DEFENSE

Security of Information

Agreement between
the UNITED STATES OF AMERICA
and POLAND

Signed at Warsaw March 8, 2007

NOTE BY THE DEPARTMENT OF STATE

Pursuant to Public Law 89—497, approved July 8, 1966 (80 Stat. 271; 1 U.S.C. 113)—

". . .the Treaties and Other International Acts Series issued under the authority of the Secretary of State shall be competent evidence . . . of the treaties, international agreements other than treaties, and proclamations by the President of such treaties and international agreements other than treaties, as the case may be, therein contained, in all the courts of law and equity and of maritime jurisdiction, and in all the tribunals and public offices of the United States, and of the several States, without any further proof or authentication thereof."

POLAND

Defense: Security of Information

Agreement signed at Warsaw March 8, 2007;
Entered into force October 9, 2007.

AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED STATES OF AMERICA AND THE GOVERNMENT OF THE REPUBLIC OF POLAND CONCERNING SECURITY MEASURES FOR THE PROTECTION OF CLASSIFIED INFORMATION IN THE MILITARY SPHERE

The Government of the United States of America and the Government of the Republic of Poland hereinafter referred to as Parties,

In furtherance of mutual cooperation to ensure the protection of classified information in the military sphere,

Have agreed as follows:

CHAPTER I
DEFINITIONS

ARTICLE 1

For the purposes of this Agreement:

1) Classified Information in the Military Sphere	Information that is generated by or for the Department of Defense of the United States of America (in the United States referred to as "Classified Military Information"), or the Ministry of National Defense of the Republic of Poland, or that is under their jurisdiction or control, and which requires protection according to the internal laws and regulations of the Parties and the provisions of this Agreement, hereinafter referred to as "Classified Information".
2) National Security Authority	The national authority of each Party responsible for the security of Classified Information as described in this Agreement.
3) Contract	An agreement regulating enforceable rights and obligations under internal laws and regulations between the bodies concluding the agreement, performance of which involves access to Classified Information or origination of such information.
4) Contracting Agency	The entity within the government organization of a Party, which has authority to enter into, administer, or terminate contracts.
5) Contractor	Any entity awarded a Contract by a Party's Contracting Agency.
6) Third Party	A government other than the government of a Party and any person or other entity whose government is not the government of a Party.

CHAPTER II
APPLICABILITY

ARTICLE 2

Classified Information provided directly or indirectly by one Party to the other Party, or to an officer or other authorized representative of the Parties, shall be protected according to the terms set forth herein and in accordance with the internal laws and regulations of the Parties.

ARTICLE 3

Each Party shall promptly notify the other of any changes to its internal laws and regulations that would affect the protection of Classified Information under this Agreement. In such case, the Parties shall consult as provided for in Chapter XIII, to consider possible changes to this Agreement. In the interim, Classified Information shall continue to be protected as described herein.

ARTICLE 4

1. Classified Information may be in oral, visual, or documentary form, or any other form including equipment or technology.

2. Classified Information is granted a security classification level in accordance to its content, pursuant to the internal laws and regulations of each Party. Each Party shall stamp or mark the name of the originating government on all Classified Information received from the other Party. The information shall be marked with a national security classification marking of the recipient Party that will afford a degree of protection equivalent to that afforded it by the originating Party.

3. The Parties agree that the following security classification levels are equivalent:

United States of America	Republic of Poland
TOP SECRET	ŚCIŚLE TAJNE
SECRET	TAJNE
CONFIDENTIAL	POUFNE
No U.S. equivalent; shall be protected as CONFIDENTIAL	ZASTRZEŻONE

CHAPTER III
NATIONAL SECURITY AUTHORITIES

ARTICLE 5

1. For the purpose of this Agreement, the National Security Authorities shall be:

1) for the United States of America: the Department of Defense;

2) for the Republic of Poland: the Head of the Internal Security Agency and the Head of the Military Counterintelligence Service.

2. The National Security Authorities may conclude supplemental implementing arrangements to this Agreement.

3. The Parties agree to notify each other regarding any changes to their National Security Authorities or their responsibilities under this Agreement.

