No. 49270*

Spain
and
Lithuania

Agreement between the Kingdom of Spain and the Republic of Lithuania on the mutual protection of classified information. Madrid, 7 May 2010

Entry into force: *14 December 2011 by notification, in accordance with article 13*

Authentic texts: *Lithuanian and Spanish*

Registration with the Secretariat of the United Nations: *Spain, 23 January 2012*

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
Lituanie

Accord entre le Royaume d'Espagne et la République de Lituanie relatif à la protection mutuelle des informations classifiées. Madrid, 7 mai 2010

Entrée en vigueur : *14 décembre 2011 par notification, conformément à l'article 13*

Textes authentiques : *lituanien et espagnol*

Enregistrement auprès du Secrétariat des Nations Unies : *Espagne, 23 janvier 2012*

* *Numéro de volume RTNU n'a pas encore été établie pour ce dossier. Les textes réproduits ci-dessous, s'ils sont disponibles, sont les textes authentiques de l'accord/pièce jointe d'action tel que soumises pour l'enregistrement et publication au Secrétariat. Pour référence, ils ont été présentés sous forme de la pagination consécutive. Les traductions, s'ils sont inclus, ne sont pas en form finale et sont fournies uniquement à titre d'information.*

[LITHUANIAN TEXT – TEXTE LITUANIEN]

ISPANIJOS KARALYSTĖS IR LIETUVOS RESPUBLIKOS

S U S I T A R I M A S

DĖL ĮSLAPTINTOS INFORMACIJOS ABIPUSĖS APSAUGOS

Ispanijos Karalystė ir Lietuvos Respublika (toliau – Šalys), *siekdamos* apsaugoti visą informaciją, kurią Šalys yra įslaptinusios pagal savo nacionalinę teisę ir kuria jos keičiasi,
s u s i t a r ė:

1 straipsnis
Tikslas ir taikymo sritis

1. Šio Susitarimo tikslas – užtikrinti įslaptintos informacijos, kuria Šalys keičiasi arba kurią parengia tarpusavyje bendradarbiaudamos, apsaugą.

2. Šis Susitarimas taikomas bet kokiai su įslaptinta informacija susijusiai veiklai, sandoriams ar susitarimams, kuriuos Šalys vykdys ar sudarys ateityje arba kuriuos jos vykdė ar sudarė iki šio Susitarimo įsigaliojimo.

2 straipsnis
Apibrėžtys

Šiame Susitarime:

1. **įslaptinta informacija** – bet kokio pavidalo, pobūdžio ar bet kuriomis priemonėmis perduodama parengta arba rengiama informacija ar medžiaga, kuri yra įslaptinta pagal nacionalinius įstatymus ir kitus norminius teisės aktus ir kuri turi būti saugoma nacionalinio saugumo interesais.

2. **slaptumo žyma** – ant įslaptintos informacijos rašoma žyma, rodanti jos įslaptinimo lygį, kuris atspindi jos svarbą, prieigos prie jos apribojimo lygį ir jos apsaugos lygį.

3. **asmens patikimumo pažymėjimas** – atlikus nacionalines patikrinimo procedūras priimtas teigiamas sprendimas, patvirtinantis fizinio asmens lojalumą ir patikimumą, taip pat kitus saugumo aspektus pagal nacionalinius įstatymus ir kitus norminius teisės aktus, ir suteikiantis tam fiziniam asmeniui teisę susipažinti ir dirbti su tam tikra slaptumo žyma žymima įslaptinta informacija.

4. **įmonės patikimumo pažymėjimas** – atlikus nacionalines patikrinimo procedūras priimtas teigiamas sprendimas, patvirtinantis, kad rangovui suteikiama teisė gauti tam tikra slaptumo žyma žymimą įslaptintą informaciją, su ja dirbti, ją apdoroti ir saugoti.

5. **informaciją parengusi Šalis** – Šalies institucija, kuri parengė įslaptintą informaciją.

1

6. **informaciją gaunanti Šalis** – Šalies institucija arba rangovas, kuriam įslaptinta informacija perduota.

7. **nacionalinė saugumo institucija** – valstybės institucija, kuri pagal atitinkamos Šalies nacionalinius įstatymus ir kitus norminius teisės aktus įgyvendina tos valstybės įslaptintos informacijos apsaugos politiką, vykdo bendrą šios srities kontrolę, taip pat prižiūri, kaip įgyvendinamas šis Susitarimas, įskaitant įgyvendinimo susitarimus. Šios institucijos yra išvardytos šio Susitarimo 5 straipsnyje.

8. **paskirtoji saugumo institucija** – kompetentinga institucija, kuri pagal atitinkamos Šalies nacionalinius įstatymus ir kitus norminius teisės aktus yra atsakinga už tam tikras jai priskirtas įslaptintos informacijos apsaugos sritis.

9. **rangovas** – fizinis ar juridinis asmuo, turintis teisę sudaryti įslaptintus sandorius pagal šio Susitarimo nuostatas.

10. **įslaptintas sandoris** – susitarimas, kuriame yra įslaptintos informacijos, kuris yra su ja susijęs arba kurio pagrindu įslaptinta informacija parengiama.

11. **principas „būtina žinoti“** – būtinybė susipažinti su įslaptinta informacija dėl einamų tarnybinių pareigų ir (arba) dėl konkrečios tarnybinės užduoties vykdymo.

12. **trečioji šalis** – valstybė arba tarptautinė organizacija, kuri nėra šio Susitarimo Šalis.

3 straipsnis
Slaptumo žymos

1. Šalys susitaria, kad toliau nurodytos informacijos slaptumo žymos atitinka viena kitą ir yra analogiškos informacijos slaptumo žymoms, nurodytoms atitinkamos Šalies nacionaliniuose įstatymuose ir kituose norminiuose teisės aktuose.

Ispanijos Karalystėje:	Lietuvos Respublikoje
SECRETO	VISIŠKAI SLAPTAI
RESERVADO	SLAPTAI
CONFIDENCIAL	KONFIDENCIALIAI
DIFUSIÓN LIMITADA	RIBOTO NAUDOJIMO

2. Informaciją parengusi Šalis praneša informaciją gaunančiai Šaliai apie visus perduotos įslaptintos informacijos slaptumo žymų pasikeitimus.

4 straipsnis
Įslaptintos informacijos abipusės apsaugos principai

1. Vadovaudamosi savo nacionaliniais įstatymais ir kitais norminiais teisės aktais, Šalys imasi visų reikiamų priemonių, kad būtų apsaugota pagal šį Susitarimą bendrai parengta įslaptinta informacija arba įslaptinta informacija, kuria buvo tiesiogiai ar netiesiogiai pasikeista. Tokiai įslaptintai informacijai turi būti užtikrinamas toks pats apsaugos lygis, koks yra suteikiamas nacionalinei ta pačia slaptumo žyma pažymėtai įslaptintai informacijai.

2. Susipažinti su įslaptinta informacija gali tik tie asmenys, kurie dėl savo vykdomų funkcijų privalo su ja susipažinti pagal principą „būtina žinoti“, kurie turi asmens patikimumo pažymėjimą, suteikiantį teisę susipažinti su įslaptinta informacija, žymima slaptumo žyma CONFIDENCIAL / KONFIDENCIALIAI ar aukštesnio lygio slaptumo žyma, ir kuriems ši teisė suteikta pagal nacionalinius įstatymus ir kitus norminius teisės aktus. Teisė susipažinti su įslaptinta informacija, žymima slaptumo žyma DIFUSIÓN LIMITADA / RIBOTO NAUDOJIMO, suteikiama pagal principa „būtina žinoti“.

3. Informaciją gaunanti Šalis įsipareigoja:

   a) neatskleisti įslaptintos informacijos trečiajai šaliai be išankstinio rašytinio informaciją parengusios Šalies nacionalinės saugumo institucijos sutikimo;

   b) suteikti įslaptintai informacijai slaptumo žymą, atitinkančią tą, kurią jai suteikė informaciją parengusi Šalis;

   c) naudoti įslaptintą informaciją tik tais tikslais, kuriais ji buvo perduota;

   d) garantuoti tokias su įslaptinta informacija susijusias privatines teises, kaip patentų teisė, autorių teisė ar komercinės paslaptys.

4. Jei kurio nors kito Šalių sudaryto susitarimo nuostatos dėl keitimosi įslaptinta informacija ar jos apsaugos yra griežtesnės, taikomos to susitarimo nuostatos.

5. Atitinkamos nacionalinės saugumo institucijos / paskirtosios saugumo institucijos gali sudaryti įgyvendinimo susitarimus dėl konkrečių šio Susitarimo nuostatų įgyvendinimo.

5 straipsnis
Nacionalinės saugumo institucijos

1. Šalių nacionalinės saugumo institucijos yra šios:

Ispanijos Karalystėje:	Lietuvos Respublikoje:
Valstybės Sekretorius, Nacionalinio žvalgybos centro direktorius Nacionalinis saugumo biuras	Paslapčių apsaugos koordinavimo komisija

2. Nacionalinės saugumo institucijos praneša viena kitai apie galiojančius nacionalinius įstatymus ir kitus norminius teisės aktus, reglamentuojančius įslaptintos informacijos apsaugą.

