spain.

    b) in the case of the Republic of South Africa, the Chief of Defence Intelligence on behalf of the Government of the Republic of South Africa;

2. The official channel of communication between the Parties for all matters relating to this Agreement shall be through the National Security Authorities.

ARTICLE 3
OBLIGATIONS

1. The Parties shall, in accordance with the domestic law in force in their respective countries, take all necessary measures to protect Classified Information exchanged or generated under this Agreement.

2. The Parties shall ensure that Classified Information received under this Agreement shall be awarded at least the same protection as that awarded to national information of the same level of classification. The standards of security contained in Annex A, which forms an integral part of this Agreement, shall be regarded as a minimum level of protection.

3. In order to achieve and maintain comparable standards of security, the Parties shall on request, provide each other with information about their national security standards, practices and procedures for the safeguarding of Classified Information including those standards, practices and procedures which relate to its industrial operations. Each Party shall inform the other Party in writing of any changes to those security standards, practices and procedures, which have an effect on the manner Classified Information is protected.

ARTICLE 4
ACCESS TO CLASSIFIED INFORMATION

1. The Parties shall use Classified Information exclusively for the purpose it was provided for.

2. In particular, access to Classified Information shall be limited to those persons whose duties require such access in accordance with the need-to-know principle, who are security cleared at the appropriate level and who have the required knowledge of security procedures. No person shall be entitled solely by virtue of rank or appointment to have access to Classified Information.

3. Classified Information shall not be disclosed by the Receiving Party to a third party without the prior written consent of the National Security Authority of the Originating Party.

ARTICLE 5
LEVELS OF SECURITY CLASSIFICATION

1. For the purpose of this Agreement, the Parties adopt the following equivalents of Security Classifications:

Spanish Classification	South African Classification
RESERVADO	SECRET
CONFIDENCIAL	CONFIDENTIAL
DIFUSIÓN LIMITADA	RESTRICTED

2. Classified Information translated, and / or copied and exchanged under this Agreement, shall be awarded a security classification in accordance with the national security laws and regulations of the Parties.

3. Classified Information generated through cooperation between the Parties shall be awarded a security classification by mutual consent of the National Security Authorities of the Parties.

4. Up- or down-grading of a security classification and declassification of Classified Information shall be the prerogative of the Originating Party.

5. The Parties shall give eight (8) weeks written notice in advance of the intent to up- or downgrade a security classification or to declassify Classified Information.

6. With regard to Classified Information originating from third parties, the procedures with respect to the protection and release thereof shall be in conformity with the relevant domestic law governing the protection of such Classified Information.

ARTICLE 6
CHANNELS FOR TRANSFER OF CLASSIFIED INFORMATION

1. Classified Information shall be transferred through the diplomatic channel. The Receiving Party shall acknowledge receipt and, if necessary, take care of further transfer.

2. In case of urgency, the use of channels other than the diplomatic channel, may be agreed upon by the National Security Authorities of both Parties.

3. The Parties may transmit Classified Information by secure electronic means in accordance with security procedures mutually determined by the Parties' National Security Authorities.

ARTICLE 7
CLASSIFIED CONTRACTS

1. A Party, wishing to place a classified contract with a contractor of the other Party, or wishing to authorise one of its own contractors to place a classified contract in the territory of the other Party within a classified project shall obtain, through its National Security Authority, prior written assurance from the National Security Authority of the other Party that the proposed contractor holds a Facility Security Clearance at an appropriate level.

2. The Contractor commits itself to:

   a) ensure that its premises have adequate facilities for the appropriate protection of Classified Information;

   b) obtain and maintain a proper level of security clearance for its premises;

   c) obtain and maintain a proper level of Personnel Security Clearance for persons who perform functions which require access to Classified Information;

   d) ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information, according to the domestic legislation in force; and

   e) perform periodical security inspections of its premises.

3. Any sub-contractor must comply with the same security obligations as contractors.

4. As soon as pre-contractual negotiations begin between a body located in the territory of one of the Parties and another body located in the other Party's territory, aiming at the signing of classified contractual instruments, the appropriate National Security Authority shall inform the other Party of the level of the security classification assigned to the Classified Information related to those pre-contractual negotiations.

5. Every classified contract concluded between entities of the Parties under the provisions of this Agreement, shall include appropriate security provisions identifying the following aspects:

   a) A classified guide and list of Classified Information;

   b) procedures for the communication of changes in the classification of information;

   c) communication channels and means for electromagnetic transmissions;

   d) procedures for the transportation for classified material;

   e) competent authorities responsible for the coordination of the safeguarding of Classified Information related to the contract; and

   f) an obligation to notify any actual or suspected loss, leak or compromise of Classified Information.

6. A copy of the security provisions of any classified contract shall be forwarded to the National Security Authority of the Party where the work is to be performed, to allow adequate security supervision and control.

7. Security experts from the National Security Authorities shall make periodical visits to each other when it is mutually convenient, to discuss the procedures and facilities for the protection of Classified Information.

8. When appropriate, Project Security Instructions shall be exchanged between the Parties.

ARTICLE 8
VISIT APPLICATIONS

1. Authorised representatives of each of the Parties or personnel of the industries involved shall have access to Classified Information and to the establishments where classified activities take place subject to the prior authorisation of the Party to be visited.

2. Applications for visits shall be made with the National Security Authority of the Party to be visited at least two (2) weeks in advance.

3. Applications shall include:

a) particulars of the representative(s) [surname and first name(s), place and date of birth, nationality and passport number];

b) name of the agency, establishment, facility or organisation they represent or to which they belong;

c) certification of the visitor's Personnel Security Clearance, its validity and any limitations;

d) anticipated highest level of Classified Information to be involved;

e) purpose of the visit;

f) time and duration of the visit and whether the request is for an intermittent recurring visit approval. In case of recurring visits the total period covered by the visits should be stated; and

g) the establishment(s) and the persons to be visited including a telephone number for contacting.

4. The validity of a visit authorisation including those for intermittent recurring visits to a specified establishment shall not exceed twelve (12) months. When it is expected that a particular visit shall not be completed within the approved period, or that an extension of the period for intermittent recurring visits is required, the visiting Party shall submit a new request for a visit approval at least twenty (20) working days prior to the expiry of the current visit approval.

5. The National Security Authority of the host Party shall inform the security officials of the agency, establishment, facility or organisation to be visited, of the details of those individuals whose visit requests have been approved. Once approval has been given, visit arrangements for individuals who have been given approval for an intermittent recurring visit may be made directly with the agency, establishment, facility or organisation concerned.

ARTICLE 9
POINTS OF CONTACT

1. Point of contact in the Kingdom of Spain:
Oficina Nacional de Seguridad
Calle Argentona 20
28023 MADRID
España

2. Point of contact in the Republic of South Africa:

a) For military related matters:
Chief of Defence Intelligence
Private Bag X367
PRETORIA
0001
Republic of South Africa

b) For military-industrial matters:
Senior Manager: Security
Armscor Security Division
Private Bag X337
PRETORIA
0001
Republic of South Africa

ARTICLE 10
SECURITY BREACHES

Security breaches which may possibly lead to or which have already led to a compromise shall be dealt with by the respective National Security Authorities in accordance with the domestic law in force in the countries of the Parties. The Parties shall inform each other immediately of the circumstances, the measures taken and the outcome thereof.

ARTICLE 11
COSTS

In the case of any cost, each Party shall bear their own costs incurred in implementing this Agreement.

ARTICLE 12
INTELLECTUAL PROPERTY RIGHTS

Nothing in this Agreement diminishes or limits any existing or acquired intellectual property rights, including patents or copyrights, associated with Classified Information to which either Party or any third party may be entitled.

ARTICLE 13
IMPLEMENTING ARRANGEMENTS

Implementing Arrangements may be concluded within the framework of this Agreement where specific collaborative programmes are identified.

ARTICLE 14
AMENDMENT

This Agreement may be amended in writing by mutual consent of both Parties through the diplomatic channel.

ARTICLE 15
ENTRY INTO FORCE, DURATION AND TERMINATION

1. This Agreement shall enter into force when the Parties have notified each other in writing of their compliance with their constitutional requirements for this Agreement to enter into force. The date of entry into force shall be the date of receipt of the last notification.

2. This Agreement shall remain in force for an indefinite period unless terminated by either Party giving six (6) months' written notice in advance through the diplomatic channel of its intention to terminate this Agreement.

3. In case of termination, the Parties shall, as far as possible, return all Classified Information exchanged or generated through the cooperation between the Parties under this Agreement. If the return of Classified Information is not possible, the Parties shall continue to protect such Classified Information in accordance with the provisions of this Agreement.