CHAPTER IV
ACCESS TO CLASSIFIED INFORMATION

ARTICLE 6

Access to Classified Information shall be granted only to those persons who have a need-to-know, whose official duties require such access and who have been granted a personnel security clearance in accordance with the prescribed standards of the Parties, and have been briefed in the scope of Classified Information protection according to the internal laws and regulations of each Party. No individual shall be entitled access to the information solely by virtue of rank, appointment, or security clearance. The Parties shall ensure that:

1) the recipient Party will not release the information to a Third Party without the written approval of the originating Party;

2) the recipient Party will afford the information a degree of protection equivalent to that afforded it by the originating Party pursuant to Article 4, paragraph 3;

3) the recipient Party will not use the information for other than the purpose for which it was provided;

4) the recipient Party shall respect and protect private rights, such as patents, copyrights, or other rights which are involved in the information, and

5) all facilities that handle Classified Information will maintain a registry of the clearance of individuals at these facilities who are authorized to have access to such information.

CHAPTER V
PERSONNEL SECURITY

ARTICLE 7

The determination on the granting of a personnel security clearance to an individual shall be consistent with the interests of national security and shall be based upon an investigation in accordance with the internal laws and regulations of the granting Party to determine if the individual possesses the capability and intent to properly handle Classified Information.

ARTICLE 8

Before a representative of a Party releases Classified Information to an officer or authorized representative of the other Party, the receiving Party shall provide to the originating Party an assurance that the officer or the representative possesses the necessary level of security clearance and requires access for official purposes and that the information will be protected by the receiving Party.

CHAPTER VI
VISITS

ARTICLE 9

Authorizations for visits by representatives of one Party to facilities of the other Party, where access to Classified Information is required, shall be limited to those necessary for official purposes and shall be transmitted sufficiently in advance. Authorizations to visit the facilities shall be granted only by the Parties or government officials designated by the Parties. The Parties or their designee shall be responsible for notification of the proposed visit, and the scope and highest level of Classified Information that may be furnished to the visitor. Requests for visits by representatives of the Parties shall be submitted through the Embassy of the United States of America in Warsaw, in the case of United States visitors and through the Embassy of the Republic of Poland in Washington, D.C., in the case of Polish visitors. Requests for a visit shall include:

1) purpose and date of the visit, and associated program (if applicable);

2) name and surname of the visitor, date and place of birth, nationality, passport number or identity card number;

3) position of the visitor together with the name of the institution or facility which he or she represents;

4) certification of the level of Personnel Security Clearance held by the visitor;

5) name and address of the facility to be visited, and

6) name, surname and position of the person to be visited.

CHAPTER VII
PHYSICAL SECURITY

ARTICLE 10

The Parties shall be responsible for all Classified Information of the other Party during transmission or storage within their territory.

ARTICLE 11

The Parties shall be responsible for the security of all facilities where Classified Information of the other Party is kept and shall assure that qualified individuals are appointed for each such facility who shall have the responsibility and authority for the control and protection of the information.

ARTICLE 12

Classified Information shall be stored in a manner that assures access only by those individuals who have been authorized access pursuant to Chapter IV and Chapter V.

CHAPTER VIII
MARKING AND TRANSMISSION OF CLASSIFIED INFORMATION

ARTICLE 13

1. Classified Information shall be transmitted between the Parties through government-to-government channels. Each Party shall stamp or mark the name of the originating government on all Classified Information received from the other Party. The information shall be marked with a national security classification marking of the recipient Party that will afford a degree of protection equivalent to that afforded it by the originating Party, pursuant to Article 4, paragraph 3.

2. The minimum requirements for the security of Classified Information during transmission shall be as follows:

1) documents or other media containing Classified Information shall be transmitted in double, sealed envelopes, the innermost envelope bearing only the classification of the documents or other media and the organizational address of the intended recipient, and an outer envelope bearing the organizational address of the recipient, the organizational address of the sender, and the registry number if applicable. No indication of the classification of the enclosed documents or other media shall be on the outer envelope. The sealed envelope shall then be transmitted according to the prescribed procedures of the Parties. Receipts shall be prepared for packages containing classified documents or other media that are transmitted between the Parties, and a receipt for the enclosed documents or media shall be signed by the final recipient and returned to the sender;

2) classified equipment shall be transported in sealed covered vehicles, or be securely packaged or protected in order to prevent identification of its details, and kept under continuous control to prevent access by unauthorized persons;

3) classified equipment which must be stored temporarily awaiting shipment shall be placed in protected storage areas. The area shall be protected by intrusion-detection equipment or guards with security clearances who shall maintain continuous surveillance of the storage area. Only authorized personnel with the requisite security clearance shall have access to the storage area;

4) receipts shall be obtained on every occasion when classified equipment changes hands en route; and, a receipt shall be signed by the final recipient and returned to the sender, and

5) Classified Information may be transmitted via protected systems and IT networks, which have been authorized for such use according to the internal laws and regulations of the Parties. Classified Information transmitted by electronic means shall be encrypted.