3. Siekdamos užtikrinti glaudų bendradarbiavimą įgyvendinant šį Susitarimą, nacionalinės saugumo institucijos vienos iš jų prašymu gali rengti konsultacijas.

4. Siekdamos panašių saugumo standartų ir stengdamosi juos palaikyti, nacionalinės saugumo institucijos, gavusios prašymą, teikia viena kitai informaciją apie atitinkamos Šalies įslaptintos informacijos apsaugai taikomus saugumo standartus, procedūras ir praktiką.

5. Atitinkamos nacionalinės saugumo institucijos praneša viena kitai apie visas paskirtąsias saugumo institucijas.

6 straipsnis
Įslaptintos informacijos perdavimas

1. Paprastai įslaptinta informacija perduodama diplomatiniais ar kariniais kanalais. Jei šiais kanalais įslaptintą informaciją perduoti būtų neįmanoma arba jei ji būtų gauta pavėluotai, ją gali perduoti tinkamai saugumo požiūriu patikrinti asmenys, kuriems toks įgaliojimas suteikiamas, įslaptintą informaciją perduodančios Šalies išduotu kurjerio pažymėjimu.

2. Informaciją gaunanti Šalis raštu patvirtina, kad gavo įslaptintą informaciją, pažymėtą slaptumo žyma CONFIDENCIAL / KONFIDENCIALIAI ar

aukštesnio lygio slaptumo žyma. Rašytinis įslaptintos informacijos, pažymėtos slaptumo žyma DIFUSIÓN LIMITADA / RIBOTO NAUDOJIMO, gavimo patvirtinimas pateikiamas informaciją parengusios Šalies prašymu.

3. Įslaptinta informacija gali būti perduodama nacionalinių saugumo institucijų / paskirtųjų saugumo institucijų patvirtintomis saugomomis elektroninių ryšių sistemomis, tinklais ar kitomis elektromagnetinėmis priemonėmis.

4. Kiti patvirtinti įslaptintos informacijos perdavimo būdai gali būti naudojami tik abipusiu nacionalinių saugumo institucijų / paskirtųjų saugumo institucijų susitarimu.

5. Jei reikia perduoti didelį įslaptintos informacijos kiekį, nacionalinės saugumo institucijos / paskirtosios saugumo institucijos abipusiškai suderina ir patvirtina transporto priemones, gabenimo maršrutą ir kitas saugumo priemones.

7 straipsnis
Vertimas, kopijavimas, naikinimas

1. Įslaptinta informacija, žymima slaptumo žyma SECRETO / VISIŠKAI SLAPTAI, verčiama arba kopijuojama tik gavus rašytinį informaciją parengusios Šalies leidimą.

2. Visą įslaptintą informaciją verčia asmenys, turintys atitinkamą asmens patikimumo pažymėjimą. Vertimai turi būti žymimi tomis pačiomis slaptumo žymomis, kokiomis buvo pažymėtas originalas.

3. Kiekviena įslaptintos informacijos kopija taip pat žymima visomis originalo slaptumo žymomis ir papildomomis darbo su ja instrukcijomis. Tokioms įslaptintos informacijos kopijoms taikoma tokia pati kontrolė kaip originalams. Kopijų daroma tik tiek, kiek reikia tarnybiniams tikslams.

4. Kai įslaptinta informacija, pažymėta slaptumo žyma RESERVADO / SLAPTAI, tampa nereikalinga, ji gali būti sunaikinta gavus išankstinį rašytinį informaciją parengusios Šalies sutikimą. Ji sunaikinama arba pakeičiama taip, kad jos – nei visos, nei dalies – nebūtų galima atkurti.

5. Be slaptumo žymos, informaciją parengusi Šalis gali pateikti ir kitas išsamias darbo su perduota įslaptinta informacija instrukcijas. Įslaptinta informacija, kurią sunaikinti draudžiama, grąžinama informaciją perdavusiai Šaliai.

6. Įslaptinta informacija, žymima slaptumo žyma SECRETO / VISIŠKAI SLAPTAI, nenaikinama. Ji grąžinama informaciją parengusiai Šaliai. Išskirtiniais atvejais, kai kyla staigus pavojus, kad tokia įslaptinta informacija gali būti prarasta arba atskleista, informaciją gaunanti Šalis ją sunaikina ir nedelsdama praneša apie tai informaciją parengusiai Šaliai.

8 straipsnis
Įslaptinti sandoriai

1. Į įslaptintus sandorius, susijusius su įslaptinta informacija, pažymėta slaptumo žyma DIFUSIÓN LIMITADA / RIBOTO NAUDOJIMO, įtraukiamas atitinkamas straipsnis, nustatantis minimalias priemones, taikytinas tokios įslaptintos informacijos apsaugai. Nacionalinės saugumo institucijos informuojamos apie tokius sandorius.

2. Įslaptintas sandoris sudaromas ir vykdomas pagal Šalių nacionalinius įstatymus ir kitus norminius teisės aktus. Kiekvienos Šalies nacionalinė saugumo institucija paprašyta teikia informaciją tik tokiam numatomam rangovui, kuriam yra išduotas atitinkamas įmonės patikimumo pažymėjimas, suteikiantis teisę susipažinti su reikiamo įslaptinimo lygio informacija. Jei numatomas rangovas neturi atitinkamo patikimumo pažymėjimo, kiekvienos Šalies nacionalinė saugumo institucija gali prašyti, kad tas rangovas būtų patikrintas saugumo požiūriu. Įslaptintas sandoris su šiuo rangovu sudaromas tik po to, kai jam buvo išduotas atitinkamas patikimumo pažymėjimas.

3. Šalies, kurioje bus vykdomas įslaptintas sandoris, nacionalinė saugumo institucija / paskirtoji saugumo institucija įsipareigoja įslaptintiems sandoriams nustatyti ir taikyti tokius pačius standartus ir reikalavimus, atitinkančias saugumo priemones, kuriuos ji taiko savo pačios įslaptintų sandorių apsaugai.

4. Prie kiekvieno įslaptinto sandorio ar jo pagrindu sudaryto sandorio su subrangovu pridedamas saugumui skirtas priedas, kuris yra įslaptinto sandorio sudedamoji dalis. Šiame priede informaciją parengusios Šalies rangovas nurodo, kokia įslaptinta informacija bus teikiama informaciją gaunančiai Šaliai ar bus jos parengta ir kokia atitinkama informacijos slaptumo žyma yra nustatyta šiai informacijai. Šio priedo kopija išsiunčiama Šalių nacionalinėms saugumo institucijoms / paskirtosioms saugumo institucijoms.

5. Rangovo įsipareigojimas saugoti įslaptintą informaciją visais atvejais mažiausiai apima:

a) rangovo įsipareigojimą įslaptintą informaciją atskleisti tik tam, kas turi asmens patikimumo pažymėjimą, kas atitinka principą „būtina žinoti" ir kam pavesta vykdyti ar kas dalyvauja vykdant įslaptintą sandorį;

b) priemones, kurios bus naudojamos įslaptintai informacijai perduoti;

c) pranešimo apie galimus pakeitimus, susijusius su įslaptinta informacija, dėl to, kad keičiama jos slaptumo žyma, arba dėl to, kad apsauga nebereikalinga, procedūras ir priemones;

d) įslaptintame sandoryje numatytų vienos Šalies personalo vizitų į kitos Šalies objektus, patekimo į juos ar jų apžiūrėjimo patvirtinimo tvarką;

e) įsipareigojimą laiku pranešti rangovo nacionalinei saugumo institucijai / paskirtajai saugumo institucijai apie visus įvykusius ar įtariamus neteisėtos prieigos prie įslaptinto sandorio įslaptintos informacijos atvejus, tai pat apie mėginimus tai padaryti;

f) su įslaptintu sandoriu susijusios įslaptintos informacijos naudojimą tik su įslaptinto sandorio dalyku susijusiems tikslams;

g) griežtą įslaptintos informacijos sunaikinimo procedūrų laikymąsi.

6. Įslaptintos informacijos apsaugai reikalingos priemonės, taip pat dėl neteisėtos prieigos prie įslaptintos informacijos rangovams padarytų galimų nuostolių įvertinimo ir kompensavimo tvarka išsamiau išdėstoma atitinkamame įslaptintame sandoryje.

9 straipsnis
Vizitai

1. Vienos Šalies piliečių vizitai į kitą Šalį, kurių metu reikės susipažinti su įslaptinta informacija, turi būti iš anksto raštu patvirtinti priimančiosios Šalies nacionalinės saugumo institucijos / paskirtosios saugumo institucijos.

2. Prašymas leisti atvykti vizito pateikiamas per nacionalinę saugumo instituciją / paskirtąją saugumo instituciją ne vėliau kaip likus dvidešimčiai (20) kalendorinių dienų iki vizito. Skubiais atvejais prašymas leisti atvyti vizito pateikiamas ne vėliau kaip likus penkioms (5) darbo dienoms iki vizito.