ARTICLE 16
SETTLEMENT OF DISPUTES

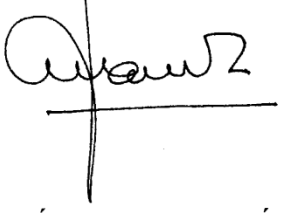
Any dispute between the Parties arising out of the application, interpretation or implementation of the provisions of this Agreement, shall be settled amicably through consultation or negotiations between them.

IN WITNESS WHEREOF the undersigned, being duly authorised thereto by their respective Governments, have signed and sealed this Agreement in two

originals in the Spanish and English languages, all texts being equally authentic.

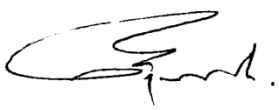
DONE in Madrid on this 4th day of October in this year 2017.

FOR THE GOVERNMENT OF THE KINGDOM OF SPAIN



FÉLIX SANZ ROLDÁN
Secretary of State, Director of the National Intelligence Centre

FOR THE GOVERNMENT OF THE REPUBLIC OF SOUTH AFRICA



JEREMIAH MDUDUZI NYEMBE
Lieutenant General Chief Defence Intelligence South Africa

ANNEX A

MINIMUM STANDARDS OF SECURITY

1. Introduction

a) The principal objectives of protective security are to safeguard:

i) Classified Information from espionage, compromise, unauthorised disclosure, loss or theft; and

ii) vital installations from sabotage.

b) The Parties shall appoint a security officer in each facility involved, e.g. factory, office, establishment where Classified Information is being handled and stored.

c) The security officer shall be responsible for the adequate security protection of Classified Information.

d) A security plan for each facility covering all security provisions and measures (personnel, documents, materials, organisation, physical and, if applicable, IT) shall be made. Security plans and any change thereof must be approved by the National Security Authority of the Party concerned.

e) The respective National Security Authority shall carry out security inspections at the facilities mentioned in paragraph (b) above on a regular basis.

2) Definition of Security Classification

a) For the Kingdom of Spain

i) RESERVADO. RESERVADO is the security classification allocated to information whose unauthorised disclosure or wrongful use would endanger or cause serious damage to national interests.

ii) CONFIDENCIAL. CONFIDENCIAL is the security classification allocated to information whose unauthorised disclosure or wrongful use would endanger or cause damage to national interests.

iii) DIFUSIÓN LIMITADA. DIFUSIÓN LIMITADA is the security classification allocated to information whose unauthorised disclosure or wrongful use would be contrary to national interests.

b) For the Republic of South Africa

i) Secret. Secret is the classification allocated to information that may be used by hostile / opposing / malicious elements to disrupt the objectives and functions of an institution and / or state.

ii) Confidential. Confidential is the security classification allocated to information that may be used by hostile / opposing / malicious elements to harm the objectives of an individual and / or institution.

iii) Restricted. Restricted is the security classification allocated to all information that may be used by hostile / opposing / malicious elements to hamper the activities of or inconvenience an institution or an individual.

3) Documents

a) Mail containing Classified Information shall be opened and handled by authorised persons only.

b) Before handling, each classified document shall be registered.

c) Registration of Classified Information shall be on separate lists according to its classification. Registration will enable the National Security Authority to trace Classified Information at all times.

d) In case of translation or copying, the security classification assigned to the new document shall be the same as assigned to the original document.

e) Classifications or special markings shall not be removed and / or extracts or paraphrases of the information shall not be made without indicating the classification or the special marking given to the original document.

4) Transfer of Classified Information

a) International transfer of Classified Information shall be by diplomatic bag, military courier service or, exceptionally, by private courier service if so agreed between the Parties.

b) In case of international transfer, the receipt of Classified Information shall be acknowledged.

c) National transfer of Classified Information shall be by courier, authorised messenger service or, exceptionally, by postal service as registered mail.

d) Couriers and messengers employed to carry Classified Information shall be security cleared by the appropriate National Security Authority. Couriers and messengers shall be instructed on their duties for the protection of the information entrusted to them.

5) Packaging

a) For the packaging of Classified Information, the following rules apply:

i) Classified Information shall be transferred under double opaque and strong cover. The inner cover shall be sealed, stamped with the appropriate classification and bear the full designation and address of the addressee. If necessary, the inner cover may be marked "TO BE OPENED ONLY BY: [name of person who has been authorised to open the (inner) cover]".

ii) The packaging of the inner cover has to be in such a way that opening is not possible without breaking the seal or damaging the cover.

iii) The inner cover shall be enclosed in a secure outer cover.

iv) The outer cover shall bear a designation (but not a name), the address and a package number for transfer purposes and shall not indicate the classification of the contents or the fact that it contains Classified Information.

v) If information is transferred under double cover by courier, the outer cover shall be clearly marked: "BY COURIER ONLY". A locked pouch or box or a sealed diplomatic bag may be considered as the outer cover.

6) Storage of Classified Information

a) Measures shall be taken to prevent unauthorised persons from gaining access to Classified Information.

b) Classified Information shall be handled and stored in a security area. Such an area requires:

i) a clearly defined and protected perimeter through which all entry and exit is controlled;

ii) an access control system which admits only those appropriately cleared and specially authorised to enter the area; and

iii) escort provisions or similar means of control of visitors.

c) Classified Information shall be stored in a steel locker approved by the National Security Authority of the Party concerned.

d) The security classification allocated to a volume of information shall be that of the portion containing the highest classification.

7) Keys and Combinations

a) Keys of safes, lockers and / or containers storing Classified Information shall be kept within the security area. Spare keys and a written record of each combination setting shall be held by the security officer in an opaque, sealed and signed envelope and be given security protection no less stringent than the Classified Information to which they give access. Working and spare keys shall be kept in separate containers.

b) Knowledge of combination settings shall be restricted to the smallest possible number of persons. Settings shall be changed:

i) at intervals of not more than six (6) months;

ii) whenever a safe, a steel locker and / or container is installed;

iii) whenever a change of personnel acquainted with the combination, occurs; and

iv) whenever a compromise is suspected or has actually occurred.

8) Physical Security

a) Outside normal working hours protection of areas containing stored Classified Information shall be carried out by guards and / or by means of electronic means such as closed-circuit television and alarm systems.

b) Patrols shall take place at intervals to be determined by the National Security Authority in light of any local threat.

c) If for maintenance, repair or other purposes, unauthorised persons have to enter areas containing Classified Information, measures shall be taken to prevent them from having access to such information. Their activities shall be carried out under permanent supervision.

9) Visitors. Visitors shall never be left unguarded in areas containing Classified Information.

10) Destruction

a) In order to avoid unnecessary accumulation, obsoleteness or redundancy, Classified Information shall be destroyed as soon as practical by burning, reducing to pulp, shredding or pulverising into an unrecognisable form and beyond reconstruction.

b) The recording of the destruction of Classified Information shall be in accordance with the procedures established by the National Security Authority of each Party.

11) Physical Dimensions of Material containing Classified Information. Whenever the abovementioned provisions and / or measures regarding transfer, packaging, storing and destruction are impractical because of the physical dimensions of material containing Classified Information, the Parties shall agree on appropriate measures.

12) Compromise of Classified Information

a) Classified Information is compromised when knowledge of it in whole or in part, has been disclosed to unauthorised persons or when it has been subject to risk of such disclosure.

b) In all cases of compromise, the final report or a progress report of the investigation shall be submitted to the National Security Authority of the other Party within 90 days.

