

985

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o wzajemnej ochronie informacji niejawnych,

podpisana w Warszawie dnia 18 sierpnia 2006 r.

W imieniu Rzeczypospolitej Polskiej

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

podaje do powszechnej wiadomości:

W dniu 18 sierpnia 2006 r. w Warszawie została podpisana Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o wzajemnej ochronie informacji niejawnych, w następującym brzmieniu:

UMOWA

między

RZĄDEM RZECZYPOSPOLITEJ POLSKIEJ

a

**RZĄDEM ZJEDNOCZONEGO KRÓLESTWA
WIELKIEJ BRYTANII i IRLANDII PÓŁNOCNEJ**

O WZAJEMNEJ OCHRONIE INFORMACJI

NIEJAWNYCH

Rząd Rzeczypospolitej Polskiej oraz Rząd Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej, zwane dalej Stronami, pragnąc zapewnić ochronę informacji niejawnych przekazywanych zgodnie z zatwierdzoną procedurą pomiędzy tymi krajami lub jednostkami organizacyjnymi prowadzącymi działalność handlową i przemysłową w każdym z tych krajów, mając na uwadze bezpieczeństwo narodowe, dokonały następujących ustaleń zawartych w niniejszej Umowie.

ARTYKUŁ 1 ZASTOSOWANIE

Niniejsza Umowa reguluje wszelkie działania pomiędzy Stronami związane z wymianą informacji niejawnych, z wyjątkiem wymiany informacji nuklearnych, biologicznych i chemicznych dotyczących wyposażenia powszechnie określanego jako Broń Masowego Rażenia, które mogą być przedmiotem odrębnych porozumień.

ARTYKUŁ 2 DEFINICJE

W rozumieniu niniejszej Umowy:

1. **„Informacje niejawne”** oznaczają informacje, które, niezależnie od formy ich wyrażania, wymagają ochrony przed nieuprawnionym ujawnieniem oraz którym nadano klauzulę tajności.
2. **„Kontrahent”** oznacza osobę fizyczną, osobę prawną lub jednostkę organizacyjną posiadającą zdolność prawną do zawierania kontraktów.
3. **„Kontrakt”** lub **„Kontrakt podwykonawczy”** oznacza umowę pomiędzy dwiema lub więcej stronami określającą oraz definiującą ciężące na nich prawa i obowiązki.
4. **„Kontrakt niejawny”** oznacza kontrakt lub kontrakt podwykonawczy, który zawiera informacje niejawne lub którego realizacja wiąże się z dostępem do informacji niejawnych.
5. **„Właściwy organ bezpieczeństwa”** oznacza właściwy organ, który zgodnie z prawem krajowym Stron jest uprawniony do realizowania postanowień niniejszej Umowy.
6. **„Krajowa władza bezpieczeństwa”** oznacza rządowy organ bezpieczeństwa, na którym spoczywa pełna odpowiedzialność za bezpieczeństwo informacji niejawnych w każdym z państw.

7. „Strona wytwarzająca” oznacza Stronę wytwarzającą informacje niejawne.
8. „Strona otrzymująca” oznacza Stronę, której przekazywane są informacje niejawne.

ARTYKUŁ 3 KLAUZULE TAJNOŚCI

1. W rozumieniu niniejszej Umowy, niżej wymienione klauzule tajności są równorzędne:

| W RZECZYPOSPOLITEJ POLSKIEJ | W ZJEDNOCZONYM KRÓLESTWIE WIELKIEJ BRYTANII I IRLANDII PÓŁNOCNEJ |
|-----------------------------|--|
| ŚCIŚLE TAJNE | UK TOP SECRET |
| TAJNE | UK SECRET |
| POUFNE | UK CONFIDENTIAL |
| ZASTRZEŻONE | UK RESTRICTED |

2. W przypadku potrzeby wymiany informacji niejawnych oznaczonych klauzulą ŚCIŚLE TAJNE / UK TOP SECRET, Strony przyjmą odrębne uzgodnienia.

ARTYKUŁ 4 KRAJOWE WŁADZE BEZPIECZEŃSTWA

1. Krajowymi władzami bezpieczeństwa odpowiedzialnymi za bezpieczeństwo informacji niejawnych w każdym z krajów są:

W Rzeczypospolitej Polskiej:

- w sferze cywilnej:

Szef Agencji Bezpieczeństwa Wewnętrznego

ul. Rakowiecka 2A

00-993 Warszawa

POLSKA

- w sferze wojskowej:
SzeF Wojskowych Służb Informacyjnych
00-909 Warszawa 60
POLSKA

W Zjednoczonym Królestwie Wielkiej Brytanii i Irlandii Północnej:

Security Policy Division
Intelligence & Security Secretariat
Cabinet Office
70 Whitehall
London, SW1P 2AS
UNITED KINGDOM