3. Viena Šalis leidžia asmenims iš kitos Šalies atvykti vizito, kurio metu reikės susipažinti su įslaptinta informacija, tik jei šie asmenys:

a) turi atitinkamą juos siunčiančios Šalies nacionalinės saugumo institucijos išduotą asmens patikimumo pažymėjimą; ir

b) pagal savo Šalies nacionalinius įstatymus ir kitus norminius teisės aktus turi teisę gauti įslaptintą informaciją ar su ja susipažinti.

4. Prašyme leisti atvykti vizito pateikiama ši informacija:

a) atvykstančio asmens vardas ir pavardė, gimimo data ir vieta, paso (arba asmens tapatybės kortelės) numeris;

b) atvykstančio asmens pilietybė;

c) atvykstančio asmens pareigos ir organizacijos, kuriai jis atstovauja, pavadinimas;

d) atvykstančio asmens asmens patikimumo pažymėjimo patvirtinimas, įslaptinimo lygis ir galiojimas;

e) vizito tikslas, siūloma darbo programa ir numatoma vizito data;

f) organizacijų ir objektų, į kuriuos prašoma leisti atvykti, pavadinimai;

g) asmens ryšiams palaikyti įmonėje (ar objekte), kuriuose bus lankomasi, vardas, pavardė ir telefono numeris, buvę kontaktai ir visa kita informacija, galinti padėti nustatyti vizito ar vizitų pagrįstumą;

h) data, parašas ir atitinkamos nacionalinės saugumo institucijos paskirtosios saugumo institucijos oficialus antspaudas.

5. Kiekviena Šalis pagal atitinkamus nacionalinius įstatymus ir kitus norminius teisės aktus užtikrina atvykstančių asmenų asmens duomenų apsaugą.

6. Leidimai atvykti vizito galioja ne ilgiau kaip vienus metus.

7. Vykdant bet kokį projektą, programą ar sandorį, Šalys bendru sutarimu gali nustatyti asmenų, kuriems leidžiama atvykti pasikartojančių vizitų, sąrašą. Šalims patvirtinus tokius sąrašus, konkrečių vizitų sąlygos derinamos tiesiogiai su organizacijų, į kurias minėtieji asmenys atvyks, saugumo pareigūnu pagal suderintas sąlygas.

10 straipsnis
Saugumo pažeidimas

1. Įvykus saugumo pažeidimui, dėl kurio prarandama ar atskleidžiama arba gali būti prarasta ar atskleista Šalių viena kitai perduota įslaptinta informacija, Šalies, kurioje saugumas buvo pažeistas, nacionalinė saugumo institucija kuo greičiau apie tai praneša kitos Šalies nacionalinei saugumo institucijai ir užtikrina atitinkamą tyrimą. Prireikus kita Šalis bendradarbiauja atliekant tyrimą.

2. Kitai Šaliai pranešami tyrimo rezultatai ir pateikiama galutinė išvada dėl saugumo pažeidimo.

11 straipsnis
Išlaidos

Kiekviena Šalis apmoka savo išlaidas, susijusias su savo įsipareigojimų pagal šį Susitarimą vykdymu.

12 straipsnis
Ginčų sprendimas

Visi ginčai dėl šio Susitarimo aiškinimo ar taikymo sprendžiami Šalių tarpusavio konsultacijomis, nesikreipiant į jokį nacionalinį ar tarptautinį teismą ar trečiąją šalį.

13 straipsnis
Baigiamosios nuostatos

1. Šis Susitarimas sudaromas neapibrėžtam laikotarpiui ir įsigalioja nuo tos dienos, kai gaunamas paskutinis pranešimas, kuriuo Šalys praneša viena kitai, kad įvykdyti visi vidaus teisės reikalavimai, būtini šiam Susitarimui įsigalioti.

2. Šis Susitarimas gali būti keičiamas abipusiu rašytiniu Šalių sutikimu. Tokie pakeitimai įsigalioja šio straipsnio 1 dalyje nustatyta tvarka.

3. Bet kuri Šalis gali nutraukti šį Susitarimą apie tai raštu pranešdama kitai Šaliai. Nutraukimas įsigalioja praėjus šešiems mėnesiams nuo dienos, kai kita Šalis gavo šį rašytinį pranešimą, tačiau neturi įtakos įsipareigojimams, prisiimtiems iki jo pagal šio Susitarimo nuostatas. Visų pirma toliau pagal

šio Susitarimo nuostatas saugoma visa įslaptinta informacija, kuri buvo perduota arba kuria buvo apsikeista pagal šį Susitarimą.

Pasirašytas 2010 m. gegužės 7 d. Madride dviem egzemplioriais lietuvių ir ispanų kalbomis. Visi tekstai yra autentiški.

Ispanijos Karalystės vardu	**Lietuvos Respublikos vardu**
Félix Sanz Roldán	**Romualdas Vaišnoras**
Valstybes Sekretorius	**Valstybės saugumo departamento**
Nacionalinio Žvalgybos Centro	**Generalinio Direktoriaus**
Direktorius	**pavaduotojas**

[SPANISH TEXT – TEXTE ESPAGNOL]

ACUERDO

ENTRE

EL REINO DE ESPAÑA

Y

LA REPÚBLICA DE LITUANIA

PARA LA PROTECCIÓN MUTUA

DE INFORMACIÓN CLASIFICADA

El Reino de España

y

la República de Lituania

(en adelante denominados las "Partes"),

con el fin de proteger mutuamente toda la información que haya sido clasificada por cualquiera de las Partes con arreglo a su derecho interno y que las Partes intercambien entre sí,

Han convenido en lo siguiente:

Artículo 1
Objeto y ámbito de aplicación

1. El objeto del presente Acuerdo es garantizar la protección de la Información Clasificada intercambiada o creada con motivo de la cooperación entre las Partes.

2. El presente Acuerdo será de aplicación a cualesquiera actividades, contratos o acuerdos que tengan relación con Información Clasificada y que se desarrollen o se celebren en el futuro entre las Partes o que se hayan desarrollado o celebrado antes de la entrada en vigor del presente Acuerdo.

Artículo 2
Definiciones

A los efectos del presente Acuerdo:

1. Por **"Información Clasificada"** se entenderá la información o el material, sea cual fuere su forma, naturaleza o medio de transmisión, ya elaborados o en proceso de elaboración, que hayan sido clasificados conforme a las leyes y reglamentos nacionales y que requieran protección en interés de la seguridad nacional.

2. Por **"Marcas de Clasificación"** se entenderá toda marca realizada sobre cualquier Información Clasificada, en la que se especifique el nivel de clasificación de seguridad y se determine la importancia de la información

clasificada, el nivel de restricción de acceso a la misma y su nivel de protección.

3. Por **"Habilitación Personal de Seguridad"** se entenderá toda decisión en sentido positivo, fruto de un procedimiento nacional de investigación, por la que se garantice la lealtad y la fiabilidad de una persona, así como otros aspectos relativos a la seguridad, de conformidad con las leyes y reglamentos nacionales, y que permita el acceso y el manejo de Información Clasificada hasta un nivel de clasificación de seguridad determinado.

4. Por **"Habilitación de Seguridad para Establecimiento"** se entenderá toda decisión en sentido positivo, fruto de un procedimiento nacional de investigación, por la que se certifique que se autoriza a un contratista a recibir, manejar, procesar y almacenar Información Clasificada hasta un nivel de clasificación de seguridad determinado.

5. Por **"Parte de Origen"** se entenderá cualquier institución de la Parte que genere la Información Clasificada.

6. Por **"Parte Receptora"** se entenderá cualquier institución o contratista de la Parte que reciba la Información Clasificada.

7. Por **"Autoridad Nacional de Seguridad"** se entenderá la autoridad que, de conformidad con las leyes y reglamentos nacionales de las respectivas Partes, ejecute la política estatal de protección de Información Clasificada, ejerza el control pleno en dicho ámbito y supervise el cumplimiento del presente Acuerdo, incluidos todos los acuerdos de ejecución. Dichas autoridades figuran en el artículo 5 del presente Acuerdo.

8. Por **"Autoridad de Seguridad Designada"** se entenderá la autoridad competente que, en cumplimiento de las leyes y reglamentos nacionales de cada Parte, sea responsable de las áreas designadas de protección de Información Clasificada.

9. Por **"Contratista"** se entenderá una persona física o jurídica que tenga la capacidad jurídica para celebrar un Contrato Clasificado con arreglo a lo dispuesto en el presente Acuerdo.

10. Por **"Contrato Clasificado"** se entenderá un acuerdo que contenga o tenga relación con Información Clasificada o en el marco del cual se genere Información Clasificada.

11. Por el principio de **"Necesidad de Conocer"** se entenderá la necesidad de tener acceso a la Información Clasificada en conexión con sus obligaciones oficiales y/o para el desempeño de una determinada tarea oficial.

12. Por **"Tercera Parte"** se entenderá cualquier Estado u organización internacional que no sea Parte en el presente Acuerdo.