[SPANISH TEXT – TEXTE ESPAGNOL]

ACUERDO DE SEGURIDAD

ENTRE

EL REINO DE ESPAÑA

Y

EL GOBIERNO DE LA REPÚBLICA DE SUDÁFRICA

SOBRE

PROTECCIÓN DE INFORMACIÓN CLASIFICADA INTERCAMBIADA EN EL MARCO DE LA COOPERACIÓN EN MATERIA DE DEFENSA

El Reino de España y el Gobierno de la República de Sudáfrica (en lo sucesivo denominados conjuntamente "las Partes" y, por separado, una "Parte"),

Deseosos de asegurar la protección de la Información Clasificada intercambiada dentro del marco de la cooperación en materia de defensa,

Han convenido en lo siguiente:

ARTÍCULO 1
DEFINICIONES

A los efectos del presente Acuerdo de Seguridad (en lo sucesivo denominado "el presente Acuerdo") y, a menos que del contexto se infiera otra cosa:

Por "**Información Clasificada**" se entenderá todo artículo, en cualquier formato, ya sea escrito, oral o visual y todo material al cual la Parte de origen, de conformidad con sus leyes y reglamentos nacionales en materia de seguridad, haya otorgado una clasificación de seguridad;

Por "**Contrato Clasificado**" se entenderá todo contrato o subcontrato entre las Partes, o entre ellas y Contratistas o posibles Contratistas, o entre estos últimos, que contenga Información Clasificada o para cuya realización se exija acceso a Información Clasificada de cualquiera de las Partes;

Por "**Contratista**" se entenderá toda persona física o jurídica que tenga capacidad jurídica para celebrar contratos;

Por **"Documento"** se entenderá toda carta, nota, acta, informe, memorando, señal, mensaje, esquema, fotografía, película, mapa, gráfico, plano, libreta, plantilla, papel carbón, cinta mecanografiada, o cualquier forma de información registrada (por ejemplo, grabaciones en cintas, grabaciones magnéticas, tarjetas perforadas o cintas);

Por "**Habilitación de Seguridad para Establecimiento**" se entenderá la acreditación por la Autoridad Nacional de Seguridad u otra autoridad competente de que un establecimiento tiene, desde el punto de vista de la seguridad, la capacidad física y organizativa para utilizar y custodiar Información Clasificada, de conformidad con las leyes y reglamentos nacionales;

Por **"Material"** se entenderá todo documento y cualquier parte de maquinaria, equipo o armas ya fabricados o en proceso de fabricación;

Por **"Autoridad Nacional de Seguridad"** se entenderá la autoridad que cada Parte designe como responsable de la aplicación y supervisión del presente Acuerdo;

Por "**Parte de Origen"** se entenderá la Parte que genera y proporciona la Información Clasificada y le otorga una clasificación nacional de seguridad y que transmite la Información Clasificada a la otra Parte;

Por **"Habilitación Personal de Seguridad"** se entenderá la acreditación por la Autoridad Nacional de Seguridad de que una persona ha obtenido la habilitación de seguridad para el acceso a Información Clasificada y la gestión de la misma, hasta un Grado de clasificación de seguridad específico, éste incluido, de conformidad con sus leyes y reglamentos nacionales;

Por **"Instrucciones de Seguridad del Proyecto"** se entenderá un conjunto de normas y procedimientos relativos a la seguridad que se apliquen a un proyecto o programa específico con el fin de normalizar los procedimientos de seguridad;

Por **"Parte Receptora"** se entenderá la Parte que recibe la Información Clasificada de la Parte de Origen;

Por **"Subcontratista"** se entenderá todo contratista a quien un contratista inicial conceda un subcontrato.

Por **"Tercero"** se entenderá todo Estado, incluidas personas físicas y jurídicas bajo su jurisdicción, u organización internacional, que no sea Parte en el presente Acuerdo.

ARTÍCULO 2
AUTORIDADES NACIONALES DE SEGURIDAD

1. Las Autoridades de Seguridad competentes responsables de la aplicación del presente Acuerdo son las siguientes:

    a) Por el Reino de España, el Secretario de Estado Director del Centro Nacional de Inteligencia, Oficina Nacional de Seguridad, España;

    b) Por el Gobierno de la República de Sudáfrica, el Director de la Agencia de Inteligencia de Defensa.

2. El conducto oficial de comunicación entre las Partes para todas las cuestiones relativas al presente Acuerdo será a través de las Autoridades Nacionales de Seguridad.

ARTÍCULO 3
OBLIGACIONES

1. Las Partes, de conformidad con la legislación interna en vigor en sus respectivos países, tomarán todas las medidas necesarias para proteger la Información Clasificada intercambiada o generada en virtud del presente Acuerdo.

2. Las Partes velarán por que se otorgue a la Información Clasificada recibida en virtud del presente Acuerdo, al menos, la misma protección que se otorgue a la información nacional de nivel equivalente de clasificación. Las Normas de Seguridad contenidas en el Anexo A, que constituye parte integrante del presente Acuerdo, se considerarán el nivel mínimo de protección.

3. Con objeto de alcanzar y mantener estándares de seguridad similares, las Partes intercambiarán, previa solicitud, información sobre sus normas, prácticas y procedimientos de seguridad nacionales para la protección de la Información Clasificada, incluidas las normas, prácticas y procedimientos relativos a sus actividades industriales. Cada Parte informará a la otra Parte por escrito de cualquier cambio en dichas normas, prácticas y procedimientos de seguridad que puedan afectar a la forma en que se protege la Información Clasificada.

ARTÍCULO 4
ACCESO A LA INFORMACIÓN CLASIFICADA

1. Las Partes utilizarán la Información Clasificada exclusivamente para los fines para los que se haya proporcionado.

2. En particular, el acceso a la Información Clasificada se limitará a las personas cuyas funciones exijan dicho acceso con arreglo al principio de la necesidad de conocer, y que posean la pertinente Habilitación de Seguridad del nivel correspondiente y los conocimientos necesarios sobre los procedimientos de seguridad. Nadie tendrá derecho de acceso a Información Clasificada por el solo motivo de su rango o cargo.

3. La Parte Receptora no podrá divulgar la Información Clasificada a un Tercero sin el consentimiento previo por escrito de la Autoridad Nacional de Seguridad de la Parte de Origen.

ARTÍCULO 5
NIVELES DE CLASIFICACIÓN DE SEGURIDAD

1. A los efectos de presente Acuerdo, las Partes adoptan las siguientes equivalencias de sus Clasificaciones de Seguridad:

Clasificación española	Clasificación sudafricana
RESERVADO	SECRET
CONFIDENCIAL	CONFIDENTIAL
DIFUSIÓN LIMITADA	RESTRICTED

2. Se otorgará a la Información Clasificada traducida y/o copiada e intercambiada en virtud del presente Acuerdo una clasificación de seguridad de conformidad con las leyes y reglamentos de seguridad de las Partes.

3. A la Información Clasificada generada mediante la cooperación entre las Partes se le otorgará una clasificación de seguridad acordada por las Autoridades Nacionales de Seguridad de las Partes.

4. La modificación al alza o a la baja de una clasificación de seguridad, así como la desclasificación de Información Clasificada, será prerrogativa de la Parte de Origen.

5. Las Partes deberán notificarse con ocho (8) semanas de antelación su intención de aumentar o rebajar una clasificación de seguridad o de desclasificar Información Clasificada.

6. En relación con la Información Clasificada originada por Terceros, los procedimientos con respecto a la protección y cesión de la misma se ajustarán a la legislación nacional que regule la protección de dicha Información Clasificada.

ARTÍCULO 6
CANALES DE TRANSMISIÓN DE LA INFORMACIÓN CLASIFICADA

1. La Información Clasificada se transmitirá por conducto diplomático. La Parte Receptora deberá acusar recibo y, cuando proceda, se ocupará de la ulterior transmisión.

2. En casos de urgencia, las Autoridades Nacionales de Seguridad de ambas Partes podrán acordar el uso de conductos distintos del diplomático.

3. Las Partes podrán transmitir Información Clasificada por medios electrónicos seguros, de conformidad con los procedimientos de seguridad que las Autoridades Nacionales de Seguridad de las Partes establezcan de mutuo acuerdo.

ARTÍCULO 7
CONTRATOS CLASIFICADOS

1. La Parte que tenga la intención de adjudicar un Contrato Clasificado a un Contratista de la otra Parte o de autorizar a uno de sus propios Contratistas a concluir un Contrato Clasificado en el territorio de la otra Parte en el contexto de un proyecto clasificado deberá obtener previamente, a través de su Autoridad Nacional de Seguridad, una garantía por escrito de la Autoridad Nacional de Seguridad de la otra Parte de que el contratista propuesto tiene una Habilitación de Seguridad para Establecimiento del nivel apropiado.

2. El contratista se compromete a:

   a) garantizar que sus instalaciones reúnen las condiciones adecuadas para la correcta protección de la Información Clasificada;

   b) obtener y mantener un nivel adecuado de habilitación de seguridad para sus instalaciones;

   c) obtener y mantener un nivel adecuado de Habilitación Personal de Seguridad para las personas que desempeñen funciones que exijan acceso a Información Clasificada;

   d) garantizar que se informe a todas las personas con acceso a Información Clasificada sobre su responsabilidad en relación con la protección de la Información Clasificada, de conformidad con la legislación interna en vigor; y

   e) llevar a cabo periódicamente inspecciones de seguridad de sus instalaciones.