2. Jeśli zajdzie taka potrzeba, Strony będą się informować o pozostałych właściwych organach bezpieczeństwa.

ARTYKUŁ 5

OGRANICZENIA W WYKORZYSTYWANIU I UJAWNIANIU INFORMACJI NIEJAWNYCH

1. Z zastrzeżeniem postanowień ustępu 2, Strona otrzymująca nie ujawnia, nie wykorzystuje, jak też nie wyraża zgody na ujawnienie lub wykorzystanie informacji niejawnych bez pisemnej zgody Strony wytwarzającej, z wyjątkiem celów oraz w granicach określonych przez lub w imieniu Strony wytwarzającej.
2. W zakresie swojego prawa krajowego Strona otrzymująca podejmuje wszelkie prawnie dostępne kroki w celu zabezpieczenia otrzymanych od Strony wytwarzającej informacji niejawnych przed ich ujawnieniem na jakiegokolwiek podstawie prawnej. W przypadku gdy zostanie zgłoszony wniosek o zniesienie klauzuli tajności lub ujawnienie informacji niejawnych przekazanych zgodnie z postanowieniami niniejszej Umowy, Strona

otrzymująca niezwłocznie zawiadamia Stronę wytwarzającą, a następnie obydwie Strony konsultują się przed podjęciem jakiegokolwiek decyzji.

3. Z zastrzeżeniem postanowień ustępów 1 oraz 2, Strona otrzymująca nie przekazuje informacji niejawnych przekazanych zgodnie z postanowieniami niniejszej Umowy przedstawicielowi rządu, kontrahentowi, pracownikowi kontrahenta lub jakiegokolwiek innej osobie posiadającej obywatelstwo strony trzeciej, a także jakiegokolwiek organizacji międzynarodowej.

ARTYKUŁ 6

OCHRONA INFORMACJI NIEJAWNYCH

1. Strona wytwarzająca zapewnia, że Strona otrzymująca jest informowana o:
 - 1) Nadanych klauzulach tajności oraz warunkach udostępniania lub ograniczeniach w wykorzystywaniu informacji;
 - 2) Wszelkich późniejszych zmianach w klasyfikacji.
2. Zgodnie ze swoim prawem krajowym Strona otrzymująca:
 - 1) Zapewnia informacjom otrzymanym od drugiej Strony taką samą ochronę, jaką zapewnia informacjom niejawnym o równorzędnych klauzulach tajności wytworzonym przez Stronę otrzymującą;
 - 2) Zapewnia nadanie informacjom niejawnym swojej własnej równorzędnej klauzuli tajności, zgodnie z postanowieniami artykułu 3 ustęp 1;
 - 3) Zapewnia zachowanie klauzul tajności, chyba że zostanie upoważniona do ich zmiany przez lub w imieniu Strony wytwarzającej.
3. W celu osiągnięcia i zachowania porównywalnych standardów bezpieczeństwa każda krajowa władza bezpieczeństwa, na prośbę drugiej Strony, przekazuje informacje na temat swoich standardów bezpieczeństwa, procedur oraz praktyk stosowanych w celu zachowania bezpieczeństwa informacji niejawnych. W tym celu krajowa władza bezpieczeństwa każdej Strony będzie ułatwiać odbywanie wizyt przez przedstawicieli odpowiednich organów bezpieczeństwa drugiej Strony.

ARTYKUŁ 7

DOSTĘP DO INFORMACJI NIEJAWNYCH

Dostęp do informacji niejawnych ogranicza się do osób, których zadania wymagają zapoznania się z nimi oraz wobec których przeprowadzono, zgodnie z prawem krajowym, postępowanie umożliwiające uzyskanie dostępu do informacji niejawnych o klauzuli tajności odpowiadającej klauzuli informacji, które mają być udostępnione.

ARTYKUŁ 8

PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne oznaczone klauzulami POUFNE / UK CONFIDENTIAL oraz TAJNE / UK SECRET są przekazywane między obydwojoma krajami zgodnie z prawem krajowym Strony wytwarzającej. Wymiana odbywa się zazwyczaj drogą dyplomatyczną, Strony mogą jednak dokonać innych ustaleń, jeśli zostaną one obustronnie zaakceptowane przez odpowiednie właściwe organy bezpieczeństwa.
2. Informacje niejawne oznaczone klauzulą ZASTRZEŻONE / UK RESTRICTED są przekazywane zgodnie z prawem krajowym Strony wytwarzającej.

ARTYKUŁ 9

POWIELANIE, TŁUMACZENIE ORAZ NISZCZENIE INFORMACJI NIEJAWNYCH

1. Strona otrzymująca powieliła informacje niejawne zgodnie ze swoim prawem krajowym. Wszelkie powielone informacje podlegają takiej samej ochronie jak oryginały. Liczba kopii ograniczona jest do minimum niezbędnego do celów służbowych.

