994

UMOWA

między Rzecząpospolitą Polską a Królestwem Hiszpanii o wzajemnej ochronie informacji niejawnych,

podpisana w Madrycie dnia 18 kwietnia 2006 r. oraz w Warszawie dnia 24 maja 2006 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

W dniu 18 kwietnia 2006 r. w Madrycie oraz w dniu 24 maja 2006 r. w Warszawie została podpisana Umowa między Rzecząpospolitą Polską a Królestwem Hiszpanii o wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA

między Rzecząpospolitą Polską

a Królestwem Hiszpanii

o wzajemnej ochronie informacji niejawnych

Rzeczpospolita Polska i Królestwo Hiszpanii, zwane dalej „Stronami",

mając świadomość zmian w sytuacji politycznej na świecie i uznając ważną rolę swej wzajemnej współpracy dla celów stabilizacji pokoju, międzynarodowego bezpieczeństwa i wzajemnej poufności, będąc świadomymi faktu, iż dobra współpraca może wymagać wymiany informacji niejawnych pomiędzy Stronami,

pragnąc stworzyć system przepisów regulujących wzajemną ochronę informacji niejawnych wymienianych pomiędzy Stronami, dla celów jakiejkolwiek przyszłej umowy o współpracy albo kontraktu niejawnego,

uzgodniły, co następuje:

Artykuł 1

Definicje

W rozumieniu niniejszej Umowy:

a) „informacja niejawna" - oznacza wszelką informację (konkretnie: wiedzę, która może być przekazana w jakiejkolwiek formie) lub materiał, wymagające ochrony przed nieuprawnionym ujawnieniem, które zostały jako takie oznaczone klauzulą tajności;

b) „materiał niejawny" - oznacza dowolny przedmiot, wyposażenie, urządzenie lub broń, wyprodukowane lub będące w trakcie produkcji, jak również komponenty użyte do ich produkcji, zawierające informacje niejawne;

c) „dokument niejawny" - oznacza jakąkolwiek formę utrwalenia informacji niejawnej niezależnie od jej fizycznej formy lub cech charakterystycznych;

d) „kontrahent" – oznacza osobę fizyczną lub osobę prawną posiadającą zdolność prawną do zawierania kontraktów;

e) „podmiot zamawiający" - oznacza podmiot, który zamierza zawrzeć kontrakt niejawny na terytorium Państwa drugiej Strony;

f) „kontrakt niejawny" - oznacza kontrakt pomiędzy dwoma lub więcej kontrahentami, tworzący i określający wykonalne prawa i obowiązki pomiędzy nimi, który zawiera lub wiąże się z wytwarzaniem lub dostępem do informacji niejawnych;

g) „właściwe organy bezpieczeństwa" - oznaczają organy wyznaczone przez Stronę, jako odpowiedzialne za wdrażanie i nadzorowanie niniejszej Umowy;

h) „strona otrzymująca" – oznacza Stronę, do której informacja niejawna jest przekazywana;

i) „strona wytwarzająca" - oznacza Stronę, która wytwarza informacje niejawne;

j) „trzecia strona" – oznacza każdą międzynarodową organizację lub państwo, które nie jest stroną niniejszej Umowy;

k) „poświadczenie bezpieczeństwa" - oznacza stwierdzenie przez właściwe organy bezpieczeństwa lub inny podmiot uprawniony zgodnie z prawem wewnętrznym Strony, że osoba fizyczna jest uprawniona do dostępu do informacji niejawnych;

l) „świadectwo bezpieczeństwa przemysłowego" - oznacza stwierdzenie przez właściwe organy bezpieczeństwa lub inny podmiot uprawniony zgodnie z prawem wewnętrznym Strony, że pod względem bezpieczeństwa przedsiębiorca posiada fizyczną i organizacyjną zdolność, aby wykorzystywać i przechowywać informacje niejawne, zgodnie z prawem i regulacjami wewnętrznymi;

m) „zasada ograniczonego dostępu" – oznacza, że dostęp do informacji niejawnych może być przyznany tylko osobom, które posiadają zweryfikowany wymóg zapoznania się lub posiadania takich informacji w celu wykonywania swych obowiązków służbowych i zawodowych.

Artykuł 2

Klauzule tajności

1. Strony uzgadniają, że poniższe klauzule tajności są równorzędne i odpowiadają klauzulom tajności określonym w prawie wewnętrznym odpowiedniej Strony:

Rzeczpospolita Polska	**Królestwo Hiszpanii**	**Odpowiednik w języku angielskim**
ŚCIŚLE TAJNE	SECRETO	TOP SECRET
TAJNE	RESERVADO	SECRET
POUFNE	CONFIDENCIAL	CONFIDENTIAL
ZASTRZEŻONE	DIFUSIÓN LIMITADA	RESTRICTED

2. Strona otrzymująca nie będzie obniżała ani znosiła klauzuli tajności otrzymanych informacji niejawnych bez uprzedniej pisemnej zgody strony wytwarzającej. Strona wytwarzająca poinformuje stronę otrzymującą o wszelkich zmianach w klauzulach tajności przekazanych informacji.
3. Obowiązek, o którym mowa w ustępie 2, będzie się również odnosił do informacji niejawnych wytworzonych w wyniku wspólnej działalności Stron, w tym także do informacji wytworzonych w związku z realizacją kontraktu niejawnego.
4. Strona otrzymująca oznacza otrzymane informacje własną, równorzędną klauzulą tajności.

Artykuł 3

Właściwe organy bezpieczeństwa

1. Właściwymi organami bezpieczeństwa odpowiedzialnymi za wdrożenie i nadzorowanie wszelkich aspektów związanych z niniejszą Umową są:
   a) w Rzeczypospolitej Polskiej:
      Szef Agencji Bezpieczeństwa Wewnętrznego
      ul. Rakowiecka 2A
      00-993 Warszawa
      POLSKA
      Szef Wojskowych Służb Informacyjnych
      00-909 Warszawa 60
      POLSKA
   b) w Królestwie Hiszpanii:
      Sekretarz Stanu, Dyrektor Krajowego Centrum Wywiadu
      Biuro Bezpieczeństwa Narodowego
      Avda. Padre Huidobro, s/n
      28023 Madryt
      HISZPANIA

2. W celu osiągnięcia i utrzymania porównywalnych standardów bezpieczeństwa, odpowiednie właściwe organy bezpieczeństwa będą, na wniosek, przekazywać sobie wzajemnie informacje o swoich standardach bezpieczeństwa, procedurach i praktykach ochrony informacji niejawnych.
3. Właściwe organy bezpieczeństwa mogą zawierać porozumienia wykonawcze w celu realizacji postanowień niniejszej Umowy.