3. Todo Subcontratista deberá cumplir las mismas obligaciones que los Contratistas en materia de seguridad.

4. Tan pronto como se entablen las negociaciones precontractuales entre un organismo situado en el territorio de una de las Partes y otro organismo situado en el territorio de la otra Parte, que tengan por objeto la firma de instrumentos contractuales clasificados, la Autoridad Nacional de Seguridad correspondiente informará a la otra Parte del nivel de clasificación de seguridad otorgado a la Información Clasificada relacionada con dichas negociaciones precontractuales.

5. Todo Contrato Clasificado celebrado entre las Partes en virtud de las disposiciones del presente Acuerdo deberá incluir las disposiciones pertinentes en materia de seguridad que reflejen los siguientes aspectos:

   a) guía de clasificación y lista de Información Clasificada;

   b) procedimientos para comunicar cualquier cambio en la clasificación de la información;

   c) canales de comunicación y medios de transmisión electromagnética;

   d) procedimientos de transporte del material clasificado;

   e) autoridades competentes responsables de coordinar la protección de la Información Clasificada relativa al Contrato;

   f) obligación de notificar cualquier pérdida, filtración o compromiso, real o supuesta, de la Información Clasificada;

6. Se remitirá a la Autoridad Nacional de Seguridad de la Parte en la que vaya a desempeñarse el trabajo una copia de las disposiciones sobre seguridad de cualquier Contrato Clasificado, con objeto de permitir una supervisión y control de seguridad adecuados.

7. Expertos en seguridad de las Autoridades Nacionales de Seguridad realizarán, periódicamente, visitas recíprocas, cuando ambas lo estimen conveniente, con el fin de tratar los procedimientos e instalaciones para la protección de Información Clasificada.

8. Cuando proceda, las Partes intercambiarán Instrucciones de Seguridad del Proyecto.

ARTÍCULO 8
SOLICITUD DE VISITAS

1. Los representantes autorizados de cada una de las Partes o el personal de los sectores implicados tendrán acceso a Información Clasificada y a los establecimientos en que se desarrollen actividades clasificadas, cuando cuenten con la autorización previa de la Parte que recibe la visita.

2. Las solicitudes de visita se cursarán a través de la Autoridad Nacional de Seguridad de la Parte que recibe la visita con al menos dos (2) semanas de antelación.

3. Las solicitudes de visita deberán contener la siguiente información:

   a) los datos del representante o representantes [nombre y apellido o apellidos, fecha y lugar de nacimiento, nacionalidad y número de pasaporte];

   b) el nombre de la agencia, establecimiento, instalación u organización a la que represente o a la que pertenezca;

   c) la certificación de la Habilitación Personal de Seguridad del visitante, su vigencia y cualesquiera limitaciones relativas a la misma;

   d) el nivel más alto de clasificación previsto de la Información Clasificada a la que se vaya a tener acceso;

   e) la finalidad de la visita;

   f) la fecha y duración de la visita e indicación de si la solicitud se refiere a visitas recurrentes de carácter intermitente. En el caso de visitas recurrentes, deberá señalarse el periodo total abarcado por las mismas; y

   g) el establecimiento o establecimientos y las personas que vayan a visitarse, así como un teléfono de contacto.

4. La validez de las autorizaciones de visita a determinado establecimiento, incluidas las de visitas recurrentes de carácter intermitente, no podrá ser superior a doce (12) meses. Si se prevé que no va a poder completarse determinada visita en el periodo aprobado, o si se necesita ampliar el periodo para visitas recurrentes de carácter intermitente, la Parte visitante presentará una nueva solicitud de aprobación de visita al menos veinte (20) días hábiles antes de que expire la aprobación relativa a la visita en curso.

5. La Autoridad Nacional de Seguridad competente de la Parte anfitriona comunicará a los oficiales de seguridad de la agencia, establecimiento, instalación u organización que vaya a visitarse los datos de las personas cuya visita haya sido aprobada. Una vez concedida la aprobación, los preparativos de las visitas de las personas que hayan recibido una autorización para realizar visitas recurrentes de carácter intermitente se podrán realizar directamente con el establecimiento, instalación u organización de que se trate.

ARTÍCULO 9
PUNTOS DE CONTACTO

1. Punto de contacto en el Reino de España
   Oficina Nacional de Seguridad
   Calle Argentona 20
   28023MADRID
   España

2. Punto de contacto en la República de Sudáfrica:

   a) Para asuntos militares:
      Jefe de Inteligencia de Defensa
      Private Bag X367
      PRETORIA
      0001
      República de Sudáfrica

   b) Para asuntos relativos a la industria militar:
      Jefe de Seguridad
      Armscor Security Division
      Private Bag X337
      PRETORIA
      0001
      República de Sudáfrica

ARTÍCULO 10
INFRACCIONES DE SEGURIDAD

Las infracciones de seguridad que puedan derivar o hayan derivado en un compromiso de la Información Clasificada se tratarán por las respectivas Autoridades Nacionales de Seguridad de conformidad con la legislación

interna en vigor en los países de las Partes. Las Partes se informarán sin demora sobre los hechos, las medidas adoptadas y el resultado de las mismas.

ARTÍCULO 11
GASTOS

En caso de producirse, cada Parte se hará cargo de sus propios gastos contraídos en la aplicación del presente Acuerdo.

ARTÍCULO 12
DERECHOS DE PROPIEDAD INTELECTUAL

Nada de lo dispuesto en el presente Acuerdo supondrá una restricción o limitación de cualesquiera derechos de propiedad intelectual adquiridos o existentes que estén en relación con la Información Clasificada, incluidas las patentes y los derechos de autor, de los que sean titulares cualquiera de las Partes o Terceros.

ARTÍCULO 13
ACUERDOS DE APLICACIÓN

En el marco del presente Acuerdo podrán celebrarse acuerdos de aplicación, cuando se establezcan programas de colaboración específicos.

ARTÍCULO 14
MODIFICACIÓN

El presente Acuerdo podrá modificarse con el consentimiento mutuo por escrito de las Partes, transmitido por conducto diplomático

ARTÍCULO 15
ENTRADA EN VIGOR, VIGENCIA Y DENUNCIA

1. El presente Acuerdo entrará en vigor cuando las Partes se comuniquen por escrito el cumplimiento de todos sus requisitos constitucionales respectivos para su entrada en vigor. La fecha de entrada en vigor será la de la última notificación.

2. El presente Acuerdo permanecerá en vigor por un periodo indefinido, salvo que se termine cuando cualquiera de las Partes notifique por escrito con al menos seis (6) meses de antelación y por conducto diplomático su intención de darlo por terminado.

3. En caso de terminación, las Partes devolverán, tan pronto como sea posible, toda la Información Clasificada intercambiada o generada mediante la cooperación entre las Partes en virtud del presente Acuerdo. En caso de imposibilidad de devolver la Información Clasificada, las Partes continuarán protegiendo dicha Información Clasificada de conformidad con lo dispuesto en el presente Acuerdo.

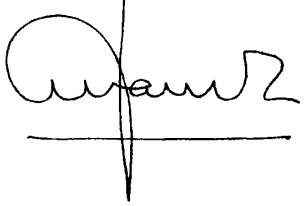
ARTÍCULO 16
RESOLUCIÓN DE CONTROVERSIAS

Toda controversia entre las Partes relativa a la aplicación, interpretación o puesta en práctica del presente Acuerdo se resolverá de forma amistosa mediante consultas o negociaciones entre ellas.

EN FE DE LO CUAL, los abajo firmantes, habiendo sido debidamente autorizados por sus respectivos Gobiernos, firman y sellan el presente Acuerdo en dos originales en español e inglés, siendo todos los textos igualmente auténticos.

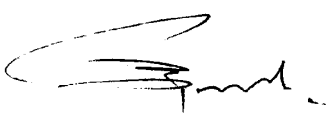
HECHO en Madrid el 4 de octubre del año 2017.

POR EL REINO DE ESPAÑA



FÉLIX SANZ ROLDÁN
Secretario de Estado Director
Del Centro Nacional de
Inteligencia

POR LA REPÚBLICA DE SUDÁFRICA



JEREMIAH MDUDUZI NYEMBE
Teniente Coronel Jefe del Servicio
de Inteligencia de la Defensa de
Sudáfrica

ANEXO A

NORMAS MÍNIMAS DE SEGURIDAD

1) Introducción

a) Los objetivos principales de la seguridad de protección son salvaguardar:

i) la Información Clasificada, frente a espionaje, compromiso, divulgación no autorizada, pérdida o robo;

ii) las instalaciones vitales, frente a sabotaje.

b) Las Partes designarán a un responsable de seguridad en cada instalación afectada, por ejemplo, una fábrica, oficina o establecimiento en que haya de tratarse y almacenarse la Información Clasificada.

c) El responsable de seguridad se encargará de la adecuada protección de la seguridad de la Información Clasificada.

d) Deberá elaborarse un plan de seguridad para cada instalación, que comprenda todas las disposiciones y medidas relativas a la seguridad (sobre personal, documentos, materiales, organización, de carácter físico y, si procede, TI). Los planes de seguridad y toda modificación de los mismos deberán ser aprobados por la Autoridad Nacional de Seguridad de la Parte de que se trate.

e) La Autoridad Nacional de Seguridad correspondiente llevará a cabo inspecciones periódicas de seguridad en las instalaciones mencionadas en el anterior apartado b).