Artículo 3
Marcas de clasificación

1. Las Partes convienen en que las Marcas de Clasificación que se indican a continuación son equivalentes y corresponden a las Marcas de Clasificación de información especificadas en las leyes y reglamentos nacionales de las respectivas Partes:

Para el Reino de España	Para la República de Lituania
SECRETO	VISISKAI SLAPTAI
RESERVADO	SLAPTAI
CONFIDENCIAL	KONFIDENCIALIAI
DIFUSIÓN LIMITADA	RIBOTO NAUDOJMO

2. La Parte De Origen informará a la Parte Receptora de cualquier cambio en las Marcas de Clasificación de la Información Clasificada que se intercambie.

Artículo 4
Principios de la protección recíproca de la Información Clasificada

1. De conformidad con sus leyes y reglamentos nacionales, las Partes adoptarán todas las medidas adecuadas para la protección de la Información Clasificada que se genere o se intercambie normalmente, ya sea directa o indirectamente, en virtud del presente Acuerdo. Deberá garantizarse el mismo nivel de protección para dicha Información Clasificada que el que se conceda a la Información Clasificada nacional, con la correspondiente Marca de Clasificación.

2. El acceso a la Información Clasificada estará restringido a las personas que, para el desempeño de sus funciones, deban tener acceso a la Información Clasificada, basándose en la "necesidad de conocer", sean titulares de una Habilitación de Seguridad del Personal para el acceso a la Información Clasificada CONFIDENCIAL/KONFIDENCIALIAI o de

grado superior y hayan sido autorizados de conformidad con las leyes y reglamentos nacionales. Se dará acceso a la Información Clasificada de DIFUSIÓN LIMITADA/RIBOTO NAUDOJMO aplicando el principio de la "necesidad de conocer"

3. La Parte Receptora está obligada a:

   a) no divulgar la Información Clasificada a una Tercera Parte, sin el consentimiento previo por escrito de la Autoridad Nacional de Seguridad de la Parte de Origen;

   b) otorgar a la Información Clasificada una marca de clasificación equivalente a la impuesta por la Parte de Origen;

   c) no utilizar la Información Clasificada para fines distintos de aquellos para los que fue proporcionada;

   d) garantizar los derechos de particulares, como derechos de patente, derechos de autor o secretos comerciales que afecten a la Información Clasificada.

4. En caso de que cualquier otro acuerdo celebrado entre las Partes contenga normas más estrictas en relación con el intercambio o la protección de Información Clasificada, se aplicarán esas normas.

5. Las respectivas Autoridades Nacionales de Seguridad/Autoridades de Seguridad Designadas podrán celebrar acuerdos de ejecución relativos a los aspectos detallados de la aplicación del presente Acuerdo.

Artículo 5
Autoridades Nacionales de Seguridad

1. Las Autoridades Nacionales de Seguridad de las Partes son:

Para el Reino de España	Para la República de Lituania
Secretario de Estado Director del Centro Nacional de Inteligencia Oficina Nacional de Seguridad	Comisión para la Coordinación de la Protección de Secretos

2. Las Autoridades Nacionales de Seguridad se informarán recíprocamente sobre las leyes y reglamentos nacionales en vigor que regulen la protección de Información Clasificada.

3. Con el fin de garantizar la estrecha colaboración en la aplicación del presente Acuerdo, las Autoridades Nacionales de Seguridad podrán celebrar consultas a petición de cualquiera de ellas.

4. Con objeto de establecer y mantener normas similares en materia de seguridad, las Autoridades Nacionales de Seguridad se proporcionarán, previa petición, información sobre las normas, procedimientos y prácticas de seguridad para la protección de Información Clasificada aplicados por cada Parte.

5. Las respectivas Autoridades Nacionales de Seguridad se informarán recíprocamente sobre todas las Autoridades de Seguridad Designadas.

Artículo 6
Transmisión de Información Clasificada

1. Como regla general, la Información Clasificada se transmitirá por conducto diplomático o militar. Si el uso de estos conductos no fuera posible o retrasara excesivamente la recepción de la Información Clasificada, las transmisiones podrán llevarse a cabo por personal con la habilitación de seguridad adecuada y con acreditación de correo expedida por la Parte que transmita la Información Clasificada.

2. La Parte Receptora deberá confirmar por escrito la recepción de la Información Clasificada CONFIDENCIAL/KONFIDENCIALIAI o de grado superior. Se dará confirmación por escrito de la recepción de Información Clasificada de DIFUSIÓN LIMITADA/RIBOTO NAUDOJMO si así lo solicita la Parte de Origen.

3. La Información Clasificada podrá transmitirse por sistemas protegidos de telecomunicaciones, redes u otros medios electromagnéticos que aprueben las Autoridades Nacionales de Seguridad/Autoridades de Seguridad Designadas.

4. Podrán utilizarse otros medios de transmisión de Información Clasificada únicamente si así lo acuerdan las Autoridades Nacionales de Seguridad/Autoridades de Seguridad Designadas.

5. En caso de transmisión de grandes volúmenes de Información Clasificada, las Autoridades Nacionales de Seguridad/Autoridades de Seguridad Designadas acordarán y aprobarán conjuntamente el medio de transporte, la ruta y otras medidas de seguridad.

Artículo 7

Traducción, reproducción y destrucción

1. Se autorizará la reproducción o la traducción de la Información Clasificada con el grado de SECRETO/VISISKAI SLAPTAI sólo con el consentimiento previo por escrito de la Parte de Origen.

2. Todas las traducciones de Información Clasificada se realizarán por personas que tengan la Habilitación Personal de Seguridad apropiada. Dicha traducción llevará todas las Marcas de Clasificación originales.

3. Al reproducir Información Clasificada todas las marcas de clasificación originales y las instrucciones adicionales para su tratamiento deberán también reproducirse o marcarse en cada copia. La Información Clasificada así reproducida se someterá al mismo control que la Información Clasificada original. El número de copias se limitará a las requeridas para fines oficiales.

4. La Información Clasificada con el grado de RESERVADO/SLAPTAI podrá destruirse cuando deje de ser necesaria, con el consentimiento previo por escrito de la Parte de Origen. La Información Clasificada se destruirá o modificará en la medida necesaria para evitar su reconstrucción total o parcial.

5. La Parte de Origen, además de las Marcas de Clasificación, podrá dar otras instrucciones relativas al tratamiento en que se detalle en uso de la Información Clasificada transmitida. En caso de que se prohíba la destrucción de la Información Clasificada, ésta se devolverá a la Parte de Origen.

6. No podrá destruirse la Información Clasificada con el grado de SECRETO/VISISKAI SLAPTAI. Deberá devolverse a la Parte de Origen. En los casos excepcionales de peligro inmediato de pérdida o divulgación la Parte Receptora deberá destruirla e informar inmediatamente a la Parte de Origen.

Artículo 8

Contratos Clasificados

1. Los Contratos Clasificados que tengan relación con Información Clasificada de DIFUSIÓN LIMITADA/RIBOTO NAUDOJMO deberán contener una cláusula apropiada en que se establecerán las medidas mínimas que han de aplicarse para la protección de dicha Información

Clasificada. Se informará a las Autoridades de Seguridad Nacional sobre dichos contratos.

2. Todo Contrato Clasificado deberá celebrarse y ejecutarse de conformidad con las leyes y reglamentos nacionales de cada Parte. Previa petición, la Autoridad Nacional de Seguridad de cada Parte únicamente proporcionará información al contratista propuesto que disponga de la adecuada Habilitación de Seguridad para Establecimiento que corresponda al nivel requerido de clasificación de seguridad de la información. En caso de que el contratista propuesto no disponga de la habilitación de seguridad adecuada, la Autoridad Nacional de Seguridad de cada Parte podrá solicitar que se expida la misma a dicho contratista. Deberá expedirse una habilitación de seguridad adecuada al contratista antes de la celebración del Contrato Clasificado.

3. La Autoridad Nacional de Seguridad/Autoridad de Seguridad Designada de la Parte en que haya de ejecutarse el Contrato Clasificado asumirá la responsabilidad de dictar y hacer cumplir las medidas de seguridad relativas al Contrato Clasificado con arreglo a las mismas normas y requisitos por los que se rija la protección de sus propios Contratos Clasificados.

4. Cada Contrato o subcontrato Clasificado incluirá, como parte integrante del mismo, un Anexo sobre Información Clasificada. En ese Anexo, el contratista de la Parte de Origen especificará la Información Clasificada que se cederá a la Parte Receptora o que será generada por ésta y la Marca de Clasificación de información que se haya asignado a dicha información. Se enviará a las Autoridades Nacionales de Seguridad/Autoridades de Seguridad Designadas de las Partes una copia de dicho anexo.