Artykuł 4

Ochrona, która ma zapewnić bezpieczeństwo informacji niejawnych

1. Zgodnie z niniejszą Umową oraz prawem i regulacjami wewnętrznymi, Strony zastosują odpowiednie środki do ochrony informacji niejawnych, przekazanych na podstawie niniejszej Umowy lub wytworzonych albo opracowanych w związku z kontraktem niejawnym lub w wyniku wszelkich stosunków pomiędzy Stronami.
2. Strony przyznają wszystkim przekazanym, wytworzonym lub opracowanym informacjom niejawnym ten sam stopień ochrony, jaki zapewniają własnym informacjom niejawnym o równorzędnej klauzuli tajności, jak zostało to określone w artykule 2 niniejszej Umowy.
3. Na wniosek, właściwe organy bezpieczeństwa Stron, uwzględniając prawo i regulacje wewnętrzne, będą wzajemnie pomagać sobie przy przeprowadzaniu procedur sprawdzeniowych w stosunku do swych obywateli lub przedsiębiorców, zamieszkałych lub posiadających siedzibę na terytorium drugiej Strony, poprzedzających wydanie poświadczenia bezpieczeństwa albo świadectwa bezpieczeństwa przemysłowego.
4. Strony uznają poświadczenia bezpieczeństwa oraz świadectwa bezpieczeństwa przemysłowego wydane zgodnie z prawem i regulacjami wewnętrznymi drugiej Strony. Równorzędność poświadczeń i świadectw jest zgodna z artykułem 2 niniejszej Umowy.

5. Właściwe organy bezpieczeństwa przekażą sobie informacje o zmianach dotyczących wydanych poświadczeń bezpieczeństwa i świadectw bezpieczeństwa przemysłowego.

Artykuł 5

Wykorzystanie i udostępnianie informacji niejawnych

1. Informacje niejawne przekazane przez jedną Stronę drugiej Stronie będą wykorzystywane jedynie do konkretnych celów, dla jakich zostały przekazane.
2. Strony nie będą udostępniały, ujawniały lub dopuszczały do udostępnienia lub ujawnienia informacji niejawnych otrzymanych na podstawie niniejszej Umowy stronom trzecim lub ich obywatelom, publicznym lub prywatnym podmiotom, bez wcześniejszej pisemnej zgody strony wytwarzającej.
3. Niniejsza Umowa nie może być stosowana przez żadną ze Stron do uzyskiwania informacji niejawnych, które druga Strona otrzymała od strony trzeciej.
4. Dostęp do informacji niejawnych i szczególnych obszarów, gdzie są wykonywane działania związane z dostępem do informacji niejawnych lub przechowywane są informacje niejawne, będzie ograniczony jedynie do osób, którym wydano odpowiednie poświadczenie bezpieczeństwa, które zostały przeszkolone i spełniają zasadę ograniczonego dostępu.

Artykuł 6

Tłumaczenie, powielanie i niszczenie

1. Informacje niejawne oznaczone klauzulą ŚCIŚLE TAJNE/SECRETO/TOP SECRET są tłumaczone lub kopiowane wyłącznie na podstawie

pisemnego zezwolenia właściwego organu bezpieczeństwa strony wytwarzającej.

2. Tłumaczenia i kopie informacji niejawnych będą wykonywane przez osoby posiadające odpowiednie poświadczenie bezpieczeństwa. Będą one oznaczone i chronione w ten sam sposób, co oryginalne informacje. Tłumaczenie i liczba kopii będzie ograniczona do wymaganej dla celów służbowych.
3. Tłumaczenia będą nosiły odpowiednią adnotację w języku, na który zostały przetłumaczone, informującą, że zawierają informacje niejawne otrzymane od strony wytwarzającej.
4. Informacje i materiały oznaczone klauzulą ŚCIŚLE TAJNE/SECRETO/TOP SECRET nie będą niszczone. Będą one zwracane właściwym organom bezpieczeństwa strony wytwarzającej. Pozostałe informacje niejawne będą niszczone zgodnie z prawem i regulacjami wewnętrznymi w taki sposób, aby uniemożliwić ich częściową lub całkowitą rekonstrukcję. Aby zniszczyć informacje, którym przyznano klauzulę TAJNE/RESERVADO/SECRET, niezbędna jest wcześniejsza pisemna zgoda strony wytwarzającej.

Artykuł 7

Wizyty

1. Wizyty obywateli jednej Strony u drugiej Strony, łączące się z dostępem do informacji niejawnych, są uzależnione od uzyskania uprzedniego pisemnego zezwolenia, udzielonego przez właściwy organ bezpieczeństwa Strony przyjmującej.
2. Wizyty obywateli strony trzeciej, łączące się z dostępem do informacji niejawnych, będą jedynie możliwe za pisemną zgodą strony wytwarzającej.

3. Właściwy organ bezpieczeństwa Strony wysyłającej powinien poinformować właściwy organ bezpieczeństwa Strony przyjmującej o spodziewanym przybyciu osób z wizytą, zgodnie z procedurami określonymi w ustępach 4-11 niniejszego artykułu. Procedury te mogą zostać zmienione na podstawie pisemnej zgody właściwych organów bezpieczeństwa obu Stron.
4. Wizyty łączące się z dostępem do informacji niejawnych będą dozwolone przez jedną Stronę osobom przybywającym od drugiej Strony tylko, jeżeli:
   a) osobom tym zostało wydane odpowiednie poświadczenie bezpieczeństwa przez właściwy organ bezpieczeństwa lub inny odpowiedni organ Strony wysyłającej;
   b) osoby te będą upoważnione do uzyskiwania lub dostępu do informacji niejawnych zgodnie z prawem i regulacjami wewnętrznymi swojej Strony.
5. Właściwy organ bezpieczeństwa Strony wysyłającej poinformuje właściwy organ bezpieczeństwa Strony przyjmującej o planowanej wizycie w drodze wniosku o wizytę, który powinien zostać otrzymany z wyprzedzeniem co najmniej dwudziestu pięciu (25) dni roboczych przed terminem wizyty lub pierwszej z wizyt powtarzających się.
6. W nagłych przypadkach wniosek o wizytę może być otrzymany z wyprzedzeniem co najmniej pięciu (5) dni roboczych.
7. Wniosek o wizytę zawiera:
   a) imię i nazwisko osoby przybywającej z wizytą, miejsce i datę urodzenia, obywatelstwo, numer paszportu lub dowodu osobistego;
   b) nazwę przedsiębiorstwa, spółki lub organizacji, którą reprezentuje lub do której przynależy;
   c) nazwę i adres przedsiębiorstwa, spółki lub organizacji, która będzie odwiedzana;

d) potwierdzenie poświadczenia bezpieczeństwa osoby odwiedzającej i jego ważności;

e) przedmiot i cel wizyty lub wizyt;

f) spodziewaną datę i czas trwania wizyty lub wizyt, o które wnioskowano. W przypadku powtarzających się wizyt powinien zostać określony całkowity czas trwania wizyt;

g) nazwę i numer telefonu punktu kontaktowego w przedsiębiorstwie/jednostce organizacyjnej, która będzie odwiedzana, wcześniejsze kontakty i wszelkie informacje użyteczne do uzasadnienia wizyty lub wizyt.