2) Definición de la clasificación de seguridad

a) Para el Reino de España

i) RESERVADO. Se otorgará la clasificación de seguridad de RESERVADO a la información cuya divulgación no autorizada o su uso indebido pudiera poner en peligro o dañar seriamente los intereses nacionales.

ii) CONFIDENCIAL. Se otorgará la clasificación de seguridad de CONFIDENCIAL a la información cuya divulgación no autorizada o su uso indebido pudiera poner en peligro o dañar los intereses nacionales.

iii) DIFUSIÓN LIMITADA. Se otorgará la clasificación de seguridad de DIFUSIÓN LIMITADA a la información cuya divulgación no autorizada o su uso indebido pudiera revertir en contra de los intereses nacionales.

b) Para la República de Sudáfrica

i) SECRET. Se otorgará la clasificación de SECRET a la información que pueda ser utilizada por elementos hostiles/opuestos/maliciosos para perturbar los objetivos y funciones de una institución y/o del Estado.

ii) CONFIDENTIAL. Se otorgará la clasificación de seguridad de CONFIDENTIAL a la información que pueda ser utilizada por elementos hostiles/opuestos/maliciosos para perjudicar los objetivos de una persona y/o de una institución.

iii) RESTRICTED. Se otorgará la clasificación de seguridad de RESTRICTED a la información que pueda ser utilizada por elementos hostiles/opuestos/maliciosos para obstaculizar las actividades o causar perturbaciones a una institución o a una persona.

3) Documentos

a) El correo que contenga Información Clasificada deberá ser abierto y manipulado únicamente por personas autorizadas.

b) Todo documento clasificado deberá registrarse antes de su manipulación.

c) El registro de Información Clasificada se realizará en listas separadas en función de su clasificación. El registro permitirá a la Autoridad Nacional de Seguridad localizar la Información Clasificada en todo momento.

d) En caso de copia o traducción, la clasificación de seguridad que se asigne al nuevo documento será la misma asignada al documento original.

e) No deberán retirarse las clasificaciones o marcas especiales y no deberán elaborarse extractos ni citar la información sin indicación de la clasificación o de la marca especial que figure en el documento original.

4) Transmisión de Información Clasificada

a) La transmisión internacional de Información Clasificada se hará por valija diplomática, servicio de mensajería militar o, excepcionalmente, por servicio de mensajería privado si así lo acuerdan las Partes.

b) En caso de transmisión internacional deberá acusarse recibo de la recepción de la Información Clasificada.

c) La transmisión nacional de Información Clasificada se hará por mensajero, servicio de mensajería autorizado o, excepcionalmente, por servicio postal certificado.

d) Los mensajeros contratados para trasladar información deberán obtener una habilitación de seguridad por parte de la Autoridad Nacional de Seguridad. Se instruirá a los mensajeros en relación con su deber de proteger la información que se les confíe.

5) Embalaje

a) Para el embalaje de la Información Clasificada serán de aplicación las siguientes normas:

i) La Información Clasificada deberá transportarse con una cobertura doble opaca y resistente. La cobertura interior deberá ir sellada y marcada con la clasificación correspondiente y en ella deberá figurar el nombre, cargo y dirección completos del destinatario. En caso necesario, la cubierta interior podrá marcarse con el siguiente texto: "ÚNICAMENTE PODRÁ SER ABIERTO POR: [nombre de la persona que ha sido autorizada a abrir la cubierta (interior)]".

ii) El embalaje de la cubierta interior deberá realizarse de manera que no pueda abrirse sin romper el sello o estropear la cubierta.

iii) La cubierta interior irá dentro de una cubierta exterior de seguridad.

iv) La cubierta exterior deberá indicar un cargo (pero no un nombre), la dirección y un número de embalaje a efectos de transporte, y en ella no deberá figurar la clasificación del contenido ni el hecho de que contiene Información Clasificada.

v) Si la información se transporta con doble cubierta por mensajería, la cubierta exterior deberá llevar la marca: "SÓLO POR MENSAJERÍA". Una bolsa o caja con candado o cerrojo o una valija diplomática sellada podrán considerarse cubierta exterior.

6) Almacenamiento de la Información Clasificada

a) Deberán adoptarse medidas para evitar que personas no autorizadas accedan a la Información Clasificada.

b) La Información Clasificada se manipulará y almacenará en una zona de seguridad. Dicha zona deberá disponer de:

i) un perímetro claramente definido y protegido con control de entrada y salida;

ii) un sistema de control de acceso por el que sólo se admita a las personas debidamente habilitadas y especialmente autorizadas para acceder a la zona; y

iii) servicio de escolta o medios similares de control de visitantes.

c) La Información Clasificada se almacenará en una caja de seguridad de acero aprobada por la Autoridad Nacional de Seguridad de la Parte de que se trate.

d) La clasificación de seguridad que se atribuya a un conjunto de información será la de la parte con la clasificación más alta.

7) Claves y combinaciones

a) Las claves de las cajas de seguridad, taquillas o contenedores en que se almacene Información Clasificada deberán mantenerse dentro de la zona de seguridad. Las llaves de repuesto y el registro escrito de cada combinación serán custodiados por el responsable de seguridad en un sobre opaco, sellado y firmado y

se les concederá una protección de seguridad no menos estricta que la de la Información Clasificada a la que dan acceso. Las llaves de trabajo y las de repuesto se guardarán en contenedores separados.

b) El conocimiento de las combinaciones estará restringido al menor número posible de personas. Se cambiarán las combinaciones:

i) a intervalos no superiores a seis meses;

ii) siempre que se instale una caja de seguridad, taquilla de acero y/o contenedor;

iii) siempre que se produzca un cambio de personal que tenga conocimiento de las combinaciones; y

iv) siempre que exista o se sospeche de la existencia de un riesgo.

8) Seguridad física

a) Fuera del horario de trabajo normal la protección de las zonas que contengan Información Clasificada almacenada se llevará a cabo por guardas y/o mediante dispositivos electrónicos como circuitos cerrados de televisión y sistemas de alarma.

b) Se realizarán patrullas a intervalos que habrá de determinar la Autoridad Nacional de Seguridad a la luz de cualquier amenaza local.

c) En caso de que, a efectos de mantenimiento, reparaciones u otros fines, se requiera la entrada de personas no autorizadas en zonas que contengan Información Clasificada, se adoptarán las medidas necesarias para evitar que tengan acceso a dicha información. Deberán llevar a cabo sus actividades bajo supervisión permanente.

9) Visitantes. No deberán dejarse visitantes sin vigilancia en zonas que contengan Información Clasificada.

10) Destrucción

a) Con el fin de evitar la acumulación innecesaria, la Información Clasificada obsoleta o superflua se destruirá tan pronto como

sea factible mediante su quema, triturado o reducción a pasta o polvo de forma que impida su reconocimiento y reconstrucción.

b) Se registrará la destrucción de Información Clasificada con arreglo a los procedimientos establecidos por la Autoridad Nacional de Seguridad de cada Parte.

11) Dimensiones físicas del material con Información Clasificada. Cuando no sea posible aplicar las disposiciones y/o medidas anteriores relativas al traslado, embalaje, almacenamiento y destrucción debido a las dimensiones del material que contenga Información Clasificada, las Partes acordarán las medidas que resulten apropiadas.

12) Compromiso de la Información Clasificada

a) Se compromete la Información Clasificada cuando se divulga su conocimiento, total o parcialmente, a personas no autorizadas o cuando se ha producido riesgo de divulgación.

b) En todos los casos de compromiso, se enviará un informe de situación o un informe final sobre la investigación a la Autoridad Nacional de Seguridad de la otra Parte en un plazo de 90 días.