2. Wszelkie informacje niejawne są tłumaczone przez osoby, wobec których przeprowadzono odpowiednie postępowanie sprawdzające. Informacjom tym nadaje się taką samą klauzulę tajności, jaką posiadają oryginały.
3. Po wykorzystaniu informacje niejawne są niszczone zgodnie z prawem krajowym Strony otrzymującej w taki sposób, aby uniemożliwić ich częściową lub całkowitą rekonstrukcję.
4. Strona wytwarzająca może zabronić powielania, wprowadzania zmian lub niszczenia informacji niejawnych poprzez odpowiednie ich oznaczenie bądź załączenie pisemnej informacji. W takich przypadkach informacje niejawne należy zwrócić Stronie wytwarzającej niezwłocznie po ich wykorzystaniu.

ARTYKUŁ 10

WIZYTY

1. Wizyta, która wiąże się z dostępem do informacji niejawnych lub jednostek, w których wykonywane są prace związane z dostępem do takich informacji, wymaga wcześniejszej zgody właściwego organu bezpieczeństwa Państwa przyjmującego. Warunek ten dotyczy również osób przybywających z wizytą oddelegowanych do wykonywania obowiązków służbowych. Wnioski o wyrażenie zgody na wizytę są dostarczane za pośrednictwem odpowiednich właściwych organów bezpieczeństwa.
2. Osoby przybywające z wizytą przestrzegają przepisów bezpieczeństwa Strony przyjmującej.
3. W przypadku zaangażowania w określony projekt lub kontrakt, za zgodą obu Stron, możliwe jest sporządzenie stałych list osób przybywających z wizytą. Listy te są ważne przez okres nieprzekraczający 12 miesięcy i mogą być przedłużane na kolejne okresy nieprzekraczające 12 miesięcy, po wcześniejszym wyrażeniu zgody przez właściwe organy bezpieczeństwa. Listy te są dostarczane zgodnie ze zwykłymi procedurami Strony otrzymującej. Po zaakceptowaniu listy, uzgodnienia dotyczące wizyt mogą

- być dokonywane bezpośrednio pomiędzy zainteresowanymi jednostkami organizacyjnymi lub przedsiębiorcami.
4. Wszelkie informacje, które mogą być przekazane bądź udostępnione osobom przybywającym z wizytą, są traktowane tak jak informacje przekazane zgodnie z postanowieniami niniejszej Umowy.
 5. Właściwy organ bezpieczeństwa Strony otrzymującej jest powiadamiany o planowanej wizycie przez właściwy organ bezpieczeństwa Strony wytwarzającej z co najmniej dwudziestopięciodniowym wyprzedzeniem. W wyjątkowych przypadkach, wizyta może być zatwierdzona w trybie przyspieszonym z zastrzeżeniem dokonania wcześniejszej koordynacji.
 6. Wnioski o wyrażenie zgody na wizytę zawierają co najmniej następujące informacje:
 - 1) Imię i nazwisko osoby przybywającej z wizytą, datę i miejsce urodzenia, obywatelstwo oraz numer paszportu lub innego dowodu tożsamości;
 - 2) Stanowisko służbowe osoby przybywającej z wizytą oraz nazwę jednostki lub organizacji, którą reprezentuje;
 - 3) Poświadczenie bezpieczeństwa osoby przybywającej z wizytą;
 - 4) Termin i czas trwania wizyty;
 - 5) Cel wizyty;
 - 6) Nazwy jednostek oraz organizacji, w których osoba przybywająca z wizytą będzie przebywać;
 - 7) Imiona i nazwiska osób przyjmujących osobę przybywającą z wizytą.
 7. Wizyty związane z dostępem do informacji o klauzuli ZASTRZEŻONE / UK RESTRICTED są organizowane bezpośrednio między jednostką wysyłającą a jednostką przyjmującą wizytę.

ARTYKUŁ 11

KONTRAKTY NIEJAWNE

1. W przypadku złożenia propozycji zawarcia lub upoważnienia kontrahenta ze swojego kraju do zawarcia kontraktu, którego realizacja wiąże się z dostępem

do informacji niejawnych oznaczonych klauzulą POUFNE / UK CONFIDENTIAL lub wyższą, z kontrahentem pochodzącym z kraju drugiej Strony, Strona wytwarzająca otrzymuje wcześniejsze zapewnienie od właściwego organu bezpieczeństwa drugiego kraju, że proponowany kontrahent spełnia warunki bezpieczeństwa, a także posiada zabezpieczenia zapewniające właściwą ochronę informacji niejawnych. Zapewnienie takie jest jednoznaczne z gwarancją, że środki bezpieczeństwa stosowane przez kontrahenta spełniającego warunki bezpieczeństwa są zgodne z prawem krajowym właściwego organu bezpieczeństwa, który sprawuje nad nim kontrolę.