8. Ważność upoważnienia do wizyty, w przypadku wizyt powtarzających się, nie powinna przekraczać dwunastu (12) miesięcy.

9. Właściwy organ bezpieczeństwa Strony przyjmującej poinformuje pełnomocników do spraw ochrony informacji niejawnych przedsiębiorstwa, jednostki organizacyjnej lub organizacji, która będzie odwiedzana, o danych osób wyznaczonych do wizyty.

10. Informacje niejawne dostępne w czasie wizyty będą chronione zgodnie z postanowieniami niniejszej Umowy.

11. Każda Strona zagwarantuje ochronę danych osobowych osób przybywających z wizytą, zgodnie z odpowiednim prawem i regulacjami wewnętrznymi.

Artykuł 8

Kontrakty niejawne

1. Zamawiający podmiot, chcąc zawrzeć kontrakt niejawny z kontrahentem, który posiada siedzibę na terytorium drugiej Strony, powinien uzyskać, za pośrednictwem właściwego organu bezpieczeństwa, uprzednie pisemne

zapewnienie od właściwego organu bezpieczeństwa drugiej Strony, że zaproponowany kontrahent posiada świadectwo bezpieczeństwa przemysłowego, dopuszczającego do dostępu do informacji niejawnych o odpowiedniej klauzuli tajności.

2. Jeżeli kontrahent nie uzyskał wcześniej świadectwa bezpieczeństwa przemysłowego umożliwiającego dostęp do informacji niejawnych o odpowiedniej klauzuli tajności, właściwy organ bezpieczeństwa, który ma wydać zapewnienie, powinien niezwłocznie poinformować właściwy organ bezpieczeństwa drugiej Strony, że na jego wniosek zostaną podjęte działania zmierzające do wydania odpowiedniego świadectwa bezpieczeństwa przemysłowego.
3. Każdy niejawny kontrakt, zawarty zgodnie z postanowieniami niniejszej Umowy, zawiera odpowiednią instrukcję bezpieczeństwa przemysłowego. Właściwe organy bezpieczeństwa mogą uzgodnić szczegóły takiej instrukcji, która zawierać będzie przewodnik klasyfikacyjny.
4. Właściwy organ bezpieczeństwa Strony, na terytorium której kontrakt niejawny będzie realizowany, zapewni, że kontrahent będzie chronił informacje niejawne przekazane przez podmiot zamawiający, zgodnie z postanowieniami niniejszej Umowy.
5. Każdy podwykonawca musi spełniać te same obowiązki dotyczące bezpieczeństwa co kontrahent.
6. Kopia instrukcji bezpieczeństwa przemysłowego każdego niejawnego kontraktu będzie przesłana właściwemu organowi bezpieczeństwa tej Strony, na terytorium której praca będzie wykonywana, aby umożliwić odpowiedni nadzór nad procedurami bezpieczeństwa.
7. Przedstawiciele właściwych organów bezpieczeństwa mogą odwiedzać się wzajemnie w celu przeanalizowania skuteczności środków przyjętych przez kontrahenta do ochrony informacji niejawnych związanych z kontraktem niejawnym.

Artykuł 9

Przekazywanie informacji niejawnych

1. Informacje niejawne przekazywane są pomiędzy Stronami w drodze dyplomatycznej.
2. Jeżeli korzystanie z drogi dyplomatycznej byłoby niepraktyczne lub nadmiernie opóźniałoby odbiór informacji niejawnych, przekazywanie może być dokonywane przez odpowiednio upoważniony do dostępu do informacji niejawnych personel, wyposażony w certyfikat kurierski wydany przez Stronę, która przekazuje informacje niejawne.
3. Strony mogą przekazywać informacje niejawne za pomocą środków elektronicznych, zgodnie z procedurami bezpieczeństwa zatwierdzonymi wspólnie poprzez właściwe organy bezpieczeństwa obydwu Stron.
4. Dostawa dużych przedmiotów lub ilości materiałów niejawnych, uzgodniona na podstawie indywidualnych przypadków, zostanie zatwierdzona przez właściwe organy bezpieczeństwa obu Stron.
5. Inne środki przekazywania informacji niejawnych mogą być użyte, jeżeli zostały zatwierdzone przez właściwe organy bezpieczeństwa obydwu Stron.

Artykuł 10

Naruszenie regulacji dotyczących wzajemnej ochrony informacji niejawnych

1. W przypadku naruszenia regulacji dotyczących wzajemnej ochrony informacji niejawnych, które ma skutek w postaci rzeczywistego lub podejrzewanego ujawnienia informacji niejawnych wytworzonych przez lub otrzymanych od drugiej Strony lub podejrzenia, że informacje niejawne zostały ujawnione nieuprawnionej osobie, właściwy organ

bezpieczeństwa Strony, na terytorium której naruszenie regulacji dotyczących wzajemnej ochrony informacji niejawnych miało miejsce, poinformuje właściwy organ bezpieczeństwa drugiej Strony tak szybko, jak będzie to możliwe i przeprowadzi odpowiednie dochodzenie. Druga Strona, o ile okaże się to konieczne, będzie współpracować w dochodzeniu.

2. W przypadku gdy do ujawnienia doszło na terytorium państwa innego niż Strony, właściwy organ bezpieczeństwa przekazującej Strony podejmie działania opisane w ustępie 1.
3. W każdym przypadku druga Strona będzie informowana o rezultatach dochodzenia i uzyska raport końcowy o przyczynie i rozmiarze szkód.

Artykuł 11

Koszty

Każda Strona będzie ponosiła własne koszty powstałe w związku z wdrażaniem i nadzorowaniem wszelkich aspektów niniejszej Umowy.

Artykuł 12

Konsultacje

1. Właściwe organy bezpieczeństwa Stron powiadomią się wzajemnie o wszelkich zmianach w prawie i regulacjach wewnętrznych dotyczących ochrony informacji niejawnych.
2. Właściwe organy bezpieczeństwa Stron będą się wzajemnie konsultować, na wniosek jednego z nich, w celu zapewnienia ścisłej współpracy przy wdrażaniu postanowień niniejszej Umowy.

3. Każda ze Stron zezwoli przedstawicielom właściwego organu bezpieczeństwa drugiej Strony na składanie wizyt na swoim terytorium w celu przedyskutowania procedur dotyczących ochrony informacji niejawnych przekazanych przez drugą Stronę.

Artykuł 13

Rozstrzyganie sporów

Wszelkie spory dotyczące interpretacji lub zastosowania niniejszej Umowy będą rozwiązywane w drodze konsultacji pomiędzy właściwymi organami bezpieczeństwa Stron lub, w przypadku gdy rozwiązanie sporu w ten sposób nie będzie możliwe, drogą dyplomatyczną.