CHAPTER IX
DESTRUCTION, REPRODUCTION AND TRANSLATION

ARTICLE 14

Classified documents and other media containing Classified Information shall be destroyed in a manner that prevents reconstruction of the Classified Information contained therein.

ARTICLE 15

Classified equipment shall be destroyed beyond recognition or modified so as to preclude reconstruction of the Classified Iinformation in whole or in part.

ARTICLE 16

Classified Information classified as TOP SECRET or SECRET that may not be reproduced shall bear a restrictive marking according to the internal laws and regulations of the originating Party.

ARTICLE 17

When a classified document or other media are reproduced, all original security markings thereon also shall be reproduced or marked on each copy. Such reproduced documents or media shall be placed under the same controls as the original document or media. The number of copies shall be limited to that required for official purposes.

ARTICLE 18

All translations of Classified Information shall be made by individuals with security clearances pursuant to Chapter V. The number of copies shall be kept to a minimum and the distribution thereof shall be controlled. Such translations shall bear appropriate security classification markings and a suitable notation in the language into which it is translated, indicating that the document or media contains Classified Information of the originating Party.

CHAPTER X
RELEASE TO CONTRACTORS

ARTICLE 19

Prior to the release to a Contractor or prospective Contractor of any Classified Information received from the other Party, the recipient Party shall ensure that:

1) such Contractor or prospective Contractor and the contractor's facility have the capability to protect the Classified Information;

2) the appropriate facility security clearance has been granted;

3) appropriate personnel security clearances for all individuals whose duties require access to Classified Information have been granted;

4) all individuals having access to Classified Information are informed of their responsibilities to protect the Classified Information in accordance with applicable laws and regulations of the Parties;

5) periodic security inspections of cleared facilities are carried out to ensure that Classified Information is protected as required herein, and

6) access to Classified Information is limited to those persons who have a need-to-know for official purposes.

CHAPTER XI
ACCOUNTABILITY AND CONTROL

ARTICLE 20

1. The Parties shall ensure necessary accountability and control over Classified Information.

2. In accordance with this Agreement and their internal laws and regulations, the Parties shall adopt appropriate measures aimed at protection of Classified Information which is transmitted or originated as a result of mutual cooperation of both Parties, including Classified Information originated in connection with performance of a contract.

CHAPTER XII
ACTION IN THE EVENT OF LOSS OR UNAUTHORIZED DISCLOSURE OR POSSIBLE LOSS OR UNAUTHORIZED DISCLOSURE

ARTICLE 21

The originating Party shall be informed immediately of all losses or unauthorized disclosures, as well as possible losses or unauthorized disclosures, of its Classified Information, and the recipient Party shall initiate an inquiry and if warranted further investigation to determine the circumstances. The results of such inquiry or investigation and information regarding measures taken to prevent recurrence shall be forwarded to the originating Party by the Party that conducts the inquiry or investigation.

CHAPTER XIII
CONSULTATIONS AND REVIEW OF SECURITY PROCEDURES

ARTICLE 22

1. The National Security Authorities of the Parties shall notify each other of any amendments to their internal laws and regulations concerning the protection of Classified Information.

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

3. Implementation of the foregoing security requirements can be advanced through reciprocal visits by representatives of the National Security Authorities of the Parties. Accordingly, these representatives, after prior consultations, shall be permitted to visit the other Party, to discuss, and view firsthand, the implementing procedures of the other Party in the interest of achieving comparable security procedures. Each Party shall assist the other Party's National Security Authority representatives in determining whether Classified Information provided by the other Party is being adequately protected.

CHAPTER XIV
COSTS

ARTICLE 23

Each Party shall cover its own expenses resulting from the implementation of this Agreement.

CHAPTER XV
SETTLEMENT OF DISPUTES

ARTICLE 24

1. Any disputes concerning this Agreement shall be settled by direct negotiations between the National Security Authorities.

2. If the settlement of a dispute cannot be reached in the manner referred to in Paragraph 1, such dispute shall be settled through diplomatic channels and shall not be referred to a national court, international tribunal, or to any other person or entity for settlement.

CHAPTER XVI
FINAL PROVISIONS

ARTICLE 25

1. Upon this Agreement entering into force, the Agreement between the Government of the United States of America and the Government of the Republic of Poland on the protection of Classified Military Information done in Washington D.C., February 17, 1995 (hereinafter referred to as "1995 Agreement"), shall be superceded.