2. Kontrakty, które zostaną zawarte po przeprowadzeniu wyżej wymienionych procedur poprzedzających, zawierają punkt dotyczący wymogów bezpieczeństwa, zawierający co najmniej:
 - 1) Definicję terminu „Informacje niejawne” oraz odpowiadające sobie wzajemnie klauzule tajności Stron zgodnie z postanowieniami artykułu 3 ustęp 1;
 - 2) Nazwy właściwych organów bezpieczeństwa każdej ze Stron, uprawnionych do udostępniania oraz koordynowania ochrony informacji niejawnych związanych z kontraktem;
 - 3) Sposób przekazywania informacji niejawnych;
 - 4) Procedury i mechanizmy informowania o wszelkich zmianach mogących mieć miejsce w odniesieniu do informacji niejawnych. Zmiany te mogą dotyczyć nadanych klauzul tajności lub ustania okresu ochrony informacji niejawnych;
 - 5) Procedury wyrażania zgody na wizytę, dostęp lub dokonanie inspekcji przez przedstawicieli jednej Strony u kontrahenta drugiej Strony, który jest objęty kontraktem.
3. Właściwy organ bezpieczeństwa Strony wytwarzającej przekazuje kopię odpowiednich części kontraktu niejawnego właściwemu organowi bezpieczeństwa Strony otrzymującej w celu umożliwienia właściwej kontroli.

4. Każdy kontrakt zawiera wytyczne dotyczące wymogów bezpieczeństwa oraz klauzul tajności nadanych poszczególnym elementom kontraktu. W Rzeczypospolitej Polskiej wytyczne te stanowi instrukcja bezpieczeństwa przemysłowego. W Zjednoczonym Królestwie Wielkiej Brytanii i Irlandii Północnej wytyczne te będą załączone w specjalnych klauzulach określających wymogi bezpieczeństwa oraz w liście określającym zasady bezpieczeństwa. Wytyczne, o których mowa, określają każdy niejawnny aspekt kontraktu lub każdą informację niejawną, która powstanie w wyniku jego realizacji, wraz z przypisaniem im odpowiednich klauzul tajności. Kiedy zachodzi potrzeba zmiany dotyczące wymogów bezpieczeństwa lub elementów kontraktu podaje się do wiadomości drugiej Stronie. Strona wytwarzająca informuje Stronę otrzymującą o obniżeniu lub zniesieniu klauzuli tajności wszystkich lub którejkolwiek informacji niejawnej.

ARTYKUŁ 12

OBUSTRONNE PRZEDSIĘWZIĘCIA W ZAKRESIE

BEZPIECZEŃSTWA

1. Na wniosek jednej ze Stron właściwy organ bezpieczeństwa drugiej Strony udziela informacji o spełnianiu warunków bezpieczeństwa przez kontrahenta prowadzącego działalność na terenie swojego kraju oraz dawaniu rękojmi zachowania tajemnicy przez obywatela swojego kraju. Takie zawiadomienia będą traktowane jako zapewnienia o posiadaniu odpowiednio świadectwa bezpieczeństwa przemysłowego oraz poświadczenia bezpieczeństwa.
2. Na wniosek jednej ze Stron właściwy organ bezpieczeństwa drugiej Strony ustala, czy kontrahent lub osoba fizyczna będący przedmiotem postępowania dają rękojmię zachowania tajemnicy, oraz przesyła zapewnienie o posiadaniu poświadczenia bezpieczeństwa, jeżeli wobec kontrahenta lub osoby fizycznej przeprowadzono już postępowanie sprawdzające. W przypadku kiedy kontrahent lub osoba fizyczna nie posiada poświadczenia bezpieczeństwa lub posiada poświadczenie uprawniające do dostępu do informacji niejawnych

objętych klauzulą niższą niż klauzula dokumentu, który ma być udostępniony, należy przesłać zawiadomienie informujące, iż zapewnienie o posiadaniu poświadczenia bezpieczeństwa nie może być przekazane natychmiast, ale podjęto działania mające na celu jego wydanie. Zapewnienie o posiadaniu świadectwa bezpieczeństwa przemysłowego lub poświadczenia bezpieczeństwa należy przekazać po pomyślnym zakończeniu postępowania sprawdzającego. Świadectwo bezpieczeństwa przemysłowego nie jest wymagane w przypadku dostępu do informacji oznaczonych klauzulą ZASTRZEŻONE / UK RESTRICTED.