Artykuł 14

Postanowienia końcowe

1. Niniejsza Umowa podlega przyjęciu zgodnie z prawem wewnętrznym każdej ze Stron, co zostanie stwierdzone w drodze wymiany not. Umowa wejdzie w życie w pierwszym dniu drugiego miesiąca następującego po dniu otrzymania późniejszej z not.
2. Umowa niniejsza zawarta jest na czas nieokreślony. Może być ona wypowiedziana przez każdą ze Stron w drodze pisemnej notyfikacji. W takim przypadku, niniejsza Umowa utraci moc po upływie sześciu miesięcy od dnia otrzymania noty informującej o wypowiedzeniu.
3. W przypadku wypowiedzenia, wszelkie informacje niejawne przekazane lub powstałe w wyniku wspólnej działalności Stron, w tym także w związku z realizacją kontraktu niejawnego, będą nadal chronione zgodnie

z postanowieniami niniejszej Umowy tak długo, jak wymaga tego obowiązywanie klauzuli tajności.

4. Niniejsza Umowa może zostać zmieniona na podstawie wzajemnej pisemnej zgody obu Stron. Takie zmiany wejdą w życie zgodnie z postanowieniami ustępu 1 niniejszego artykułu.

Sporządzono w dwóch oryginalnych egzemplarzach, każdy w językach polskim, hiszpańskim i angielskim. W przypadku rozbieżności w interpretacji, tekst angielski będzie tekstem rozstrzygającym.

W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

ZBIGNIEW WASSERMANN
Minister
Członek Rady Ministrów

Data: 24.05.2006 r.

Miejsce: Warszawa

W IMIENIU KRÓLESTWA HISZPANII

ALBERTO SAIZ CORTÉS
Sekretarz Stanu
Dyrektor Narodowego Centrum Wywiadu

Data: 18.04.2006

Miejsce: Madrid

ACUERDO

entre

LA REPÚBLICA DE POLONIA

y

EL REINO DE ESPAÑA

para la Protección Mutua y el Intercambio de Información Clasificada

La República de Polonia y El Reino de España,

en adelante denominados las "Partes".

Siendo conscientes de los cambios en la situación política mundial

y reconociendo el importante papel de su mutua cooperación

para la estabilización de la paz, la seguridad internacional y la confianza mutua.

Comprendiendo que una buena cooperación puede requerir el intercambio

de información clasificada entre las Partes.

Deseando crear un conjunto de normas para la protección mutua

de información clasificada intercambiada entre las Partes en virtud de cualquier

futuro acuerdo de cooperación o contrato clasificado.

Han acordado lo siguiente:

ARTÍCULO 1

DEFINICIONES

A los efectos del presente Acuerdo:

(1) Por **"Información Clasificada"** se entenderá cualquier información (a saber, conocimiento que pueda ser comunicado de cualquier forma) o "material", respecto de los cuales se decida que requieren protección contra su divulgación no autorizada y a los que se haya asignado un nivel de clasificación de seguridad.

(2) Por **"Material Clasificado"** se entenderá cualquier artículo técnico, equipo, dispositivo o arma, fabricado o en proceso de fabricación, así como los componentes usados para su fabricación, que contengan Información Clasificada.

(3) Por **"Documento Clasificado"** se entenderá cualquier forma de Información Clasificada registrada, independientemente de su forma o características físicas.

(4) Por **"Contratista"** se entenderá una persona física o jurídica que posea la capacidad jurídica para concluir contratos.

(5) Por **"Entidad Contratante"** se entenderá cualquier entidad que pretenda concluir un Contrato Clasificado en el territorio de la otra Parte.

(6) Por **"Contrato Clasificado"** se entenderá un contrato entre dos o más Contratistas que cree y defina derechos y obligaciones exigibles entre ellos y que contenga o implique la generación de Información Clasificada o el acceso a la misma.

(7) Por **"Autoridad de Seguridad Competente"** se entenderá la autoridad designada por una Parte como responsable de la aplicación y supervisión de este Acuerdo.

(8) Por **"Parte Receptora"** se entenderá la Parte a la que se transmita Información

Clasificada.

(9) Por **"Parte Originadora"** se entenderá la Parte que cree Información Clasificada.

(10) Por **"Tercera Parte"** se entenderá cualquier organización internacional o Estado que no sea Parte en este Acuerdo.

(11) Por **"Habilitación Personal de Seguridad"** se entenderá la determinación por las Autoridades de Seguridad Competentes u otra entidad autorizada según el derecho nacional de una Parte, de que una persona reúne los requisitos necesarios para tener acceso a Información Clasificada.

(12) Por **"Habilitación de Seguridad del Establecimiento"** se entenderá la determinación por las Autoridades de Seguridad Competentes u otra entidad autorizada según el derecho nacional de una Parte, de que, desde un punto de vista de seguridad, una instalación tiene capacidad física y organizativa para utilizar y guardar Información Clasificada, conforme a las leyes y reglamentos nacionales.

(13) Por **"Principio de Necesidad de Conocer"** se entenderá que el acceso a la Información Clasificada sólo puede concederse a personas que tengan una necesidad comprobada de conocer o poseer tal información para desempeñar sus obligaciones oficiales y profesionales.

ARTÍCULO 2

CLASIFICACIONES DE SEGURIDAD

(1) Las Partes acuerdan que los siguientes niveles de clasificación de seguridad son equivalentes y corresponden a los niveles de clasificación de seguridad especificados en las leyes y reglamentos nacionales de cada Parte:

EN LA REPÚBLICA DE POLONIA	EN EL REINO DE ESPAÑA	EQUIVALENTE EN INGLÉS
ŚCIŚLE TAJNE	SECRETO	TOP SECRET
TAJNE	RESERVADO	SECRET
POUFNE	CONFIDENCIAL	CONFIDENTIAL
ZASTRZEŻONE	DIFUSIÓN LIMITADA	RESTRICTED

(2) La Parte Receptora no podrá reducir el nivel ni desclasificar la Información Clasificada recibida sin el previo consentimiento por escrito de la Parte Originadora. La Parte Originadora informará a la Parte Receptora de cualquier cambio en los niveles de clasificación de seguridad de la información transmitida.

(3) La obligación mencionada en el apartado 2 también se aplicará a la Información Clasificada generada como resultado de la mutua cooperación entre las Partes, incluida la originada en relación a la ejecución de un Contrato Clasificado.

(4) La Parte Receptora marcará la Información Clasificada recibida con su propia clasificación de seguridad equivalente.

ARTÍCULO 3

AUTORIDADES DE SEGURIDAD COMPETENTES

(1) Las Autoridades de Seguridad Competentes responsables de la aplicación y supervisión de todos los aspectos del presente Acuerdo son:

En la República de Polonia:

Jefe de la Agencia de Seguridad Interior

ul. Rakowiecka 2ª

00-993 Varsovia

POLONIA

Jefe de los Servicios de Información Militares
00-909 Varsovia 60
POLONIA

En el Reino de España:

Secretario de Estado, Director del Centro Nacional de Inteligencia
Oficina Nacional de Seguridad
Avda. Padre Huidobro, s/n
28023 Madrid
ESPAÑA

(2) Para conseguir y mantener normas de seguridad comparables, las respectivas Autoridades de Seguridad Competentes se proporcionarán recíprocamente, previa petición, información sobre sus normas, procedimientos y prácticas de seguridad para la protección de Información Clasificada.