2. Classified Information that was previously exchanged by the Parties and to which the 1995 Agreement applied, shall be covered by this Agreement.

ARTICLE 26

1. This Agreement shall enter into force on the date of the later note exchanged by the Parties informing each other of the completion of all their internal processes necessary to bring the Agreement into force.

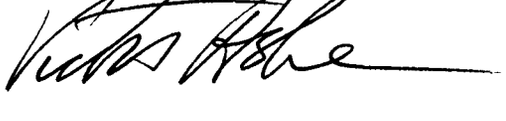
2. Amendments to the present Agreement shall be made by mutual consent of the Parties and shall enter into force in accordance with the provisions of Paragraph 1.

3. This Agreement shall remain in force for a period of five years and shall be automatically renewed for consecutive one year periods, unless either Party notifies the other in writing through diplomatic channels, ninety days in advance, of its intention to terminate the Agreement.

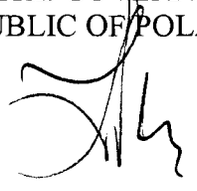
4. Not withstanding the termination of this Agreement, all Classified Information provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

DONE at Warsaw this 8th day of March, 2007, in the English and Polish languages, both texts being equally authentic.

FOR THE GOVERNMENT OF
THE UNITED STATES OF AMERICA:



FOR THE GOVERNMENT OF THE
REPUBLIC OF POLAND:



UMOWA MIĘDZY RZĄDEM STANÓW ZJEDNOCZONYCH AMERYKI A RZĄDEM RZECZYPOSPOLITEJ POLSKIEJ W SPRAWIE ŚRODKÓW BEZPIECZEŃSTWA SŁUŻĄCYCH OCHRONIE INFORMACJI NIEJAWNYCH W SFERZE WOJSKOWEJ

Rząd Stanów Zjednoczonych Ameryki oraz Rząd Rzeczypospolitej Polskiej, zwane dalej Stronami,

popierając wzajemną współpracę w celu zapewnienia ochrony informacji niejawnych w sferze wojskowej,

uzgodniły, co następuje:

ROZDZIAŁ I
DEFINICJE

ARTYKUŁ 1

W rozumieniu niniejszej Umowy:

1) Informacje niejawne w sferze wojskowej	Informacje wytworzone przez lub dla Departamentu Obrony Stanów Zjednoczonych Ameryki (w Stanach Zjednoczonych zwane „wojskowymi informacjami niejawnymi") lub Ministerstwa Obrony Narodowej Rzeczypospolitej Polskiej, lub informacje, które znajdują się pod ich jurysdykcją bądź kontrolą i które wymagają ochrony zgodnie z prawem krajowym Stron oraz postanowieniami niniejszej Umowy, zwane dalej „informacjami niejawnymi";
2) Krajowa władza bezpieczeństwa	Krajowa władza każdej ze Stron odpowiedzialna za bezpieczeństwo informacji niejawnych zgodnie z postanowieniami niniejszej Umowy;
3) Kontrakt	Umowa regulująca ciążące na zawierających ją podmiotach prawa i obowiązki zgodnie z prawem krajowym, której realizacja wiąże się z dostępem do lub wytwarzaniem informacji niejawnych;
4) Agencja do spraw kontraktów	Podmiot funkcjonujący w ramach struktur rządowych Strony, który posiada uprawnienia do zawierania, zarządzania oraz wypowiadania kontraktów;
5) Kontrahent	Podmiot, któremu przyznano kontrakt przez agencję do spraw kontraktów jednej ze Stron;
6) Strona trzecia	Rząd, nie będący rządem żadnej ze Stron niniejszej Umowy oraz osoba lub inny podmiot, których rząd nie jest rządem żadnej ze Stron niniejszej Umowy.

ROZDZIAŁ II
ZASTOSOWANIE

ARTYKUŁ 2

Informacje niejawne przekazywane bezpośrednio lub pośrednio przez jedną Stronę drugiej Stronie, lub oficerowi bądź innemu upoważnionemu przedstawicielowi Stron, są chronione zgodnie z warunkami niniejszej Umowy oraz prawem krajowym Stron.