5. La obligación del contratista de proteger la Información Clasificada incluirá en todo caso, como mínimo, los siguientes aspectos:

   a) la obligación de que el contratista divulgue la Información Confidencial únicamente a la persona que posea una Habilitación Personal de Seguridad, que tenga "necesidad de conocer" y que haya sido contratada para la ejecución del Contrato Clasificado o participe en dicha ejecución.

   b) los medios que habrán de emplearse para transmitir la Información Clasificada;

   c) los procedimientos y mecanismos para comunicar los cambios que puedan producirse respecto de la Información Clasificada, ya sea debido

a cambios en la Marca de Clasificación de información o a que la protección deje de ser necesaria;

d) el procedimiento para la aprobación de las visitas, el acceso o la inspección por el personal de una Parte a las instalaciones de la otra Parte, en el marco del Contrato Clasificado;

e) la obligación de notificar oportunamente a la Autoridad Nacional de Seguridad/Autoridad de Seguridad Designada del contratista todo acceso no autorizado efectivo o presunto, a la Información Clasificada a que se refiera el Contrato Clasificado;

f) la utilización de la Información Clasificada en virtud del Contrato Clasificado únicamente para los fines mencionados en el objeto del mismo;

g) la estricta observancia de los procedimientos de destrucción de la Información Clasificada.

6. En cada Contrato Clasificado se especificarán más detalladamente las medidas requeridas para la protección de la Información Clasificada, así como el procedimiento de evaluación e indemnización por las posibles pérdidas sufridas por los contratistas debido al acceso no autorizado a dicha información.

Artículo 9
Visitas

1. Las visitas de nacionales de una Parte a la otra Parte que supongan acceso a Información Clasificada estarán sujetas a la previa autorización por escrito de la Autoridad de Seguridad Nacional/Autoridad de Seguridad Designada de la Parte anfitriona.

2. Toda solicitud de visita se cursará a través de la Autoridad de Seguridad Nacional/Autoridad de Seguridad Designada, al menos veinte (20) días naturales antes de la visita. En casos urgentes, podrá cursarse la solicitud de visita al menos cinco (5) días hábiles antes de la fecha de la misma.

3. Una Parte sólo permitirá a visitantes de la otra Parte visitas que supongan acceso a Información Clasificada cuando:

a) hayan obtenido la Habilitación Personal de Seguridad correspondiente de la Autoridad de Seguridad Nacional de la Parte que envía; y

b) hayan sido autorizados a recibir Información Clasificada o tener acceso a la misma de conformidad con las leyes y reglamentos nacionales de su Parte.

4. La solicitud de visita deberá contener la siguiente información:

a) nombre del visitante, fecha y lugar de nacimiento, número de pasaporte (o tarjeta de identidad);

b) nacionalidad del visitante;

c) cargo del visitante y nombre de la entidad a la que representa;

d) certificado de Habilitación Personal de Seguridad del visitante, su nivel de clasificación y periodo de validez;

e) finalidad, programa de trabajo previsto y fecha de la visita;

f) nombre de las organizaciones e instalaciones que se desee visitar;

g) nombre y número de teléfono del punto de contacto en el establecimiento o instalación objeto de la visita, contactos previos y cualquier otra información que sirva para justificar la visita o visitas;

h) fecha, firma y sello oficial de la correspondiente Autoridad de Seguridad Nacional/Autoridad de Seguridad Designada.

5. Cada Parte garantizará la protección de los datos personales de los visitantes, de conformidad con las leyes y reglamentos nacionales respectivos.

6. Una autorización de visita tendrá una validez máxima de un año.

7. Las Partes podrán acordar, respecto de cualquier proyecto, programa o contrato, la elaboración de listados de personas autorizadas a realizar visitas recurrentes. Una vez que las Partes hayan aprobado estos listados, las condiciones de cada visita se acordarán directamente con el Oficial de Seguridad de las organizaciones que vayan a ser visitadas por dichas personas, con arreglo a los términos y condiciones que se convengan.

Artículo 10
Infracción de la seguridad

1. En caso de que tenga lugar una infracción de la seguridad que dé o pueda dar lugar a la pérdida o a la divulgación de la Información Clasificada intercambiada entre la Partes, la Autoridad Nacional de Seguridad en la que se haya producido la infracción de la seguridad informará a la Autoridad Nacional de Seguridad de la otra Parte tan pronto como sea posible y garantizará que se lleve a cabo la investigación apropiada. La otra Parte colaborará en la investigación si fuera necesario.

2. La otra Parte será informada de los resultados de la investigación y recibirá un informe final sobre la infracción de la seguridad.

Artículo 11
Gastos

Cada Parte correrá con sus propios gastos derivados del cumplimiento de sus obligaciones en virtud del presente Acuerdo.

Artículo 12
Solución de controversias

Toda controversia relativa a la interpretación o a la aplicación del presente Acuerdo se resolverá mediante consultas entre las Partes y no podrá someterse para su resolución a ningún tribunal, ya sea nacional o internacional, ni a ninguna tercera Parte.

Artículo 13
Disposiciones finales

1. El presente Acuerdo se celebra por un periodo indefinido y entrará en vigor en la fecha de recepción de la última notificación por la cual las Partes se informen mutuamente del cumplimiento de todos los procedimientos jurídicos internos para su entrada en vigor.

2. El presente Acuerdo podrá ser enmendado con el consentimiento mutuo por escrito de las dos Partes. Dichas enmiendas entrarán en vigor de conformidad con el apartado 1 del presente artículo.

3. Cualquiera de las Partes podrá denunciar el presente Acuerdo mediante notificación por escrito a la otra Parte. La denuncia surtirá efecto seis meses después de la recepción de la notificación por la otra Parte, pero no afectará a las obligaciones ya contraídas en virtud de lo dispuesto en el presente Acuerdo. En particular, se mantendrá la protección de toda la información clasificada que se proporcione o se intercambie en virtud del presente Acuerdo, de conformidad con lo dispuesto en el mismo.

Hecho en Madrid el 7 de mayo de 2010 en dos originales, cada uno en español y lituano, siendo ambos textos igualmente auténticos.

Por el Reino de España

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

Por la República de Lituania

ROMUALDAS VAIŠNORAS
Director General Adjunto del
Departamento de Seguridad del Estado

[TRANSLATION – TRADUCTION]

AGREEMENT BETWEEN THE KINGDOM OF SPAIN AND THE REPUBLIC OF LITHUANIA CONCERNING THE RECIPROCAL PROTECTION OF CLASSIFIED INFORMATION

The Kingdom of Spain and the Republic of Lithuania,

(hereinafter referred to as "the Parties"),

For the purpose of reciprocal protection of all information classified by either of the Parties in accordance with its domestic legislation and exchanged between the Parties,

Have agreed as follows:

Article 1. Purpose and scope of application

1. The purpose of this Agreement is to ensure the protection of classified information exchanged, or created for purposes of cooperation, between the Parties.

2. This Agreement shall apply to all activities, contracts or agreements having any connection with classified information and prepared or concluded between the Parties at any future time or developed or concluded prior to the entry into force of this Agreement.

Article 2. Definitions

1. "Classified information" shall mean information and materials, regardless of their form and nature or means of transmission, whether already prepared or in course of preparation, classified in accordance with national laws and regulations and requiring protection in the interest of national security;

2. "Classification marking" shall mean any marking assigned to any classified information indicating the security classification level and the importance of the information indicated together with the level of restriction of access thereto and its level of protection.

3. "Personnel security clearance" shall mean any positive decision being the outcome of a national investigation proceeding guaranteeing the loyalty and trustworthiness of a person and other security elements in accordance with national laws and regulations and permitting access to and handling of classified information up to a given security classification level.

4. "Facility security clearance" shall mean any positive decision being the outcome of a national investigation proceeding, certifying that a contractor is authorized to receive, handle, process and store classified information up to a given security classification level.

5. "Originating Party" shall mean any institution of the Party creating the classified information,

6. “Receiving Party” shall mean any institution or contractor of the Party receiving the classified information.

7. “National security authority” shall mean the authority which, in conformity with the national laws and regulations of the respective Parties, implements State policy concerning protection of classified information, exercises full control in that area and supervises compliance with this Agreement, including all implementation agreements. The authorities concerned are listed in article 5 of this Agreement.

8. “Designated security authority” shall mean the authority responsible, in compliance with the national laws and regulations of each Party, in the designated areas of protection of classified information.

9. “Contractor” shall mean any physical or legal person with the legal capacity to conclude a classified contract in accordance in accordance with the provisions of this Agreement.

10. “Classified contract” shall mean an agreement containing or relating to classified information or within which classified information is created.

11. The “need-to-know” principle shall mean the need to have access to classified information in connection with a person’s official duties and/or the performance of a specific official task.

12. “Third Party” shall mean any State or international organization which is not a Party to this Agreement.

Article 3.Classification markings

1. The Parties agree that the classification markings given below are equivalent and correspond to the information classification markings specified in the national laws and regulations of the respective Parties:

For the Kingdom of Spain	For the Republic of Lithuania:
SECRETO (TOP SECRET)	VISISKAI SLAPTAI
RESERVADO (SECRET)	SLAPTAI
CONFIDENCIAL(CONFIDENTIAL)	KONFID ENCIALIAI
DIFUSION LIMITADA (RESTRICTED)	RIBOTO NAUDOJMO

2. The originating Party shall inform the receiving Party of any change in the classification markings on classified information exchanged.

Article 4.Principles governing reciprocal protection of classified information

1. In accordance with their national laws and regulations, the Parties shall adopt all appropriate measures for the protection of classified information normally developed or exchanged, either directly or indirectly, under this Agreement. The level of protection guaranteed for such classified information shall be the same as that accorded to national classified information with the corresponding classification marking.