(3) Las Autoridades de Seguridad Competentes podrán concluir acuerdos ejecutivos para la aplicación de las estipulaciones del presente documento.

ARTÍCULO 4

PROTECCIÓN DE SEGURIDAD

(1) De conformidad con el presente Acuerdo y con sus leyes y reglamentos nacionales, las Partes aplicarán las medidas apropiadas para proteger la Información Clasificada que se intercambie en virtud del presente Acuerdo o que se produzca o desarrolle en conexión con un Contrato Clasificado o cualquier relación entre las Partes.

(2) Las Partes concederán a toda la Información Clasificada transmitida, producida o desarrollada, el mismo grado de protección de seguridad que se proporciona a su propia Información Clasificada de nivel equivalente, tal y como se define en el artículo 2 del presente Acuerdo.

(3) Previa petición, las Autoridades de Seguridad Competentes de las Partes,

teniendo en cuenta sus leyes y reglamentos nacionales, se asistirán entre sí. durante los procedimientos de investigación de sus ciudadanos que residan en el territorio

de la otra Parte o de las instalaciones que estén ubicadas en el territorio de la otra Parte, procedimientos que precederán a la expedición de la Habilitación Personal de Seguridad y de la Habilitación de Seguridad del Establecimiento.

(4) Las Partes reconocerán la validez de las Habilitaciones de Seguridad Personal y del Establecimiento emitidas conforme a las leyes y reglamentos nacionales de la otra Parte. La equivalencia de las habilitaciones de seguridad se ajustará al artículo 2 del presente Acuerdo.

(5) Las Autoridades de Seguridad Competentes se comunicarán entre sí cualquier información relativa a cambios relativos a las Habilitaciones de Seguridad Personal y del Establecimiento emitidas.

ARTÍCULO 5

USO Y DIVULGACIÓN DE INFORMACIÓN CLASIFICADA

(1) La Información Clasificada transmitida por una Parte a la otra Parte se usará sólo para el fin específico para el que fue proporcionada.

(2) Las Partes no cederán, divulgarán ni permitirán la cesión o divulgación de Información Clasificada recibida en virtud del presente Acuerdo a Terceras Partes, o a sus ciudadanos o entidades públicas o privadas, sin el previo consentimiento por escrito de la Parte Originadora.

(3) Ninguna de las Partes podrá acogerse al presente Acuerdo para obtener Información Clasificada que la otra Parte haya recibido de una Tercera Parte.

(4) El acceso a Información Clasificada y a zonas específicas donde se desempeñan actividades clasificadas o donde se almacena Información Clasificada se limitará sólo a aquellas personas a las que se haya concedido Habilitación Personal de Seguridad y que respondan al "Principio de Necesidad de Conocer".

ARTÍCULO 6

TRADUCCIÓN, REPRODUCCIÓN Y DESTRUCCIÓN DE INFORMACIÓN CLASIFICADA

(1) La Información Clasificada marcada como ŚCIŚLE TAJNE/SECRETO/TOP SECRET se traducirá o reproducirá sólo con el previo consentimiento por escrito de la Autoridad de Seguridad Competente de la Parte Originadora.

(2) Las traducciones y reproducciones de Información Clasificada serán realizadas por personas que tengan la Habilitación Personal de Seguridad apropiada. Se marcarán y se someterán a la misma protección que la información original. La traducción y el número de copias se limitará al requerido para fines oficiales.

(3) Las traducciones llevarán una nota adecuada en el idioma al que se traducen indicando que contienen Información Clasificada recibida de la Parte Originadora.

(4) La información y el material ŚCIŚLE TAJNE/SECRETO/TOP SECRET no se destruirán. Se devolverán a la Autoridad de Seguridad Competente de la Parte Originadora. La Información Clasificada restante se destruirá de acuerdo con las leyes y reglamentos nacionales de tal manera que se evite su reconstrucción total o parcial. Para la destrucción de información clasificada TAJNE/RESERVADO/SECRET, se requiere previo consentimiento por escrito de la Parte Originadora.

ARTÍCULO 7

VISITAS

(1) Las visitas que supongan el acceso a Información Clasificada por ciudadanos de una Parte a la otra Parte estarán sujetas a previa autorización por escrito de la Autoridad de Seguridad Competente de la Parte anfitriona.

(2) Las visitas que supongan el acceso a Información Clasificada por un ciudadano

de una Tercera Parte sólo se autorizarán con el consentimiento por escrito de la Parte Originadora.

(3) La Autoridad de Seguridad Competente de la Parte remitente notificará a la Autoridad de Seguridad Competente de la Parte anfitriona los visitantes esperados conforme a los procedimientos definidos en los apartados 4 a 11 de este Artículo. Estos procedimientos podrán cambiarse de mutuo acuerdo por escrito de ambas Autoridades Competentes de Seguridad.

(4) Cada Parte permitirá las visitas que conlleven el acceso a Información Clasificada a los visitantes de la otra Parte sólo si:

a) Se les ha concedido Habilitación Personal de Seguridad apropiada por la Autoridad de Seguridad Competente u otra autoridad pertinente de la Parte remitente.

b) Han sido autorizados para recibir o tener acceso a Información Clasificada conforme a las leyes y reglamentos nacionales de su Parte.

(5) La Autoridad de Seguridad Competente de la Parte remitente notificará a la Autoridad de Seguridad Competente de la Parte anfitriona la visita prevista mediante una solicitud de visita, la cual deberá ser recibida al menos veinticinco (25) días laborables antes de que la visita o la primera de las visitas recurrentes tengan lugar.

(6) En casos urgentes, la solicitud de visita podrá ser recibida con al menos cinco (5) días laborables de antelación.

(7) La solicitud de visita incluirá:

a) Nombre y apellidos del visitante, lugar y fecha de nacimiento, nacionalidad y número de pasaporte o tarjeta de identidad.

b) Nombre del establecimiento empresa u organización a la que representa o a la que pertenece.

c) Nombre y dirección del establecimiento, empresa u organización que se vaya a visitar.

d) Certificación de la Habilitación Personal de Seguridad del visitante

y su vigencia.

e) Objeto y finalidad de la visita o visitas.

f) Fecha y duración previstas de la visita o visitas solicitadas. En el caso de visitas recurrentes deberá indicarse el período total cubierto por las mismas.

g) Nombre y número de teléfono del punto de contacto en el establecimiento/instalación que se vaya a visitar, contactos previos y cualquier otra información útil para determinar la justificación de la visita o visitas.

(8) La validez de la autorización para la visita en caso de visitas recurrentes no excederá de doce (12) meses.