3. Jeżeli właściwy organ bezpieczeństwa kraju, w którym kontrahent jest zarejestrowany, uzna, że kontrahent ten nie spełnia wymogów bezpieczeństwa niezbędnych do wydania świadectwa bezpieczeństwa przemysłowego, należy o tym poinformować właściwy organ bezpieczeństwa, który wystąpił z wnioskiem o przekazanie zapewnienia o posiadaniu świadectwa bezpieczeństwa przemysłowego.
4. W przypadku kiedy właściwy organ bezpieczeństwa którejkolwiek ze Stron wejdzie w posiadanie informacji wskazującej, że kontrahent lub osoba fizyczna, którym wydane zostało świadectwo bezpieczeństwa przemysłowego lub poświadczenie bezpieczeństwa, nie daje rękojmi zachowania tajemnicy, powiadamia on właściwy organ bezpieczeństwa drugiej Strony o charakterze takiej informacji oraz o czynnościach, które zamierza lub już w tej sprawie podjął. Właściwy organ bezpieczeństwa którejkolwiek ze Stron może wystąpić z wnioskiem o sprawdzenie wydanego wcześniej przez właściwy organ bezpieczeństwa drugiej Strony świadectwa bezpieczeństwa przemysłowego lub poświadczenia bezpieczeństwa, pod warunkiem że wniosek ten zawiera uzasadnienie. Strona występująca z takim wnioskiem jest informowana o wynikach sprawdzenia oraz o podjętych w jego następstwie czynnościach.
5. Jeżeli właściwy organ bezpieczeństwa którejkolwiek ze Stron zawiesza lub podejmuje decyzję o cofnięciu poświadczenia bezpieczeństwa, o którym wcześniej poinformowano drugą Stronę, lub jeśli zawiesza bądź podejmuje

decyzję o cofnięciu upoważnienia do dostępu do informacji niejawnych przyznanego obywatelowi drugiej Strony na podstawie poświadczenia bezpieczeństwa, organ ten informuje o zaistniałej sytuacji drugą Stronę oraz podaje przyczyny takiego działania.

ARTYKUŁ 13

NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH

1. W przypadku naruszenia przepisów o ochronie informacji niejawnych polegającego na utracie informacji niejawnych lub podejrzeniu, że informacje niejawne otrzymane od drugiej Strony zostały ujawnione osobom nieupoważnionym, właściwy organ bezpieczeństwa Strony otrzymującej niezwłocznie informuje o tym fakcie właściwy organ bezpieczeństwa Strony wytwarzającej.
2. Strona otrzymująca przeprowadza, w trybie natychmiastowym i zgodnie z prawem krajowym, postępowanie wyjaśniające. W razie potrzeby w postępowaniu wyjaśniającym bierze udział Strona wytwarzająca. Strona otrzymująca informuje niezwłocznie Stronę wytwarzającą o okolicznościach i wyniku postępowania wyjaśniającego oraz środkach zastosowanych w celu uniknięcia powtórzenia się takiej sytuacji.

ARTYKUŁ 14

KOSZTY

Każda ze Stron pokrywa swoje własne koszty poniesione w związku z implementacją i wejściem w życie niniejszej Umowy.

ARTYKUŁ 15

ROZSTRZYGANIE SPORÓW

Wszelkie sporne kwestie dotyczące interpretacji lub stosowania niniejszej Umowy są rozstrzygane wyłącznie w drodze konsultacji między Stronami i nie są przedkładane do rozstrzygnięcia żadnemu krajowemu lub międzynarodowemu trybunałowi.

ARTYKUŁ 16

POSTANOWIENIA KOŃCOWE

1. Każda ze Stron informuje drugą Stronę drogą dyplomatyczną o zakończeniu wewnętrznych procedur wymaganych do wejścia niniejszej Umowy w życie. Niniejsza Umowa wchodzi w życie pierwszego dnia drugiego miesiąca, który nastąpi po dniu otrzymania noty późniejszej.
2. Niniejsza Umowa zawarta jest na czas nieokreślony. W dowolnym czasie do niniejszej Umowy mogą być wprowadzane na piśmie poprawki za obustronną zgodą Stron. Poprawki wchodzi w życie zgodnie z postanowieniami ustępu 1.
3. Niniejsza Umowa może zostać wypowiedziana przez którąkolwiek ze Stron w drodze przekazania noty drugiej Stronie. Umowa utraci wówczas moc po upływie sześciu miesięcy od dnia otrzymania noty zawiadamiającej o wypowiedzeniu. W przypadku wypowiedzenia wszystkie informacje niejawną przekazane lub wytworzone na podstawie niniejszej Umowy będą w dalszym ciągu traktowane zgodnie z jej postanowieniami.

Na dowód czego niżej podpisani, należycie do tego upoważnieni przez swoje Rządy, podpisali niniejszą Umowę.

Sporządzono w Warszawie dnia 18 sierpnia 2006 roku w dwóch egzemplarzach, każdy w językach polskim i angielskim, przy czym obydwie teksty są jednakowo autentyczne.