2. Access to classified information shall be restricted to persons who must have access to the classified information for the performance of their duties on the basis of the

"need-to-know" principle and have a personnel security clearance for access to classified information at CONFIDENTIAL (CONFIDENCIAL/KONFIDENCIAI) or a higher level and have received authorization in accordance with national laws and regulations. Access to RESTRICTED (DIFUSION LIMITADA/RIBOTO NAUDOJMO) classified information shall be given applying the "need-to-know" principle.

3. The receiving Party shall be required:

(a) Not to disclose classified information to a third Party without the prior written consent of the national security authority of the originating Party;

(b) To assign to the classified information a classification marking equivalent to that fixed by the originating Party;

(c) Not to use the classified information for any purposes other than those for which it was provided;

(d) To guarantee individual rights such as patent rights, copyright and trade secrets affecting the classified information.

4. If any other agreement concluded between the Parties contains stricter standards relating to the exchange or protection of classified information, those standards shall be applied.

5. The national security authorities/designated security authorities concerned may conclude implementation agreements concerning detailed aspects of implementation of this Agreement.

Article 5.National security authorities

1. The national security authorities of the Parties are:

For the Kingdom of Spain	For the Republic of Lithuania
Director of the National Intelligence	Coordination Committee for Secrecy Agency, National Security Office Protection

2. The national security authorities shall reciprocally inform one another on the national laws and regulations in force regulating the protection of classified information.

3. In order to ensure close cooperation in the implementation of this Agreement, the national security authorities may enter into consultations at the request of either.

4. In order to establish and maintain similar standards with regard to security matters, the national security authorities shall furnish one another on request with information on the security standards, procedures and practices applied by each Party for the protection of classified information.

5. The national security authorities shall keep one another informed of all designated security authorities.

Article 6.Transmission of classified information

1. As a general rule, classified information shall be transmitted through diplomatic or military channels. If the use of such channels would be impracticable or unduly delay receipt of the classified information, transmissions may be effected by appropriately

security-cleared personnel empowered with a courier certificate issued by the Party transmitting the classified information.

2. The receiving Party must confirm receipt of classified information of CONFIDENTIAL (CONFIDENCIAL/KONFIDENCIAI) or a higher level in writing. It shall confirm receipt of classified information of RESTRICTED (DIFUSION LIMITADA/RIBOTO NAUDOJMO) level in writing if so requested by the originating Party.

3. Classified information may be transmitted by secure telecommunication systems, networks or other electromagnetic media approved by the national security authorities/designated security authorities.

4. Other means of transmission of classified information may be used only with the agreement of the national security authorities/designated security authorities.

5. In cases of transmission of classified information in bulk, the national security authorities/designated security authorities shall jointly decide on and approve the means of transport, the route and other security measures.

Article 7.Translation, reproduction and destruction

1. Reproduction and translation of TOP SECRET (SECRETO/VISISKAI SLAPTAI) classified information shall be authorized solely with the prior consent in writing of the originating Party.

2. All translations of classified information shall be effected by persons with the appropriate security clearance. Such translations shall carry all the original classification markings.

3. When classified information is reproduced, all the original classification markings and additional instructions for treatment of the information must also be reproduced or marked on each copy. Classified information so reproduced shall be subject to the same controls as the original classified information. The number of copies shall be restricted to the number required for official use.

4. Information classified at the SECRET (RESERVADO/SLAPTAI) level may when no longer required be destroyed with the prior written consent of the originating Party. The classified information shall be destroyed or modified in such a manner as to prevent its total or partial reconstruction.

5. In addition to the classification markings, the originating Party may give other instructions on treatment specifying the use of the classified information transmitted. In such cases destruction of the classified information is prohibited, it shall be returned to the originating Party.

6. Classified information of the TOP SECRET (RESERVADO/VISISKAI SLAPTAI) level may not be destroyed. It must be returned to the originating Party. In special cases, where there is an immediate danger of loss or disclosure, the receiving Party must destroy the information and immediately inform the originating Party.

Article 8.Classified contracts

1. Classified contracts having any connection with classified information of the RESTRICTED (DIFUSION LIMITADA/RIBOTO NAUDOJMO) level must contain an appropriate clause laying down the minimum measures to be taken to protect that classified information. The national security authorities shall be informed of such contracts.

2. Every classified contract shall be concluded and performed in accordance with the national laws and regulations of each Party. On prior request the national security authority of either Party shall supply information only to the proposed contractor holding the appropriate facility security clearance corresponding to the required security classification level of the information. If the contractor proposed does not hold the appropriate security clearance, the national security of either Party may request that such clearance be conferred on the contractor concerned. The contractor must be issued with the appropriate security clearance before conclusion of the contract.

3. The national security authority/designated security authority of the Party in which the contract is to be performed shall take responsibility for laying down security measures concerning the contract and compliance therewith, in accordance with the same standards and requirements as those governing protection of its own classified contracts.

4. Every classified contract and subcontract shall include, as an integral part thereof, an annex concerning classified information. In that annex the contractor of the originating Party shall specify the classified information to be made over to the receiving Party, or which will be created by the latter, and the information classification marking to be assigned to that information. Copies of that annex shall be sent to the national security authorities/designated security authorities of the Parties.

5. The obligation of the contractor to protect classified information shall in all cases, and as a minimum, the following elements:

(a) The obligation of the contractor to disclose confidential information solely to the person with a personnel security clearance, who has a “need to know” and is under contract for the performance of the contract or is participating therein;

(b) The measures to be taken to transmit the classified information;

(c) Procedures and mechanisms for communicating any changes related to classified information because of a modification in its security classification or because protection is no longer necessary;

(d) Procedures for authorizing visits, access or inspections by the personnel of one Party to facilities of the other Party under the contract;

(e) The obligation to notify the national security authorities/designated security authorities of the contractor in due time of any case of unauthorized access, whether actual or suspected, to classified information referred to in the contract;

(f) Use of classified information under the contract solely for the purposes mentioned in the object thereof;

(g) Strict compliance with procedures for the destruction of the classified information.

6. Each classified contract shall set out in greater detail the measures required for the protection of classified information and the procedure for evaluation and compensation of possible losses suffered by contractors on account of unauthorized access to that information.

Article 9. Visits

1. Visits implying access to classified information by nationals of one Party to the other Party are subject to prior written approval by the national security authority/designated national security authority of the host Party.

2. Requests for visits shall be submitted through the national security authority/designated national security authority not less than twenty (20) calendar days before the visit. In urgent cases a request may be submitted not less than five (5) working days before the date of the visit.

3. One Party may permit visitors from the other Party to make visits implying access to classified information only if:

(a) The visitors have obtained the appropriate personnel security clearance from the national security authority of the sending Party;

(b) They have been authorized to receive or have access to classified information under the national laws and regulations of their Party.

4. Requests for visits must contain the following information:

(a) The name, date and place of birth of the visitor and his/her passport or identity card number;

(b) The nationality of the visitor;

(c) The function of the visitor and the name of the entity he/she represents;

(d) The personnel security clearance certificate of the visitor and its classification level and period of validity;

(e) The purpose of the visit, the proposed programme of work and the date of the visit;

(f) The names of the organizations and facilities it is desired to visit;

(g) The name and phone number of the point of contact at the establishment or facility to be visited, the purpose of the visit, previous contacts and any other information useful for determining the justification of the visit or visits;

(h) The date, signature and official seal of the appropriate national security authority/designated national security authority.

5. Each Party guarantees protection of the personal data of visitors in accordance with the national laws and regulations of each.

6. A visitor’s permit is valid for one year.

7. For any project, programme or contract the Parties may agree to establish lists of individuals authorized to make recurring visits. Once the lists have been approved by the Parties, the terms of each visit shall be directly arranged with the security officers in the organizations to be visited by these individuals in accordance with the terms and conditions agreed on.

Article 10. Breaches of security

1. In the event of a breach of security which gives rise to, or may give rise to, the loss or disclosure of classified information exchanged between the Parties, the national security authority in which the breach has occurred shall inform the national security authority of the other Party as soon as possible and guarantee to carry out an appropriate investigation. The other Party shall cooperate in the investigation where necessary.

2. The other Party shall be informed of the result of the investigation and shall receive a final report on the security breach.

Article 11.Expenses

Each Party will meet its own expenses arising from discharge of its obligations under this Agreement.

Article 12. Disputes

Any disputes arising from the interpretation or implementation of this Agreement shall be settled through consultations between the Parties. They may not be referred for settlement to any national or international tribunal or any third Party.

Article 13.Final provisions

1. This Agreement shall be valid for an indefinite period. It shall enter into force on the date of receipt of the last notification whereby the Parties inform one another that all domestic legal procedures for its entry into force have been completed.

2. This Agreement may be amended by mutual consent in writing by the two Parties. Such amendments shall enter into force in accordance with paragraph 1 of this article.