ARTYKUŁ 3

Każda ze Stron powiadamia bezzwłocznie drugą Stronę o wszelkich zmianach w swoim prawie krajowym mających wpływ na zgodną z postanowieniami niniejszej Umowy ochronę informacji niejawnych. W takim przypadku, Strony konsultują się, zgodnie z postanowieniami rozdziału XIII, w celu rozważenia wprowadzenia ewentualnych zmian do niniejszej Umowy. W międzyczasie, informacje niejawne są chronione zgodnie z postanowieniami niniejszej Umowy.

ARTYKUŁ 4

1. Informacje niejawne mogą mieć formę ustną, wizualną lub formę dokumentu, lub każdą inną, w tym także formę sprzętu lub technologii.

2. Informacjom niejawnym przyznaje się adekwatną do ich treści klauzulę tajności, zgodnie z prawem krajowym każdej ze Stron. Każda ze Stron opieczętowuje lub oznacza wszystkie informacje niejawne otrzymane od drugiej Strony nazwą rządu Strony wytwarzającej. Informacje są oznaczane klauzulami tajności Strony otrzymującej w celu zapewnienia poziomu ochrony odpowiadającego określonemu przez Stronę wytwarzającą.

3. Strony uzgadniają, że niżej wymienione klauzule tajności są równorzędne:

STANY ZJEDNOCZONE AMERYKI	RZECZPOSPOLITA POLSKA
TOP SECRET	ŚCIŚLE TAJNE
SECRET	TAJNE
CONFIDENTIAL	POUFNE
brak amerykańskiego odpowiednika; traktowane jak POUFNE	ZASTRZEŻONE

ROZDZIAŁ III
KRAJOWE WŁADZE BEZPIECZEŃSTWA

ARTYKUŁ 5

1. Krajowymi władzami bezpieczeństwa w rozumieniu niniejszej Umowy są:

1) w Stanach Zjednoczonych Ameryki: Departament Obrony;

2) w Rzeczypospolitej Polskiej: Szef Agencji Bezpieczeństwa Wewnętrznego oraz Szef Służby Kontrwywiadu Wojskowego.

2. Krajowe władze bezpieczeństwa mogą zawierać dodatkowe porozumienia wykonawcze do niniejszej Umowy.

3. Strony informują się o wszelkich zmianach w swoich krajowych władzach bezpieczeństwa lub zakresie ich odpowiedzialności wynikającym z postanowień niniejszej Umowy.

ROZDZIAŁ IV
DOSTĘP DO INFORMACJI NIEJAWNYCH

ARTYKUŁ 6

Na dostęp do informacji niejawnych zezwala się, zgodnie z zasadą ograniczonego dostępu, tylko tym osobom, których zadania służbowe wymagają zapoznania się z nimi, które posiadają poświadczenie bezpieczeństwa wydane zgodnie z określonymi wymaganiami Stron, oraz które zostały przeszkolone w zakresie ochrony informacji niejawnych zgodnie z prawem krajowym każdej ze Stron. Stopień, stanowisko służbowe lub posiadanie poświadczenia bezpieczeństwa nie są wystarczającymi przesłankami na uzyskanie dostępu do informacji niejawnych. Strony zapewniają, że:

1) Strona otrzymująca nie przekaże informacji stronie trzeciej bez pisemnej zgody Strony wytwarzającej;

2) Strona otrzymująca zapewni informacjom poziom ochrony odpowiadający określonemu przez Stronę wytwarzającą, zgodnie z postanowieniami artykułu 4 ustęp 3;

3) Strona otrzymująca będzie wykorzystywać informacje wyłącznie w celu, w jakim zostały one przekazane;

4) Strona otrzymująca będzie respektować i chronić prawa osobiste, takie jak patenty, prawa autorskie lub inne prawa, które stanowią część informacji, oraz

5) wszystkie jednostki, w których wykorzystywane są informacje niejawne będą prowadziły rejestr osób posiadających poświadczenia bezpieczeństwa, które w danych jednostkach są uprawnione do dostępu do takich informacji.

ROZDZIAŁ V
BEZPIECZEŃSTWO OSOBOWE

ARTYKUŁ 7

Postanowienie o wydaniu poświadczenia bezpieczeństwa osobie fizycznej pozostaje w zgodzie z interesami bezpieczeństwa narodowego i jest możliwe po przeprowadzeniu postępowania sprawdzającego zgodnie z prawem krajowym Strony wydającej. Celem postępowania sprawdzającego jest ocena zdolności i intencji osoby fizycznej do właściwego wykorzystywania informacji niejawnych.