**Z UPOWAŻNIENIA RZĄDU
RZECZYPOSPOLITEJ
POLSKIEJ**



**Marek Pasionek
Podsekretarz Stanu
w Kancelarii Prezesa
Rady Ministrów**

**Z UPOWAŻNIENIA RZĄDU
ZJEDNOCZONEGO KRÓLESTWA
WIELKIEJ BRYTANII I IRLANDII
PÓŁNOCNEJ**



**Patrick Davies
Chargé d'Affaires
Ambasada Brytyjska**

AGREEMENT

between

THE GOVERNMENT OF THE REPUBLIC OF

POLAND

and

THE GOVERNMENT OF THE UNITED KINGDOM

OF GREAT BRITAIN AND NORTHERN IRELAND

CONCERNING

THE MUTUAL PROTECTION OF CLASSIFIED

INFORMATION

The Government of the Republic of Poland and the Government of the United Kingdom of Great Britain and Northern Ireland, hereinafter referred to as the Parties, wishing to ensure the protection of Classified Information transferred between the two countries or to commercial and industrial organisations in either of the two countries, through approved channels, have, in the interests of national security, established the following arrangements which are set out in this Agreement.

ARTICLE 1 APPLICABILITY

This Agreement shall govern any activities between the Parties involving the exchange of Classified Information, with the exception of the exchange of Nuclear, Biological or Chemical information related to equipment commonly referred to as Weapons of Mass Destruction, which would be the subject of separate arrangements.

ARTICLE 2 DEFINITIONS

For the purpose of this Agreement:

1. “**Classified Information**” means information in any form requiring protection against unauthorised disclosure and has so been marked with a security classification.
2. “**Contractor**” means an individual, legal entity or organisational unit possessing the legal capability to undertake contracts.
3. “**Contract**” or “**Sub Contract**” means an agreement between two or more parties creating and defining enforceable rights and obligations.
4. “**Classified Contract**” means a Contract or Sub Contract which contains or involves Classified Information.
5. “**Competent Security Authority**” means a competent body authorised according to the national law and regulations of the Parties which is responsible for the implementation of this Agreement.
6. “**National Security Authority**” means the government Security Authority with ultimate responsibility for the security of Classified Information in each country.
7. “**Originating Party**” means the Party initiating the Classified Information.

8. “**Recipient Party**” means the Party to which the Classified Information is transmitted.

ARTICLE 3 SECURITY CLASSIFICATIONS

1. For the purpose of this Agreement the equivalent security classifications are:

| IN THE REPUBLIC OF POLAND | IN THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND |
|---------------------------|---|
| ŚCIŚLE TAJNE | UK TOP SECRET |
| TAJNE | UK SECRET |
| POUFNE | UK CONFIDENTIAL |
| ZASTRZEŻONE | UK RESTRICTED |

2. In the event that Classified Information at the ŚCIŚLE TAJNE / UK TOP SECRET level needs to be exchanged, separate provisions will be agreed between the Parties.

ARTICLE 4 NATIONAL SECURITY AUTHORITIES

1. The National Security Authorities responsible for the security of Classified Information in each country are:

For the Republic of Poland:

- in the civilian sphere:

Szef Agencji Bezpieczeństwa Wewnętrznego

ul. Rakowiecka 2A

00-993 Warszawa

POLAND

- in the military sphere:
Szeft Wojskowych Służb Informacyjnych
00-909 Warszawa 60
POLAND

For the United Kingdom of Great Britain and Northern Ireland:

Security Policy Division
Intelligence & Security Secretariat
Cabinet Office
70 Whitehall
London, SW1P 2AS
UNITED KINGDOM

2. The Parties shall inform each other of any additional Competent Security Authorities as appropriate.

ARTICLE 5

**RESTRICTIONS ON USE AND DISCLOSURE
OF CLASSIFIED INFORMATION**

1. Subject to the provisions of paragraph 2, the Recipient Party shall not disclose, use, or permit the disclosure or use of any Classified Information without the written consent of the Originating Party except for the purposes, and within any limitations, stated by or on behalf of the Originating Party.
2. Within the scope of its national law and regulations the Recipient Party shall take all steps legally available to it to keep Classified Information transmitted to it by the Originating Party free from disclosure under any applicable law. If there is any request to declassify or disclose any Classified Information transmitted under the provisions of this Agreement, the Recipient Party shall immediately notify the Originating Party and both Parties shall consult each other before any decision is taken.

3. Subject to the provisions of paragraphs 1 and 2 the Recipient Party shall not pass to a Government official, Contractor, Contractor's employee or any other person holding the nationality of any third country, or to any international organisation, any Classified Information, supplied under the provisions of this Agreement.

ARTICLE 6

PROTECTION OF CLASSIFIED INFORMATION

1. The Originating Party shall ensure that the Recipient Party is informed of:
 - 1) The classification of the information and of any conditions of release or limitations on its use;
 - 2) Any subsequent change in classification.
2. The Recipient Party shall, in accordance with its national law and regulations:
 - 1) Afford information received from the other Party a level of security protection that is afforded to Classified Information of an equivalent classification originated by the Recipient Party;
 - 2) Ensure that Classified Information is marked with its own equivalent classification in accordance with Article 3 paragraph 1;
 - 3) Ensure that classifications are not altered, except as authorised in writing by or on behalf of the Originating Party.
3. In order to achieve and maintain comparable standards of security, each National Security Authority shall, on request, provide to the other information about its security standards, procedures and practices for the safeguarding of Classified Information, and shall for this purpose facilitate visits by the relevant Security Authorities.