[TRANSLATION – TRADUCTION]

ACCORD DE SÉCURITÉ ENTRE LE ROYAUME D'ESPAGNE ET LE GOUVERNEMENT DE LA RÉPUBLIQUE SUD-AFRICAINE CONCERNANT LA PROTECTION DES INFORMATIONS CLASSIFIÉES ÉCHANGÉES ENTRE EUX DANS LE CADRE DE LA COOPÉRATION EN MATIÈRE DE DÉFENSE

Le Royaume d'Espagne et le Gouvernement de la République sud-africaine, ci-après dénommés collectivement les « Parties » et individuellement la « Partie »,

SOUHAITANT garantir la protection adéquate des informations classifiées échangées entre eux dans le cadre de la coopération en matière de défense,

SONT CONVENUS de ce qui suit :

ARTICLE PREMIER. DÉFINITIONS

Dans le présent Accord de sécurité (ci-après désigné le « présent Accord »), à moins que le contexte n'exige une interprétation différente :

le terme « information classifiée » désigne tout élément sous quelque forme que ce soit, y compris écrite, orale ou visuelle, et tout matériel auquel la Partie d'origine a, conformément à sa législation et à sa réglementation en matière de sécurité nationale, attribué une classification de sécurité ;

le terme « contrat classifié » désigne un contrat ou un contrat de sous-traitance conclu entre les Parties, entre les Parties et des contractants ou contractants potentiels ou entre contractants ou contractants potentiels, qui contient des informations classifiées ou dont l'exécution nécessite l'accès à des informations classifiées de l'une ou l'autre des Parties ;

le terme « contractant » désigne toute personne physique ou morale dotée de la capacité juridique de conclure des contrats ;

le terme « document » désigne toute lettre, toute note, tout procès-verbal, tout rapport, tout mémorandum, tout signal, tout message, tout croquis, toute photographie, tout film, toute carte, tout graphique, tout plan, tout carnet, tout pochoir, tout carbone, tout ruban de machine à écrire ou toute autre forme d'information enregistrée (par exemple, enregistrement sur bande, enregistrement magnétique, carte perforée ou ruban) ;

le terme « habilitation de sécurité d'établissement » désigne la constatation par l'Agence nationale de sécurité ou par une autre autorité compétente du fait que, du point de vue de la sécurité, une installation a la capacité physique et organisationnelle d'utiliser et de déposer des informations classifiées, conformément à la législation et à la réglementation nationales ;

le terme « matériel » désigne tout document et toute partie de machine, d'équipement et d'arme, fabriqué ou en cours de fabrication ;

le terme « Agence nationale de sécurité » désigne l'autorité désignée par une Partie responsable de l'élaboration de la politique de sécurité applicable et de la supervision du présent Accord ;

le terme « Partie d'origine » désigne la Partie qui génère et fournit une information classifiée et lui attribue une classification de sécurité nationale, et qui transmet des informations classifiées à l'autre Partie ;

le terme « habilitation de sécurité personnelle » désigne la reconnaissance par l'Agence nationale de sécurité qu'une personne a été habilitée à accéder à des informations classifiées et à les traiter jusqu'à un niveau de classification de sécurité spécifié conformément à la législation et à la réglementation nationales ;

le terme « instructions de sécurité du projet » désigne une compilation de la réglementation et des procédures de sécurité qui sont appliquées à un projet ou à un programme spécifique afin de normaliser les procédures de sécurité ;

le terme « Partie destinataire » désigne la Partie qui reçoit les informations classifiées de la Partie d'origine ;

le terme « sous-traitant » désigne un contractant à qui un maître d'œuvre confie un contrat de sous-traitance ;

le terme « tierce partie » désigne tout État, y compris les personnes physiques et morales sous sa juridiction, ou toute organisation internationale qui n'est pas partie au présent Accord.

ARTICLE 2. AGENCES NATIONALES DE SÉCURITÉ

1. Les Agences nationales de sécurité responsables du présent Accord sont les suivantes :
   a) en ce qui concerne le Royaume d'Espagne, le Secrétaire d'État, le Directeur du Centre national d'intelligence, le Bureau national de sécurité, au nom du Royaume d'Espagne;
   b) en ce qui concerne la République sud-africaine, le Chef des services de renseignement de la défense au nom du Gouvernement de la République sud-africaine.

2. Les Agences nationales de sécurité sont le canal officiel de communication entre les Parties pour toutes les questions relatives au présent Accord.

ARTICLE 3. OBLIGATIONS

1. Les Parties prennent, conformément au droit interne en vigueur dans leur pays respectif, toutes les mesures nécessaires en vue de protéger les informations classifiées échangées ou générées dans le cadre du présent Accord.

2. Les Parties veillent à ce que les informations classifiées reçues dans le cadre du présent Accord bénéficient au moins de la même protection que celle accordée aux informations nationales de même niveau de classification. Les normes de sécurité énoncées à l'annexe A, qui fait partie intégrante du présent Accord, sont considérées comme un niveau minimal de protection.

3. En vue d'atteindre et de maintenir des normes de sécurité comparables, les Parties se fournissent mutuellement, si l'une ou l'autre d'entre elles en fait la demande, des renseignements sur leurs normes, leurs pratiques et leurs procédures nationales de sécurité aux fins de la protection des informations classifiées, y compris les normes, les pratiques et les procédures relatives aux opérations industrielles. Chacune des Parties informe par écrit l'autre Partie de toute modification

apportée à ces normes, à ces pratiques et à ces procédures de sécurité affectant la manière dont les informations classifiées sont protégées.

ARTICLE 4. ACCÈS AUX INFORMATIONS CLASSIFIÉES

1. Les Parties n'utilisent les informations classifiées qu'aux fins pour lesquelles elles ont été transmises.

2. L'accès aux informations classifiées est notamment limité aux personnes dont les fonctions exigent cet accès conformément au principe du besoin d'en connaître, qui sont titulaires d'une habilitation de sécurité du niveau approprié et qui ont la connaissance requise des procédures de sécurité. Nul ne peut avoir accès à des informations classifiées du seul fait de son rang ou de sa nomination.

3. Les informations classifiées ne sont pas divulguées par la Partie destinataire à une tierce partie sans le consentement préalable écrit de l'Agence nationale de sécurité de la Partie d'origine.

ARTICLE 5 . NIVEAUX DE CLASSIFICATION DE SÉCURITÉ

1. Aux fins du présent Accord, les Parties adoptent les équivalents suivants des classifications de sécurité :

Classification espagnole	**Classification sud-africaine**
RESERVADO	SECRET (SECRET)
CONFIDENCIAL	CONFIDENTIAL (CONFIDENTIEL)
DIFUSION LIMITADA	RESTRICTED (À DIFFUSION RESTREINTE)

2. Les informations classifiées traduites ou copiées et échangées dans le cadre du présent Accord se voient attribuer une classification de sécurité conformément à la législation et à la réglementation des Parties en matière de sécurité nationale.

3. Les informations classifiées générées par la coopération entre les parties se voient attribuer une classification de sécurité par consentement mutuel des Agences nationales de sécurité des Parties.

4. L'augmentation ou la diminution du niveau de la classification de sécurité et la déclassification des informations classifiées sont la prérogative de la Partie d'origine.

5. Les parties notifient par écrit, huit semaines à l'avance, leur intention d'augmenter ou de diminuer le niveau d'une classification de sécurité ou de déclassifier des informations classifiées.

6. En ce qui concerne les informations classifiées provenant de tierces parties, les procédures relatives à leur protection et à leur diffusion sont conformes à la législation nationale en la matière régissant la protection de ces informations classifiées.

ARTICLE 6 . CANAUX DE TRANSFERT DES INFORMATIONS CLASSIFIÉES

1. Les informations classifiées sont transmises par la voie diplomatique. La Partie destinataire accuse réception et, le cas échéant, se charge de la poursuite du transfert.

2. En cas d'urgence, l'utilisation de canaux autres que la voie diplomatique peut être convenue par les Agences nationales de sécurité des deux Parties.

3. Les Parties peuvent transférer des informations classifiées par des moyens électroniques sécurisés conformément aux procédures de sécurité établies d'un commun accord par les Agences nationales de sécurité des Parties.

ARTICLE 7. CONTRATS CLASSIFIÉS

1. Une Partie qui souhaite conclure un contrat classifié avec un contractant de l'autre Partie ou qui souhaite autoriser l'un de ses propres contractants à conclure un contrat classifié sur le territoire de l'autre Partie dans le cadre d'un projet classifié obtient au préalable, par l'intermédiaire de son Agence nationale de sécurité, l'assurance écrite de l'Agence nationale de sécurité de l'autre Partie que le contractant proposé dispose d'une habilitation de sécurité d'établissement du niveau approprié.