(9) La Autoridad de Seguridad Competente de la Parte anfitriona informará a los oficiales de seguridad del establecimiento, instalación u organización que se vaya a visitar de los datos de aquellas personas a las que se ha autorizado la visita.

(10) La Información Clasificada a la que se acceda durante la visita deberá ser protegida conforme a lo establecido en el presente Acuerdo.

(11) Cada una de las Partes garantizará la protección de los datos personales de los visitantes de conformidad con sus respectivas leyes y reglamentos nacionales.

ARTÍCULO 8

CONTRATOS CLASIFICADOS

(1) Una Entidad Contratante que desee concluir un Contrato Clasificado con un Contratista establecido en el territorio de la otra Parte deberá obtener a través de su Autoridad de Seguridad Competente previa garantía por escrito de la Autoridad de Seguridad Competente de la otra Parte de que el Contratista propuesto tiene una Habilitación de Seguridad del Establecimiento de nivel apropiado.

(2) Si al Contratista no le ha sido previamente concedida una Habilitación de Seguridad del Establecimiento del nivel de clasificación de seguridad especificado, la Autoridad de Seguridad Competente que deba recibir la garantía notificará inmediatamente a la Autoridad de Seguridad Competente de la otra Parte que, a la recepción de la solicitud, tomará las medidas necesarias para la concesión de la Habilitación de Seguridad del Establecimiento apropiada.

(3) Cada Contrato Clasificado concluido con arreglo a las disposiciones del presente Acuerdo deberá incluir una sección de seguridad adecuada. Las Autoridades de Seguridad Competentes podrán ponerse de acuerdo sobre los detalles que deba contener dicha sección de seguridad, la cual deberá incluir una guía de clasificación.

(4) La Autoridad de Seguridad Competente de la Parte en cuyo territorio deba ejecutarse el Contrato Clasificado deberá asegurarse de que el Contratista proteja la Información Clasificada transmitida por la Entidad Contratante conforme a las disposiciones del presente Acuerdo.

(5) Cualquier subcontratista deberá cumplir las mismas obligaciones de seguridad que el Contratista.

(6) Se remitirá una copia de la sección de seguridad de cualquier Contrato Clasificado a la Autoridad de Seguridad Competente de la Parte donde se vaya a desempeñar el trabajo, para permitir un control de seguridad adecuado.

(7) Representantes de las Autoridades de Seguridad Competentes podrán visitarse entre sí para analizar la eficiencia de las medidas adoptadas por un Contratista para la protección de la Información Clasificada comprendida en un Contrato Clasificado.

ARTÍCULO 9

TRANSMISIÓN DE INFORMACIÓN CLASIFICADA

(1) La Información Clasificada se transmitirá entre las Partes por canales diplomáticos.

(2) Si el uso de tales canales no resultara práctico o retrasara excesivamente la recepción de la Información Clasificada, las transmisiones podrán llevarse a cabo por personal con habilitación de seguridad apropiada y con acreditación de correo emitida por la Parte que transmita la Información Clasificada.

(3) Las Partes podrán transmitir Información Clasificada por medios electrónicos de conformidad con los procedimientos de seguridad mutuamente aprobados por las autoridades de seguridad competentes de ambas Partes.

(4) El envío de grandes artículos o cantidades de Materiales Clasificados acordado caso por caso será aprobado por ambas Autoridades de Seguridad Competentes

(5) Se podrán utilizar otros medios de transmisión de Información Clasificada si lo aprueban ambas Autoridades de Seguridad Competentes

ARTICULO 10

INFRACCIÓN DE SEGURIDAD

(1) En caso de que ocurra una infracción de seguridad de la que se derive un peligro cierto o la sospecha de un peligro con respecto a Información Clasificada originada por la otra Parte o recibida de ella o se sospeche que la Información Clasificada haya sido divulgada a personas no autorizadas, la Autoridad de Seguridad Competente de la Parte donde la infracción de seguridad haya ocurrido informará a la Autoridad de Seguridad Competente de la otra Parte tan pronto como sea posible y llevará a cabo la investigación apropiada La otra Parte colaborará en la investigación si fuera requerida para ello.

(2) En caso de que la infracción ocurra en un Estado distinto al de las Partes, la Autoridad de Seguridad Competente de la Parte remitente actuará de conformidad con el apartado 1 del presente artículo.

(3) En cualquiera de los casos, la otra Parte será informada de los resultados de la investigación y recibirá un informe final sobre los motivos y el alcance de los daños.

ARTÍCULO 11

GASTOS

Cada Parte cubrirá los propios gastos en que incurra con motivo de la aplicación y supervisión de todos los aspectos del presente Acuerdo.

ARTICULO 12

CONSULTA

(1) Las Autoridades de Seguridad Competentes de las Partes deberán notificarse mutuamente cualquier modificación de la normativa nacional relativa a la protección de la Información Clasificada.

(2) Las Autoridades de Seguridad Competentes de las Partes deberán consultarse mutuamente, a requerimiento de una de ellas, con el fin de asegurar una estrecha cooperación en la aplicación de las disposiciones del presente Acuerdo.

(3) Cada Parte permitirá las visitas a su territorio de los representantes de la Autoridad de Seguridad Competente de la otra Parte, con la finalidad de discutir los procedimientos para la protección de la información Clasificada transmitida por la otra Parte.

ARTÍCULO 13

SOLUCIÓN DE CONTROVERSIAS

Cualquier controversia relativa a la interpretación o aplicación del presente Acuerdo se resolverá mediante consultas entre las Autoridades de Seguridad Competentes de las Partes o, en el caso de que sea imposible alcanzar tal solución, a través de canales diplomáticos.

ARTÍCULO 14

DISPOSICIONES FINALES

(1) El presente Acuerdo entrará en vigor de conformidad con las leyes nacionales de cada una de las Partes, lo que se comunicará mediante canje de notas. El Acuerdo entrará en vigor el primer día del segundo mes siguiente a la recepción de la última de las notas.

(2) El presente Acuerdo se concluye por un período de tiempo indefinido. Cada Parte podrá denunciar el presente Acuerdo mediante notificación por escrito remitida a la otra Parte. En ese caso, el presente Acuerdo expirará seis meses después de la fecha de recepción de la notificación.

(3) En caso de terminación, toda la Información Clasificada transmitida u originada como resultado de la cooperación mutua entre las Partes, incluida la originada con motivo de la ejecución de un Contrato Clasificado, continuará estando protegida de conformidad con las disposiciones establecidas en el presente Acuerdo durante tanto tiempo como lo requiera el nivel de clasificación de seguridad.

(4) El presente Acuerdo podrá ser enmendado con el mutuo consentimiento por escrito de ambas Partes. Dichas enmiendas entrarán en vigor de acuerdo con el apartado 1 del presente artículo.

Hecho en dos originales, cada uno de ellos en polaco, español e inglés. En caso de discrepancia en la interpretación prevalecerá el texto inglés.