3. Either Party may denounce this Agreement by written notice to the other Party. Denunciation shall take effect six months after receipt of the notice from the other Party but shall not affect the obligations already entered into under the provisions of this Agreement. In particular, protection of all the information provided or exchanged under this Agreement shall remain in place, in accordance with the provisions of the latter.

DONE at Madrid on 7 May 2010 in two originals, each in Spanish and Lithuanian, both texts being equally authentic.

For the Kingdom of Spain:

FELIX SANZ ROLDÁN
Secretary of State, Director, National Intelligence Centre

For the Republic of Lithuania:

ROMUALDAS VAIŠNORAS
Deputy Director-General, Department of State Security

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE ROYAUME D'ESPAGNE ET LA RÉPUBLIQUE DE LITUANIE RELATIF À LA PROTECTION MUTUELLE DES INFORMATIONS CLASSÉES

Le Royaume d'Espagne et la République de Lituanie

(ci-après dénommés les « Parties »),

Afin de garantir la protection mutuelle de toutes les informations que l'une des deux Parties a classées conformément à son droit interne et que les Parties échangent,

Sont convenus de ce qui suit :

Article premier. Objet et champ d'application

1. L'objet du présent Accord est de garantir la protection des informations classées qui sont échangées ou produites aux fins de la coopération entre les Parties.

2. Le présent Accord s'applique à toutes les activités menées et à tous les contrats ou accords conclus à l'avenir par les Parties en ce qui concerne des informations classées, ou à celles menées ou ceux conclus en la matière avant l'entrée en vigueur du présent Accord.

Article 2. Définitions

Aux fins du présent Accord, les termes ci-après s'entendent comme suit :

1. « Informations classées » : toute information ou tout matériel, quels qu'en soient la forme, la nature ou le moyen de transmission, déjà produit ou en cours d'élaboration, qui ont été classés conformément aux lois et réglementations nationales et qui nécessitent une protection dans l'intérêt de la sécurité nationale.

2. « Cote de sécurité » : toute mention apposée sur des informations classées, indiquant le niveau de sécurité et fixant l'importance des informations classées, les restrictions d'accès et le niveau de protection.

3. « Habilitation personnelle de sécurité » : toute décision découlant d'une enquête nationale attestant la loyauté et la fiabilité d'une personne, de même que d'autres facteurs afférents à la sécurité, conformément aux lois et réglementations nationales, et habilitant cette personne à avoir accès à des informations classées jusqu'à une certaine cote de sécurité, et à les manipuler.

4. « Habilitation de sécurité d'un établissement » : toute décision découlant d'une enquête nationale certifiant qu'un contractant est habilité à recevoir, gérer, manipuler et stocker des informations classées jusqu'à un certain niveau de sécurité.

5. « Partie d'origine » : toute institution de la Partie qui produit les informations classées.

6. « Partie destinataire » : toute institution ou tout contractant de la Partie qui reçoit les informations classées.

7. « Autorité nationale de sécurité » : autorité qui, conformément aux lois et réglementations nationales de chacune des Parties, est responsable de l'exécution de la politique nationale de protection des informations classées, exerce pleinement le contrôle dans ce domaine, et supervise la mise en œuvre du présent Accord, y compris des accords d'exécution. Ces autorités figurent à l'article 5 du présent Accord.

8. « Autorité de sécurité désignée » : autorité compétente qui, conformément aux lois et réglementations nationales de chacune des Parties, est chargée des domaines désignés de protection des informations classées.

9. « Contractant » : toute personne physique ou morale dotée de la capacité juridique de conclure un contrat classé conformément aux dispositions du présent Accord.

10. « Contrat classé » : accord qui renferme ou implique des informations classées, ou dans le cadre duquel des informations classées sont produites.

11. « Besoin d'en connaître » : principe en vertu duquel l'accès à des informations classées est accordé aux personnes qui en ont besoin pour mener à bien leurs obligations officielles et/ou s'acquitter d'une tâche officielle donnée.

12. « Tierce partie » : tout État ou organisation internationale qui n'est pas partie au présent Accord.

Article 3. Cotes de sécurité

1. Les Parties conviennent que les cotes de sécurité suivantes sont équivalentes et correspondent aux cotes de sécurité des informations spécifiées dans les lois et règlementations nationales respectives des Parties :

Pour le Royaume d'Espagne	Pour la République de Lituanie :
Secreto (top secret)	Visiskaislaptai (top secret)
Reservado (secret)	Slaptai (secret)
Confidencial (confidentiel)	Konfidencialiai (confidentiel)
Difusión limitada (diffusion restreinte)	Riboto naudojmo (diffusion restreinte)

2. La Partie d'origine informe la Partie destinataire de toute modification de la cote de sécurité des informations classées qui ont été échangées.

Article 4. Principe de la protection réciproque des informations classées

1. Conformément à leurs lois et règlementations nationales, les Parties prennent toutes les mesures nécessaires aux fins de la protection des informations classées qui sont produites ou échangées normalement, que ce soit directement ou indirectement, en vertu du présent Accord. Ces informations classées doivent recevoir le même niveau de protection que celui qui est accordé aux informations classées sur le plan national, ainsi que la cote de sécurité correspondante.

2. L'accès aux informations classées est limité aux personnes qui en ont besoin dans le cadre de l'exercice de leurs fonctions, selon le principe du « besoin d'en connaître », ainsi qu'aux personnes qui sont titulaires d'une habilitation personnelle de sécurité leur octroyant l'accès aux informations classées « Confidencial/Konfidencialiai » (confidentiel) ou plus, et qui ont obtenu cette autorisation conformément aux lois et réglementations nationales. L'accès aux informations classées « Difusión limitada/Riboto naudojmo » (diffusion restreinte) est autorisé sur la base du principe du « besoin d'en connaître ».

3. La Partie destinataire est tenue :

a) De ne pas divulguer des informations classées à une tierce partie sans le consentement préalable écrit de l'autorité nationale de sécurité de la Partie d'origine;

b) D'attribuer aux informations classées une cote de sécurité équivalente à celle attribuée par la Partie d'origine;

c) De n'utiliser les informations classées qu'aux fins pour lesquelles elles ont été transmises;

d) De garantir les droits des individus, tels que les droits de brevet, les droits d'auteur ou les secrets industriels, qui ont trait aux informations classées.

4. Si un autre accord conclu entre les Parties contient des normes plus restrictives en matière d'échange et de protection d'informations classées, ces normes s'appliquent.

5. Les autorités nationales de sécurité/autorités de sécurité désignées de chacune des deux Parties peuvent conclure des accords d'exécution relativement à certains aspects précis de l'application du présent Accord.

Article 5. Autorités nationales de sécurité

1. Les autorités nationales de sécurité des Parties sont les suivantes :

Pour le Royaume d'Espagne	Pour la République de Lituanie
Le Secrétaire d'État	Le Bureau de la sécurité nationale
Le Directeur du Centre national de renseignements	
La Commission pour la coordination de la protection des secrets	

2. Les autorités nationales de sécurité s'informent mutuellement des lois et réglementations nationales en vigueur qui régissent la protection des informations classées.

3. Afin de garantir une étroite collaboration aux fins de l'application du présent Accord, les autorités nationales de sécurité peuvent tenir des consultations à la demande de l'une d'entre elles.

4. Dans le but d'établir et d'utiliser des normes comparables en matière de sécurité, les autorités nationales de sécurité s'informent, sur demande, des normes, procédures et pratiques de sécurité en matière de protection des informations classées appliquées par chacune des Parties.

5. Les autorités nationales de sécurité de chacune des deux Parties s'informent mutuellement de ce qui a trait à toutes les autorités de sécurité désignées.

Article 6. Transmission des informations classées

1. Les informations classées sont normalement transmises entre les Parties par la voie diplomatique ou militaire. Si le recours à ces voies est impossible ou retarde indûment la réception des informations classées, les transmissions peuvent être effectuées par des agents dotés de l'habilitation de sécurité adéquate et habilités par un ordre de mission délivré par la Partie qui transmet les informations classées.

2. La Partie destinataire doit confirmer par écrit la réception des informations classées « Confidencial/Konfidencialiai » (confidentiel) ou plus. Si la Partie d'origine le demande, la réception des informations classées « Difusión limitada/Riboto naudojmo » (diffusion restreinte) est confirmée par écrit.

3. Les informations classées peuvent se transmettre par des systèmes de télécommunication sécurisés, des réseaux ou d'autres moyens électromagnétiques, approuvés par les autorités nationales de sécurité/autorités de sécurité désignées.

4. D'autres moyens de transmission des informations classées peuvent être utilisés à condition que les autorités nationales de sécurité/autorités de sécurité désignées y consentent.

5. Lorsque d'importants volumes d'informations classées doivent être transmis, les autorités nationales de sécurité/autorités de sécurité désignées choisissent et approuvent d'un commun accord le moyen de transport et l'itinéraire emprunté et les autres mesures de sécurité.

Article 7. Traduction, reproduction et destruction

1. Les informations classées « Secreto/Visiskai slaptai » (top secret) ne peuvent être traduites ou reproduites qu'avec le consentement préalable écrit de la Partie d'origine.