2. Le contractant s'engage :

a) à s'assurer que ses locaux disposent d'installations adéquates pour la protection appropriée des informations classifiées ;

b) à obtenir et à maintenir un niveau approprié d'habilitation de sécurité pour ses locaux ;

c) à obtenir et à maintenir un niveau approprié d'habilitation de sécurité personnelle pour les personnes qui exercent des fonctions nécessitant l'accès à des informations classifiées ;

d) à garantir que toutes les personnes ayant accès aux informations classifiées sont informées de leurs responsabilités en matière de protection des informations classifiées, conformément à la législation nationale en vigueur ;

e) à effectuer des inspections de sécurité régulières de ses locaux.

3. Tout sous-traitant se conforme aux mêmes obligations de sécurité que les contractants.

4. Dès le début de négociations précontractuelles entre un organisme établi sur le territoire de l'une des Parties et un autre organisme établi sur le territoire de l'autre Partie, visant à la signature d'instruments contractuels classifiés, l'Agence nationale de sécurité compétente informe l'autre Partie du niveau de classification de sécurité assigné aux informations classifiées relatives auxdites négociations précontractuelles.

5. Tout contrat classifié conclu entre des organismes des Parties en vertu des dispositions du présent Accord contient des dispositions appropriées en matière de sécurité, qui définissent les aspects suivants :

a) un guide de classification et une liste des informations classifiées ;

b) des procédures de communication des modifications du niveau de classification des informations ;

c) des canaux de communication et des moyens de transmission électromagnétique ;

d) des procédures de transport du matériel classifié ;

e) les autorités compétentes responsables de la coordination de la protection des informations classifiées relatives au contrat ;

f) une obligation de notifier toute perte, toute fuite ou toute compromission constatée ou présumée des informations classifiées.

6. Un exemplaire des dispositions en matière de sécurité de tout contrat classifié est transmis à l'Agence nationale de sécurité de la Partie sur le territoire de laquelle il est prévu d'effectuer les travaux afin de permettre une supervision et un contrôle adéquats en matière de sécurité.

7. Les experts en sécurité des Agences nationales de sécurité se rendent périodiquement visite, lorsque cela convient aux deux Parties, afin de discuter des procédures et des installations de protection des informations classifiées.

8. Le cas échéant, les instructions de sécurité du projet sont échangées entre les Parties.

ARTICLE 8. DEMANDES DE VISITE

1. Les représentants autorisés de chacune des Parties ou le personnel des industries concernées ont accès aux informations classifiées et aux établissements où se déroulent des activités classifiées, sous réserve de l'autorisation préalable de la Partie à visiter.

2. Les demandes de visites sont faites auprès de l'Agence nationale de sécurité de la Partie à visiter au moins deux semaines à l'avance.

3. Les demandes contiennent les renseignements suivants :

a) les coordonnées du ou des représentants [nom et prénom(s), lieu et date de naissance, nationalité et numéro de passeport] ;

b) le nom de l'agence, de l'établissement, de l'installation ou de l'organisation que le visiteur représente ou duquel il fait partie ;

c) la certification, la validité et les limites de l'habilitation de sécurité personnelle du visiteur ;

d) le niveau le plus élevé anticipé des informations classifiées concernées ;

e) l'objet de la visite ;

f) la date et la durée de la visite, et si la demande concerne une autorisation de visites récurrentes intermittentes ; en cas de visites récurrentes, la période totale cumulée des visites est indiquée ;

g) le ou les établissements et les personnes à visiter, y compris un numéro de téléphone afin de les contacter.

4. La validité de l'autorisation de visite, y compris pour les visites récurrentes intermittentes d'un établissement spécifié, ne dépasse pas douze mois. Lorsqu'il est prévu qu'une visite particulière ne sera pas effectuée dans les délais approuvés, ou qu'une prolongation de la période pour les visites récurrentes intermittentes est nécessaire, la Partie effectuant la visite soumet une nouvelle demande d'autorisation de visite au moins vingt jours ouvrables avant l'expiration de l'autorisation de visite actuelle.

5. L'Agence nationale de sécurité de la Partie hôte informe les responsables de la sécurité de l'agence, de l'établissement, de l'installation ou de l'organisation à visiter des détails des

personnes dont la demande de visite a été approuvée. Une fois l'autorisation donnée, les dispositions de visite pour les personnes qui ont reçu une autorisation de visite récurrente intermittente peuvent être prises directement auprès de l'agence, de l'établissement, de l'installation ou de l'organisation concernés.

ARTICLE 9. POINTS DE CONTACT

1. Point de contact au Royaume d'Espagne :

Oficina Nacional de Seguridad,
Calle Argentona 20
28023 MADRID
Espagne

2. Point de contact en République sud-africaine :

a) pour les questions d'ordre militaire :

Chef des services de renseignement de la défense
Private Bag X367
PRETORIA
0001
République sud-africaine

b) pour les questions relatives à l'industrie militaire :

Directeur principal de la sécurité
Division de la sécurité Armscor
Private Bag X337
PRETORIA
0001
République sud-africaine

ARTICLE 10. ATTEINTES À LA SÉCURITÉ

Les atteintes à la sécurité qui peuvent éventuellement conduire ou qui ont déjà conduit à une compromission sont traitées par les Agences nationales de sécurité concernées, conformément au droit interne en vigueur dans les pays des Parties. Les Parties s'informent immédiatement des circonstances, des mesures prises et de leur résultat.

ARTICLE 11. FRAIS

Si des frais sont générés, chacune des Parties prend en charge ses propres frais liés à la mise en œuvre du présent Accord.

ARTICLE 12. DROITS DE PROPRIÉTÉ INTELLECTUELLE

Aucune disposition du présent Accord ne réduit ou ne restreint tout droit de propriété intellectuelle acquis ou existant, y compris les brevets et les droits d'auteurs, relatif à une information classifiée auquel l'une ou l'autre des Parties ou une tierce partie peut prétendre.

ARTICLE 13. ACCORDS DE MISE EN ŒUVRE

Des accords de mise en œuvre peuvent être conclus dans le cadre du présent Accord lorsque des programmes de collaboration spécifiques sont identifiés.

ARTICLE 14. MODIFICATION

Le présent Accord peut être modifié à tout moment par écrit, par la voie diplomatique, d'un commun accord entre les Parties.

ARTICLE 15. ENTRÉE EN VIGUEUR, DURÉE ET DÉNONCIATION

1. Le présent Accord entre en vigueur lorsque les Parties se sont mutuellement notifié par écrit l'accomplissement de leurs procédures constitutionnelles nécessaires à cet effet. Le présent Accord entre en vigueur à la date de réception de la dernière notification.

2. Le présent Accord reste en vigueur pour une durée illimitée, sauf dénonciation par l'une ou l'autre des Parties moyennant un préavis de six mois donné par écrit à l'autre Partie par la voie diplomatique l'informant de son intention de dénoncer le présent Accord.

3. En cas de dénonciation, les Parties restituent, dans la mesure du possible, toutes les informations classifiées échangées ou générées par la coopération entre les Parties dans le cadre du présent Accord. Si la restitution des informations classifiées n'est pas possible, les Parties continuent à protéger ces informations classifiées conformément aux dispositions du présent Accord.

ARTICLE 16. RÈGLEMENT DES DIFFÉRENDS

Tout différend relatif à l'interprétation, à l'application ou à la mise en œuvre des dispositions du présent Accord est réglé à l'amiable par voie de consultation ou de négociation entre les Parties.

EN FOI DE QUOI les soussignés, dûment autorisés à cet effet par leur gouvernement respectif, ont signé le présent Accord en deux exemplaires originaux en langues espagnole et anglaise, les deux textes faisant également foi, et y ont apposé leur sceau.

FAIT à Madrid, le 4 octobre 2017.