En nombre de la República de Polnia	En nombre del Reino de España
ZBIGNIEW WASSERMANN **Ministro** **Miembro del Consejo de Ministros**	**ALBERTO SAIZ CORTÉS** **Secretario de Estado Director** **del Centro Nacional de Inteligencia**
Fecha: 24.05.2006	**Fecha:** 18.04.2006
Lugar: Warszawa	**Lugar:** Madrid

AGREEMENT

between the Republic of Poland

and the Kingdom of Spain

on the Mutual Protection of

Classified Information

The Republic of Poland and the Kingdom of Spain,

hereinafter referred to as the "Parties",

Being aware of the changes in the political situation in the world

and recognising the important role of their mutual co-operation

for the stabilisation of peace, international security and mutual confidence,

Realising that good co-operation may require exchange

of classified information between the Parties,

Desiring to create a system of rules on the mutual protection

of classified information exchanged between the Parties under any

future co-operation agreement or classified contract,

Have agreed as follows:

ARTICLE 1

DEFINITIONS

For the purpose of this Agreement:

a. "Classified Information" means any information (namely knowledge that can be communicated in any form) or material, determined to require protection against unauthorised disclosure which has been so designated by security classification;

b. "Classified Material" means any item, equipment, device or weapon, either manufactured or in a process of manufacture, as well as components used for their manufacture, containing Classified Information;

c. "Classified Document" means any form of recorded Classified Information regardless of its physical form or characteristics;

d. "Contractor" means an individual or a legal entity possessing the legal capacity to conclude contracts;

e. "Contracting Entity" means an entity which intends to conclude a Classified Contract in the territory of the State of the other Party;

f. "Classified Contract" means a contract between two or more Contractors creating and defining enforceable rights and obligations between them, which contains or involves generation of or access to Classified Information;

g. "Competent Security Authorities" mean authorities designated by a Party as being responsible for the implementation and supervision of this Agreement;

h. "Receiving Party" means the Party whereto Classified Information is transmitted;

i. "Originating Party" means the Party that creates Classified Information;

j. "Third Party" means any international organisation or state that is not a Party to this Agreement;

k. "Personnel Security Clearance" means the determination by the Competent Security Authorities or other entity authorized under the national law of a Party, that an individual is eligible to have access to Classified Information;

l. "Facility Security Clearance" means the determination by the Competent Security Authorities or other entity authorized under the national law of a Party, that, from a security point of view, a facility has the physical and organisational capability to use and store Classified Information, in accordance with the national laws and regulations;

m. "Need-to-know" means that access to Classified Information may only be granted to persons who have a verified requirement for knowledge of, or possession of such information in order to perform their official and professional duties.

ARTICLE 2

SECURITY CLASSIFICATIONS

(1) The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the national Law of the respective Party:

Republic of Poland	Kingdom of Spain	Equivalent in English
ŚCIŚLE TAJNE	SECRETO	TOP SECRET
TAJNE	RESERVADO	SECRET
POUFNE	CONFIDENCIAL	CONFIDENTIAL
ZASTRZEŻONE	DIFUSIÓN LIMITADA	RESTRICTED

(2) The Receiving Party shall neither downgrade nor declassify the received Classified Information without the prior written consent of the Originating

Party. The Originating Party shall inform the Receiving Party of any changes in security classification of the transmitted information.

(3) The obligation referred to in Paragraph 2 shall also apply to Classified Information generated as a result of mutual co-operation of the Parties, including this originated in the connection with performance of a Classified Contract.

(4) The Receiving Party shall mark the received Classified Information with its own equivalent security classification.

ARTICLE 3

COMPETENT SECURITY AUTHORITIES

(1) The Competent Security Authorities responsible for the implementation and supervision of all aspects of this Agreement are:

In the Republic of Poland:

Head of the Internal Security Agency
ul. Rakowiecka 2A
00-993 Warsaw
POLAND

Head of the Military Information Services
00-909 Warsaw 60
POLAND

In the Kingdom of Spain:

Secretary of State, Director of the National Intelligence Centre
National Security Office
Avda. Padre Huidobro, s/n
28023 Madrid
SPAIN

(2) In order to achieve and maintain comparable standards of security, the respective Competent Security Authorities shall, on request, provide each other with information about their security standards, procedures and practices for protection of Classified Information.

(3) The Competent Security Authorities may conclude executive agreements for the purpose of implementation of the provisions hereof.

ARTICLE 4

SECURITY PROTECTION

(1) In accordance with this Agreement and their national laws and regulations, the Parties shall implement appropriate measures to protect Classified Information, which is transmitted under this Agreement or produced or developed in connection with a Classified Contract or any relation between the Parties.

(2) The Parties shall afford all transmitted, produced or developed Classified Information the same degree of security protection as is provided for their own Classified Information of the equivalent level, as defined in Article 2 of this Agreement.

(3) On request, the Competent Security Authorities of the Parties, taking into account their national laws and regulations, shall assist each other during the vetting procedures of their citizens or facilities living or located in the territory of the other Party, preceding the issue of the Personnel Security Clearance and the Facility Security Clearance.

(4) The Parties shall recognise the Personnel and Facility Security Clearances issued in accordance with the national laws and regulations of the other Party. The equivalence of the security clearances shall be in compliance with Article 2 of this Agreement.

(5) The Competent Security Authorities shall communicate to each other information on changes regarding the issued Personnel and Facility Security Clearances.

ARTICLE 5

USE AND DISCLOSURE OF CLASSIFIED INFORMATION

(1) Classified Information transmitted from one Party to the other Party shall be used only for the specific purpose that it has been provided for.

(2) The Parties shall not release, disclose or permit the release or disclosure of Classified Information received under this Agreement to Third Parties, or to their citizens or public or private entities, without the prior written consent of the Originating Party.

(3) This Agreement may not be invoked by either Party in order to obtain Classified Information that the other Party has received from a Third Party.

(4) Access to Classified Information and to specific areas where classified activities are performed or where Classified Information is stored, shall be limited only to those persons who have been granted appropriate Personnel Security Clearance, who have been briefed and who have a "need-to-know".

ARTICLE 6

TRANSLATION, REPRODUCTION AND DESTRUCTION

(1) Classified Information marked as ŚCIŚLE TAJNE/SECRETO/TOP SECRET shall be translated or reproduced only upon the written permission of the Competent Security Authority of the Originating Party.

(2) Translations and reproductions of Classified Information shall be made by individuals holding the appropriate Personnel Security Clearance. They shall

be marked and placed under the same protection as the original information. The translation and number of copies shall be limited to that required for official purposes.

(3) Translations shall bear an appropriate note in the language into which they are translated indicating that they contain Classified Information received from the Originating Party.