2. La traduction d'informations classées ne peut être assurée que par des personnes auxquelles a été délivrée l'habilitation personnelle de sécurité voulue. Les traductions portent les mêmes cotes de sécurité que les originaux.

3. Toutes les reproductions d'informations classées portent les mêmes cotes de sécurité que les originaux, et les instructions supplémentaires concernant le traitement des informations classées doivent être reproduites ou indiquées pour chaque exemplaire. Les informations classées ainsi reproduites sont soumises au même contrôle que les informations classées originales. Le nombre de reproductions est limité au nombre requis à des fins officielles.

4. Les informations classées « Reservado/Slaptai » (secret) peuvent être détruites lorsqu'elles ne présentent plus d'utilité, avec le consentement préalable écrit de la Partie d'origine. Les informations classées sont détruites ou modifiées de telle manière que leur reconstitution totale ou partielle soit impossible.

5. Outre l'attribution d'une cote de sécurité, la Partie d'origine peut donner d'autres instructions relatives au traitement des informations classées, précisant l'utilisation qui peut en être faite. Si les informations classées ne doivent pas être détruites, elles sont restituées à la Partie d'origine.

6. Les informations classées « Secreto/Visiskai slaptai » (top secret) ne peuvent être détruites et doivent être restituées à la Partie d'origine. Dans les cas exceptionnels où ces informations courent le risque imminent d'être perdues ou divulguées, la Partie destinataire doit les détruire et en informer immédiatement la Partie d'origine.

Article 8. Contrats classés

1. Les contrats classés qui ont trait à des informations classées « Difusión limitada/Riboto naudojmo »(diffusion restreinte) doivent contenir une clause appropriée définissant les mesures minimales qu'il convient d'appliquer pour protéger ces informations. Les autorités nationales de sécurité sont informées de l'existence de tels contrats.

2. Tout contrat classé doit être conclu et exécuté conformément aux lois et réglementations nationales de chacune des Parties. Sur demande, l'autorité nationale de sécurité de chacune des Parties ne fournit des informations au contractant proposé que s'il dispose de l'habilitation de sécurité (établissement) qui est nécessaire et correspond à la cote de sécurité des informations. Si le contractant proposé ne dispose pas de l'habilitation de sécurité requise, l'autorité nationale de sécurité de chacune des Parties peut demander à ce qu'il lui en soit délivré une. Le contractant doit disposer de l'habilitation de sécurité nécessaire avant la signature du contrat classé.

3. L'autorité nationale de sécurité/autorité de sécurité désignée de la Partie sur le territoire de laquelle le contrat classé doit être exécuté assume la responsabilité de l'imposition et de l'application des mesures de sécurité relatives au contrat classé, et ce, conformément aux mêmes normes et exigences qui régissent la protection de ses propres contrats classés.

4. Chaque contrat ou marché classé comprend une annexe concernant les informations classées, , qui en fait partie intégrante et dans laquelle le contractant de la Partie d'origine indique les informations classées qui sont transmises à la Partie destinataire ou que cette dernière produit, ainsi que la cote de sécurité qui a été assignée aux informations. Une copie de cette annexe est envoyée aux autorités nationales de sécurité/autorités de sécurité désignées des Parties.

5. Les obligations du contractant en matière de protection des informations classées sont au minimum les suivantes :

a) Ne divulguer d'informations classées qu'à des personnes qui détiennent une habilitation de sécurité personnelle, qui justifient du « besoin d'en connaître » et qui sont employées pour exécuter le contrat classé ou participent à son exécution;

b) Mettre en œuvre les moyens nécessaires pour transmettre les informations classées;

c) Mettre en œuvre les procédures et mécanismes permettant de communiquer tout changement éventuel concernant les informations classées, soit du fait de la modification de la cote de sécurité des informations, soit parce que les mesures de protection ne sont plus nécessaires;

d) Mettre en œuvre les procédures d'autorisation des visites, d'accès ou d'inspection applicables, aux termes du contrat classé, au personnel d'une Partie s'agissant des installations de l'autre Partie;

e) Informer en temps voulu son autorité nationale de sécurité/autorité de sécurité désignée de tout accès ou de toute tentative d'accès non autorisé aux informations classées sur lesquelles porte le contrat classé;

f) N'utiliser les informations classées en vertu du contrat classé qu'aux fins indiquées dans l'objet de celui-ci;

g) Se conformer strictement aux procédures établies en ce qui concerne la destruction des informations classées.

6. Chaque contrat classé précise plus en détail les mesures à prendre pour assurer la protection des informations classées, ainsi que la procédure d'évaluation et d'indemnisation en cas de pertes subies par les contractants faute d'avoir pu accéder à ces informations classées.

Article 9. Visites

1. Les visites effectuées par des ressortissants d'une Partie chez l'autre Partie, nécessitant un accès à des informations classées, sont subordonnées à l'autorisation écrite préalable de l'autorité nationale de sécurité/autorité de sécurité désignée de la Partie d'accueil.

2. Toutes les demandes de visite sont présentées à l'autorité nationale de sécurité/autorité de sécurité désignée au moins vingt (20) jours avant la date de la visite. En cas d'urgence, une demande peut être présentée au moins cinq (5) jours ouvrables avant la date de la visite.

3. Chaque Partie autorise des visiteurs de l'autre Partie à effectuer des visites nécessitant un accès à des informations classées uniquement si ceux-ci :

a) Ont reçu l'habilitation personnelle de sécurité correspondante de la part de l'autorité nationale de sécurité de la Partie qui les envoie; et

b) Sont habilités à recevoir des informations classées ou à y accéder conformément aux lois et réglementations nationales de leur Partie.

4. La demande de visite doit contenir les informations suivantes :

a) Nom, date et lieu de naissance, et numéro du passeport (ou de la carte d'identité) du visiteur;

b) Nationalité du visiteur;

c) Fonction du visiteur et personne morale qu'il représente;

d) Certificat d'habilitation personnelle, cote de sécurité et durée de validité de l'habilitation du visiteur;

e) Objet, programme de travail et date de la visite;

f) Nom des organisations et installations que le visiteur souhaite voir;

g) Nom et numéro de téléphone du point de contact de l'établissement ou de toute autre installation faisant l'objet de la visite, contacts précédents et tout autre renseignement justifiant la visite ou les visites;

h) Date, signature et cachet officiel de l'autorité nationale de sécurité/autorité de sécurité désignée correspondante.

5. Chacune des Parties veille à ce que les données personnelles des visiteurs soient protégées, conformément à ses lois et réglementations nationales et à celles de l'autre Partie.

6. L'autorisation de visite délivrée reste valable pendant un an maximum.

7. Les Parties peuvent convenir, pour tout projet, programme ou contrat, de dresser des listes de personnes autorisées à effectuer des visites périodiques. Une fois les listes approuvées par les Parties, les modalités de chaque visite sont définies directement avec le responsable de la sécurité des organisations que les personnes concernées visitent, selon les modalités et les conditions convenues.

Article 10.Infractions à la sécurité

1. Lorsque se produit une infraction à la sécurité entraînant ou susceptible d'entraîner la perte ou la divulgation des informations classées échangées entre les Parties, l'autorité nationale de sécurité responsable là où l'infraction à la sécurité s'est produite informe dès que possible l'autorité nationale de sécurité de l'autre Partie, et veille à ce qu'une enquête appropriée soit diligentée. L'autre Partie coopère à l'enquête, si besoin est.

2. Cette autre Partie est tenue informée des résultats de l'enquête et reçoit un rapport final sur l'infraction à la sécurité.

Article 11. Dépenses

Chaque Partie prend en charge les dépenses qu'elle engage aux fins de l'application du présent Accord.

Article 12. Règlement des différends

Tout différend concernant l'interprétation ou l'application du présent Accord est réglé par voie de consultations entre les Parties, sans recours à une juridiction, qu'elle soit nationale ou internationale, ni à une tierce partie.

Article 13. Dispositions finales

1. Le présent Accord est conclu pour une durée indéterminée et entre en vigueur à la date de réception de la dernière notification échangée entre les Parties attestant que les formalités légales internes requises pour son entrée en vigueur ont été accomplies.

2. Le présent Accord peut être modifié par écrit d'un commun accord par les deux Parties. Les modifications entrent en vigueur conformément au paragraphe 1 du présent article.

3. Chacune des Parties peut dénoncer le présent Accord par notification écrite adressée à l'autre Partie. La dénonciation prend effet six mois après la date à laquelle l'autre Partie a reçu la notification écrite, mais n'a pas d'incidence sur les obligations contractées en vertu des dispositions du présent Accord. En particulier, toutes les

informations classées échangées ou produites en vertu du présent Accord restent protégées, conformément aux dispositions dudit Accord.

FAIT à Madrid, le 7 mai 2010, en deux exemplaires originaux, en espagnol et lituanien, les deux textes faisant également foi.

Pour le Royaume d'Espagne :

FÉLIX SANZ ROLDÁN

Secrétaire d'État, Directeur du Centre national de renseignement

Pour la République de Lituanie :

ROMUALDAS VAIŠNORAS

Directeur général adjoint du Département de sécurité de l'État