Pour le Gouvernement du Royaume d'Espagne :

FÉLIX SANZ ROLDÁN,

Secrétaire d'État, Directeur du Centre national du renseignement

Pour le Gouvernement de la République sud-africaine :

JEREMIAH MDUDUZI NYEMBE,

Général de corps d'armée, Chef des services de renseignement de la défense de l'Afrique du Sud

ANNEXE A
NORMES MINIMALES DE SÉCURITÉ

1) Introduction
   a) Les principaux objectifs de la sécurité sont la protection :
      i) des informations classifiées contre l'espionnage, la compromission, la divulgation non autorisée, la perte ou le vol ;
      ii) des installations vitales contre le sabotage.
   b) Les Parties désignent un agent responsable de la sécurité dans chaque installation concernée, par exemple une usine, un bureau ou un établissement où des informations classifiées sont traitées et stockées.
   c) L'agent responsable de la sécurité est chargé d'assurer la protection adéquate des informations classifiées.
   d) Un plan de sécurité établissant toutes les dispositions et mesures de sécurité (personnel, documents, matériel, organisation, physique et, le cas échéant, informatique) est établi pour chaque installation. Les plans de sécurité et toute modification de ceux-ci doivent être approuvés par l'Agence nationale de sécurité de la Partie concernée.
   e) L'Agence nationale de sécurité concernée effectue régulièrement des inspections de sécurité dans les installations visées au paragraphe b) ci-dessus.
2) Définition de la classification de sécurité
   a) Pour le Royaume d'Espagne
      i) RESERVADO. « RESERVADO » est la classification de sécurité attribuée aux informations dont la divulgation non autorisée ou l'utilisation illicite mettrait en danger les intérêts nationaux ou leur causerait un dommage grave.
      ii) CONFIDENCIAL. « CONFIDENCIAL » est la classification de sécurité attribuée aux informations dont la divulgation non autorisée ou l'utilisation illicite mettrait en danger les intérêts nationaux ou leur causerait un dommage.
      iii) DIFUSION LIMITADA. « DIFUSION LIMITADA » est la classification de sécurité attribuée aux informations dont la divulgation non autorisée ou l'utilisation illicite serait contraire aux intérêts nationaux.
   b) Pour la République sud-africaine
      i) SECRET. SECRET (« SECRET ») est la classification attribuée aux informations qui peuvent être utilisées par des éléments hostiles, opposants ou malveillants pour perturber les objectifs et les fonctions d'une institution ou d'un État.
      ii) CONFIDENTIAL. CONFIDENTIAL (« CONFIDENTIEL ») est la classification de sécurité attribuée aux informations qui peuvent être utilisées par des éléments hostiles, opposants ou malveillants pour causer des dommages aux objectifs d'une personne ou d'une institution.
      iii) RESTRICTED. RESTRICTED (« À DIFFUSION RESTREINTE ») est la classification de sécurité attribuée à toutes les informations qui peuvent être

utilisées par des éléments hostiles, opposants ou malveillants afin de gêner une institution ou une personne ou entraver ses activités.

3) Documents

a) Le courrier contenant des informations classifiées n'est ouvert et traité que par des personnes autorisées.

b) Avant d'être traité, chaque document classifié est enregistré.

c) L'enregistrement des informations classifiées se fait sur des listes séparées en fonction de leur classification. L'enregistrement permet à l'Agence nationale de sécurité de suivre à tout moment les informations classifiées.

d) En cas de traduction ou de copie, la classification de sécurité attribuée au nouveau document est la même que celle attribuée au document original.

e) Les classifications ou les marquages spéciaux ne sont pas supprimés et des extraits ou des paraphrases de l'information ne sont pas faits sans indiquer la classification ou le marquage spécial attribués au document original.

4) Transfert des informations classifiées

a) Le transfert international d'informations classifiées se fait par valise diplomatique, par service de courrier militaire ou, exceptionnellement, par service de courrier privé si les Parties en conviennent ainsi.

b) En cas de transfert international, la réception des informations classifiées doit faire l'objet d'un accusé de réception.

c) Le transfert national d'informations classifiées se fait par courrier, par service de messagerie autorisé ou, exceptionnellement, par service postal sous forme de courrier recommandé.

d) Les coursiers et les messagers employés aux fins du transport des informations classifiées disposent d'une habilitation de sécurité délivrée par l'Agence nationale de sécurité compétente. Les coursiers et les messagers sont instruits de leurs devoirs en matière de protection des informations qui leur sont confiées.

5) Conditionnement

a) Les règles suivantes s'appliquent au conditionnement des informations classifiées :

i) les informations classifiées sont transférées sous une double couverture opaque et solide ; la couverture intérieure est scellée et estampillée de la classification appropriée et porte la désignation et l'adresse complètes du destinataire ; le cas échéant, la couverture intérieure peut porter la mention « À OUVRIR UNIQUEMENT PAR : [nom de la personne autorisée à ouvrir la couverture (intérieure)] » ;

ii) le conditionnement de la couverture intérieure doit être tel qu'il est impossible de l'ouvrir sans briser le sceau ou endommager la couverture ;

iii) la couverture intérieure doit être entourée d'une couverture extérieure solide ;

iv) la couverture extérieure porte une désignation (mais pas de nom), l'adresse et un numéro de colis à des fins de transfert et n'indique pas la classification du contenu ni le fait qu'elle contient des informations classifiées ;

v) si les informations sont transférées sous double couverture par service de courrier, la couverture extérieure doit porter clairement la mention : « PAR

SERVICE DE COURRIER UNIQUEMENT » ; une pochette ou une boîte fermée à clé ou une valise diplomatique scellée peuvent être considérées comme la couverture extérieure.

6) Stockage des informations classifiées

a) Des mesures sont prises pour empêcher les personnes non autorisées d'avoir accès aux informations classifiées.

b) Les informations classifiées doivent être traitées et stockées dans une zone de sécurité. Cette zone nécessite :

i) un périmètre clairement défini et protégé par lequel toutes les entrées et sorties sont contrôlées ;

ii) un système de contrôle d'accès qui n'admet que les personnes disposant de l'habilitation appropriée et spécialement autorisées à pénétrer dans la zone ;

iii) des dispositions d'escorte ou des moyens similaires de contrôle des visiteurs.

c) Les informations classifiées sont stockées dans une armoire métallique approuvée par l'Agence nationale de sécurité nationale de la Partie concernée.

d) La classification de sécurité attribuée à un volume d'informations est celle de la partie contenant la classification la plus élevée.

7) Clés et combinaisons

a) Les clés des coffres-forts, des armoires ou des conteneurs stockant des informations classifiées sont conservées dans la zone de sécurité. Les clés de rechange et un enregistrement écrit de chaque réglage de combinaison sont conservés par l'agent responsable de la sécurité dans une enveloppe opaque, scellée et signée et bénéficient d'une protection non moins stricte que les informations classifiées auxquelles ils donnent accès. Les clés de travail et les clés de rechange sont conservées dans des conteneurs séparés.

b) La connaissance des réglages de combinaison est limitée au plus petit nombre possible de personnes. Les paramètres sont modifiés :

i) à des intervalles ne dépassant pas six mois ;

ii) lorsqu'un coffre-fort, une armoire en acier ou un conteneur est installé ;

iii) à chaque changement de personnel connaissant la combinaison ;

iv) lorsqu'une compromission est soupçonnée ou s'est effectivement produite.

8) Sécurité physique

a) En dehors des heures de travail normales, la protection des zones contenant des informations classifiées stockées est assurée par des gardes ou par des moyens électroniques tels que la télévision en circuit fermé et les systèmes d'alarme.

b) Les patrouilles ont lieu à des intervalles déterminés par l'Agence nationale de sécurité en fonction de toute menace locale.

c) Si, à des fins de maintenance, de réparation ou autres, des personnes non autorisées doivent pénétrer dans des zones contenant des informations classifiées, des mesures sont prises pour les empêcher d'avoir accès à ces informations. Leurs activités s'exercent sous une surveillance permanente.

9) Visiteurs. Les visiteurs ne sont jamais laissés sans surveillance dans les zones contenant des informations classifiées.

10) Destruction.

a) Afin d'éviter toute accumulation inutile, toute obsolescence ou toute redondance, les informations classifiées sont détruites dès que possible par incinération, réduction en pulpe, déchiquetage ou pulvérisation sous une forme non reconnaissable et impossible à reconstituer.

b) L'enregistrement de la destruction des informations classifiées se fait conformément aux procédures établies par l'Agence nationale de sécurité de chacune des Parties.

11) Dimensions physiques du matériel contenant des informations classifiées. Lorsque les dispositions ou les mesures susmentionnées en ce qui concerne le transfert, le conditionnement, le stockage et la destruction ne sont pas réalisables en raison des dimensions physiques du matériel contenant des informations classifiées, les Parties conviennent de mesures appropriées.

12) Compromission des informations classifiées

a) Une information classifiée est compromise lorsque sa connaissance, en tout ou en partie, a été divulguée à des personnes non autorisées ou lorsqu'elle a été soumise au risque d'une telle divulgation.

b) Dans tous les cas de compromission, le rapport final ou un rapport d'avancement de l'enquête est soumis à l'Agence nationale de sécurité de l'autre Partie dans un délai de quatre-vingt-dix jours.