ARTICLE 7
ACCESS TO CLASSIFIED INFORMATION

Access to Classified Information shall be limited to those persons who have a “need to know”, and who have been security cleared, in accordance with their national law and regulations, to the level appropriate to the classification of the information to be accessed.

ARTICLE 8
TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information at the POUFNE / UK CONFIDENTIAL and the TAJNE / UK SECRET levels shall be transmitted between the two countries in accordance with the national law and regulations of the Originating Party. The normal route shall be through diplomatic channels, but other arrangements may be established if mutually acceptable to the respective Competent Security Authorities.
2. Classified Information at the ZASTRZEŻONE / UK RESTRICTED level shall be transmitted in accordance with the national law and regulations of the Originating Party.

ARTICLE 9
REPRODUCTION, TRANSLATION AND DESTRUCTION
OF CLASSIFIED INFORMATION

1. The Recipient Party shall only reproduce Classified Information in accordance with its national law and regulations. Any reproduced information shall be given the same protection as the originals. The number of copies shall be limited to the minimum required for official purposes.

2. Any translation of Classified Information shall be made by appropriately security cleared individuals and shall be marked with the same classification as the original.
3. When no longer required, Classified Information shall be destroyed in accordance with the national law and regulations of the Recipient Party, in such a manner as to prevent its partial or total reconstruction.
4. The Originating Party may prohibit the making of copies, alterations or destruction of Classified Information by giving it an appropriate marking or by attaching written notice. In such cases, the Classified Information shall be returned to the Originating Party when no longer required.

ARTICLE 10

VISITS

1. The prior approval of the Competent Security Authority of the host country shall be required in respect of visitors, including those on detached duty from the other country, where access is required to Classified Information or to establishments engaged in classified work. Requests for such visits shall be submitted through the respective Competent Security Authority.
2. All visitors shall comply with the security regulations of the host country.
3. In cases involving a specific project or a particular Contract it may, subject to the approval of both Parties, be possible to establish recurring visitors lists. These lists shall be valid for an initial period not exceeding 12 months and may be extended for further periods of time, not to exceed 12 months, subject to the prior approval of the Competent Security Authorities. These lists shall be submitted in accordance with the normal procedures of the Recipient Party. Once a list has been approved, visit arrangements may be made directly between the establishments or companies involved in respect of listed individuals.

4. Any Classified Information which may be provided to, or come to the notice of, visiting personnel, shall be treated by them as if such information has been provided in accordance with the provisions of this Agreement.
5. The Competent Security Authority of the Originating Party shall notify the Competent Security Authority of the Recipient Party of visitors at least twenty five days prior to the planned visit. In exceptional circumstances, security approval of the visit shall be granted as soon as possible, subject to prior co-ordination.
6. Visit applications shall include at least the following information:
 - 1) Name of visitor, date and place of birth, nationality and passport or ID card number;
 - 2) Official title of the visitor and the name of the establishment or organisation the visitor represents;
 - 3) Security clearance of the visitor;
 - 4) Dates and duration of visit;
 - 5) Purpose of visit;
 - 6) Names of establishments and organisations to be visited;
 - 7) Names of persons to be visited.
7. Visits relating to Classified Information at the ZASTRZEŻONE / UK RESTRICTED level shall be arranged directly between the sending establishment and the establishment to be visited.

ARTICLE 11

CLASSIFIED CONTRACTS

1. When proposing to place, or authorising a Contractor in its country to place, a Contract involving Classified Information at the POUFNE / UK CONFIDENTIAL level or above with a Contractor in the other country, the Originating Party shall obtain prior assurance from the Competent Security Authority of the other country that the proposed Contractor is security cleared

- to the appropriate level, and also has suitable security safeguards to provide adequate protection for Classified Information. The assurance shall carry a responsibility that the security measures applied by the cleared Contractor shall be in accordance with national law and regulations and monitored by his Competent Security Authority.
2. Contracts placed as a consequence of these pre-contract enquiries shall contain a security requirement clause incorporating at least the following provisions:
 - 1) The definition of the term “Classified Information” and the equivalent levels of security classification of the Parties in accordance with Article 3 paragraph 1;
 - 2) The names of the Competent Security Authorities of the Parties empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Contract;
 - 3) The channels to be used for the transmission of the Classified Information;
 - 4) The procedures and mechanisms for communicating any changes that may arise in respect of Classified Information either because of changes in its security classification or because protection is no longer necessary;
 - 5) The procedures for the approval of visits, access or inspection by personnel of one Party to a Contractor of the other Party which are covered by the Contract.
 3. The Competent Security Authority of the Originating Party shall pass a copy of the relevant parts of the Classified Contract to the relevant Competent Security Authority of the Recipient Party to allow adequate security monitoring.
 4. Each Contract shall include guidance on the security requirements and on the classification of each aspect of the Contract. In the Republic of Poland this guidance shall be set out in the Industrial Security Instruction. In the United Kingdom of Great Britain and Northern Ireland the guidance shall be

contained in specific security clauses and in a Security Aspects Letter. The guidance must identify each classified aspect of the Contract, or any classified aspect which is to be generated in the course of the Contract, and allocate to it a specific security classification. Changes in the requirements or to the classified aspects shall be notified when necessary and the Originating Party shall notify the Recipient Party when all or any of the information has been downgraded or declassified.