(4) ŚCIŚLE TAJNE/SECRETO/TOP SECRET information and material shall not be destroyed. They shall be returned to the Competent Security Authority of the Originating Party. Remaining Classified Information shall be destroyed in accordance with national laws and regulations in such a manner as to prevent its partial or total reconstruction. For information classified as TAJNE/RESERVADO/SECRET, prior written approval of the Originating Party is required.

ARTICLE 7

VISITS

(1) Visits entailing access to Classified Information by citizens from one Party to the other Party are subject to prior written authorisation given by the Competent Security Authority of the host Party.

(2) Visits entailing access to Classified Information by a citizen of a Third Party, shall only be authorised upon the written consent of the Originating Party.

(3) The Competent Security Authority of the sending Party shall notify the Competent Security Authority of the host Party of expected visitors in accordance with the procedures defined in paragraphs (4) to (11) of this article. These procedures can be changed on the basis of written consent of Competent Security Authorities of both Parties.

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

a. granted appropriate Personnel Security Clearance by the Competent Security Authority or other relevant authority of the sending Party;

b. authorised to receive or to have access to Classified Information in accordance with the national laws and regulations of their Party.

(5) The Competent Security Authority of the sending Party shall notify the Competent Security Authority of the host Party of the planned visit through a request for visit, which has to be received at least twenty-five (25) working days before the visit or the first of the recurring visits take place.

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

(7) The request for visit shall include:

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

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

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

d. certification of the visitor's Personnel Security Clearance and its validity;

e. object and purpose of the visit or visits;

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

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

(8) The validity of visit authorisation in case of recurring visits shall not exceed twelve (12) months.

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

(10) Classified Information accessible during the visit shall be protected pursuant to the provisions of this Agreement.

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

ARTICLE 8

CLASSIFIED CONTRACTS

(1) The Contracting Entity, wishing to conclude a Classified Contract with the Contractor having a seat in the territory of the other Party, shall obtain through its Competent Security Authority prior written assurance from the Competent Security Authority of the other Party that the proposed Contractor holds a Facility Security Clearance of an appropriate level.

(2) If the Contractor has not been previously granted a Facility Security Clearance of the specified security classification level, the Competent Security Authority which is to issue the assurance, shall immediately notify the Competent Security Authority of the other Party, that upon its request, the actions to issue the appropriate Facility Security Clearance will be undertaken.

(3) Every Classified Contract concluded under the provisions of this Agreement shall include an appropriate security section. The Competent Security Authorities may agree upon the details of such security section, which shall include the classification guide.

(4) The Competent Security Authority of the Party in the territory of which the Classified Contract is to be performed shall ensure that the Contractor

protects Classified Information transmitted by the Contracting Entity in accordance with the provisions of this Agreement.

(5) Any subcontractor must fulfil the same security obligations as the Contractor.

(6) Copy of the security section of any Classified Contract shall be forwarded to the Competent Security Authority of the Party where the work is to be performed, to allow adequate security monitoring.

(7) Representatives of the Competent Security Authorities may visit each other in order to analyse the efficiency of the measures adopted by the Contractor for the protection of Classified Information involved in a Classified Contract.

ARTICLE 9

TRANSMISSION OF CLASSIFIED INFORMATION

(1) Classified Information shall be transmitted between the Parties through diplomatic channels.

(2) If the use of such channels would be impractical or unduly delay receipt of the Classified Information, transmissions may be undertaken by appropriately security cleared personnel empowered with a courier certificate issued by the Party which transmits the Classified Information.

(3) The Parties may transmit Classified Information by electronic means in accordance with security procedures mutually approved by the competent security authorities of both Parties.

(4) Delivery of large items or quantities of Classified Materials arranged on a case by case basis shall be approved by both Competent Security Authorities.

(5) Other means of transmission of Classified Information may be used if approved by both Competent Security Authorities.

ARTICLE 10

BREACH OF SECURITY

(1) In case of a breach of security that results in a certain or suspected compromise of Classified Information originated by or received from the other Party or suspicion that Classified Information has been disclosed to unauthorised persons, the Competent Security Authority of the Party where the breach occurs shall inform the Competent Security Authority of the other Party as soon as possible and carry out the appropriate investigation. The other Party shall, if required, co-operate in the investigation.

(2) In case the compromise occurs in a state other than the Parties, the Competent Security Authority of the despatching Party shall take the actions prescribed in paragraph (1) above.

(3) In any case, the other Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of the damage.

ARTICLE 11

EXPENSES

Each Party shall bear its own expenses incurred in connection with the implementation and supervision of all aspects of this Agreement.

ARTICLE 12

CONSULTATION

(1) The Competent Security Authorities of the Parties shall notify each other of any amendments to the national regulations concerning the protection of Classified Information.

(2) The Competent Security Authorities of the Parties shall consult each other, upon the request of one of them, in order to ensure close cooperation in the implementation of the provisions hereof.

(3) Each Party shall allow the representatives of the Competent Security Authority of the other Party to come on visits to its own territory to discuss the procedures for protection of Classified Information transmitted by the other Party.

ARTICLE 13

SETTLEMENT OF DISPUTES

Any dispute regarding the interpretation or application of this Agreement shall be settled by consultations between the Competent Security Authorities of the Parties or, in the case that such a settlement is impossible to reach, through diplomatic channels.

ARTICLE 14

FINAL PROVISIONS

(1) This Agreement shall enter into force in accordance with the national laws of each of the Parties, what shall be stated in the way of exchange of the notes. The Agreement shall enter into force on the first day of the second month following the receipt of the latter of the notes.

(2) This Agreement is concluded for an unlimited period of time. It may be terminated by either Party upon giving written notice to the other Party. In such a case, this Agreement shall expire after six months following the receipt of the notice of termination.

(3) In the event of termination thereof, any Classified Information transmitted or originated as a result of mutual co-operation of the Parties, including those originated in the connection with performance of a Classified Contract, shall continue to be protected pursuant to the provisions of this Agreement as long as required under the security classification level.

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

Done in two originals, each one in the Polish, Spanish and English languages. In case of any divergence of interpretation the English text shall prevail.

On behalf of the Republic of Poland

ZBIGNIEW WASSERMANN
Minister
Member of the Council of Ministers

Date: 24.05.2006

Place: Warsaw

On behalf of the Kingdom of Spain

ALBERTO SAIZ CORTÉS
Secretary of State
Director of the National Intelligence Centre

Date: 18.04.2006

Place: Madrid

Po zaznajomieniu się z powyższą umową, w imieniu Rzeczypospolitej Polskiej oświadczam, że:

— została ona uznana za słuszną zarówno w całości, jak i każde z postanowień w niej zawartych,

— jest przyjęta, ratyfikowana i potwierdzona,

— będzie niezmiennie zachowywana.

Na dowód czego wydany został akt niniejszy, opatrzony pieczęcią Rzeczypospolitej Polskiej.

Dano w Warszawie dnia 15 lutego 2007 r.

Prezydent Rzeczypospolitej Polskiej: *L. Kaczyński*

L.S.

Prezes Rady Ministrów: *J. Kaczyński*