ARTICLE 12

RECIPROCAL SECURITY ARRANGEMENTS

1. When requested, each Competent Security Authority shall advise on the security status of a Contractor in its own country or the security clearance status of one of its nationals. These notifications shall be known as Facility Security Clearance and Personnel Security Clearance assurances respectively.
2. When requested, the Competent Security Authority shall establish the security clearance status of the Contractor or individual which is the subject of the enquiry and forward a security clearance assurance if the Contractor or individual is already cleared. If the Contractor or individual does not have a security clearance, or the clearance is at a lower security level than that which has been requested, notification shall be sent that the security clearance assurance cannot be issued immediately, but that action is being taken to process the request. Following successful enquiries an assurance of Facility Security Clearance or Personnel Security Clearance shall be provided. A Facility Security Clearance is not required for information at the ZASTRZEŻONE / UK RESTRICTED level.
3. If a Contractor is considered by the Competent Security Authority in the country in which it is registered to be ineligible for a Facility Security Clearance assurance the requesting Competent Security Authority shall be notified.

4. If either Competent Security Authority learns of any adverse information about a Contractor or individual for which or for whom a Facility Security Clearance or a Personnel Security Clearance assurance has been issued, it shall notify the other Competent Security Authority of the nature of the information and the action it intends to take, or has taken. Either Competent Security Authority may request a review of any Facility Security Clearance or Personnel Security Clearance which has been furnished earlier by the other Competent Security Authority, provided that the request is accompanied by the reasons. The requesting Competent Security Authority shall be notified of the results of the review and any subsequent action taken.
5. If either Competent Security Authority suspends or takes action to revoke a reciprocal Personnel Security Clearance, or suspends or takes action to revoke access which has been granted to a national of the other country based upon a security clearance, the other Party shall be notified and given the reasons for such an action.

ARTICLE 13

BREACHES OF SECURITY

1. In the event of a security infringement involving the loss of Classified Information or suspicion that Classified Information received from the other Party has been disclosed to unauthorised persons, the Competent Security Authority of the Recipient Party shall immediately inform the Competent Security Authority of the Originating Party.
2. An immediate investigation shall be carried out by the Recipient Party in accordance with national law and regulations and with the assistance of the Originating Party if necessary. The Recipient Party shall inform the Originating Party about the circumstances, the outcome of the investigation and measures adopted to prevent a recurrence, as soon as possible.

ARTICLE 14**COSTS**

Each Party shall bear any expenses it incurs from the implementation and enforcement of this Agreement.

ARTICLE 15**SETTLEMENT OF DISPUTES**

Any dispute relating to the interpretation or the application of this Agreement shall be settled exclusively by consultation between the Parties and shall not be referred to any national or international tribunal for settlement.

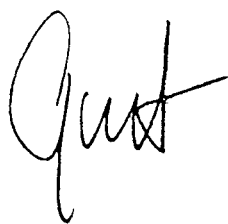
ARTICLE 16**FINAL PROVISIONS**

1. Each of the Parties shall notify the other through diplomatic channels once the internal procedures required in order to bring this Agreement into force have been completed. This Agreement shall come into force on the first day of the second month following the day of receipt of the second notification.
2. This Agreement is concluded for an unlimited period of time. It may be amended at any time, in writing, by mutual consent of the Parties. Amendments shall enter into force under the conditions laid down in paragraph 1.
3. This Agreement may be terminated by either Party upon giving notice to the other Party. In such case, this Agreement shall expire six months after the receipt of the termination notice. In the event of its termination, all items of Classified Information transmitted or generated on the basis of this Agreement shall continue to be treated in accordance with the provisions hereof.

In witness whereof the undersigned, being duly authorised by their respective Governments, have signed this Agreement.

Done in Warsaw on 18 August 2006 in duplicate in the Polish and English languages, both texts being equally authentic.

**FOR THE GOVERNMENT
OF THE REPUBLIC OF POLAND**



**Marek Pasionek
Under-Secretary of State
in the Chancellery
of the Prime Minister**

**FOR THE GOVERNMENT
OF THE UNITED KINGDOM OF
GREAT BRITAIN AND NORTHERN
IRELAND**



**Patrick Davies
Chargé d'Affaires
British Embassy**

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 6 marca 2007 r.

Prezes Rady Ministrów: *J. Kaczyński*

L.S. Prezydent Rzeczypospolitej Polskiej: *L. Kaczyński*