ARTYKUŁ 8

Zanim przedstawiciel jednej ze Stron udostępni informacje niejawne oficerowi lub uprawnionemu przedstawicielowi drugiej Strony, Strona otrzymująca udzieli Stronie przekazującej zapewnienia, że dany oficer lub przedstawiciel posiada wymagane poświadczenie bezpieczeństwa, potrzebuje dostępu do informacji niejawnych w celach służbowych oraz że informacje będą chronione przez Stronę otrzymującą.

ROZDZIAŁ VI
WIZYTY

ARTYKUŁ 9

Upoważnienia do składania wizyt przez przedstawicieli jednej Strony w obiektach należących do drugiej Strony, w których wymagany jest dostęp do informacji niejawnych, są ograniczone wyłącznie do wizyt służbowych i przekazywane ze stosownym wyprzedzeniem. Upoważnienia do składania wizyt w obiektach udzielają wyłącznie Strony lub urzędnicy rządowi wyznaczeni przez Strony. Strony lub osoby przez nie wyznaczone są odpowiedzialne za uprzedzenie o proponowanej wizycie oraz zakresie i najwyższej klauzuli informacji niejawnych, do jakich może mieć dostęp osoba przybywająca z wizytą. Wnioski o wizyty przedstawicieli Stron są przekazywane przez Ambasadę Stanów Zjednoczonych Ameryki w Warszawie, w przypadku osób przybywających na wizytę ze Stanów Zjednoczonych oraz przez Ambasadę Rzeczypospolitej Polskiej w Waszyngtonie D.C., w przypadku osób przybywających na wizytę z Polski . Wnioski o wizytę zawierają:

1) cel oraz termin wizyty wraz z załączonym programem (w przypadku, kiedy ma zastosowanie);

2) imię i nazwisko osoby przybywającej z wizytą, datę oraz miejsce urodzenia, obywatelstwo, numer paszportu lub innego dowodu tożsamości;

3) stanowisko służbowe osoby przybywającej z wizytą wraz z nazwą instytucji lub jednostki, którą reprezentuje;

4) potwierdzenie poziomu poświadczenia bezpieczeństwa osoby przybywającej z wizytą;

5) nazwę oraz adres odwiedzanego obiektu, oraz

6) imię, nazwisko oraz stanowisko służbowe osoby odwiedzanej.

ROZDZIAŁ VII
BEZPIECZEŃSTWO FIZYCZNE

ARTYKUŁ 10

Strony są odpowiedzialne za wszystkie informacje niejawne drugiej Strony podczas ich przekazywania, bądź przechowywania na swoim terytorium.

ARTYKUŁ 11

Strony są odpowiedzialne za bezpieczeństwo wszystkich obiektów, w których przechowywane są informacje niejawne przekazane przez drugą Stronę oraz zapewniają wyznaczenie do każdego takiego obiektu wykwalifikowanych osób, które będą odpowiedzialne i uprawnione do kontroli i ochrony tych informacji.

ARTYKUŁ 12

Informacje niejawne są przechowywane w taki sposób, aby dostęp do nich był ograniczony wyłącznie do osób posiadających uprawnienia, o których mowa w rozdziale IV i rozdziale V.

ROZDZIAŁ VIII
OZNACZANIE I PRZEKAZYWANIE INFORMACJI NIEJAWNYCH

ARTYKUŁ 13

1. Informacje niejawne są przekazywane między Stronami drogą rządową. Każda ze Stron ostemplowuje lub oznacza wszystkie informacje niejawne otrzymane od drugiej Strony nazwą rządu Strony wytwarzającej. Informacje są oznaczane zgodnie z klasyfikacją Strony otrzymującej, umożliwiając w ten sposób zapewnienie poziomu ochrony określonego przez Stronę wytwarzającą, zgodnie z postanowieniami artykułu 4 ustęp 3.

2. Minimalne wymagania dotyczące bezpieczeństwa informacji niejawnych podczas przekazywania przedstawiają się następująco:

1) dokumenty lub inne nośniki zawierające informacje niejawne są przekazywane w podwójnych, zapieczętowanych kopertach, przy czym na kopercie wewnętrznej znajduje się jedynie klauzula tajności, którą oznaczono dokumenty lub inne nośniki oraz służbowy adres docelowego odbiorcy, natomiast na kopercie zewnętrznej znajduje się służbowy adres odbiorcy, służbowy adres nadawcy oraz numer, pod którym zarejestrowany został dany dokument lub inny nośnik w przypadku, kiedy ma to zastosowanie. Na kopercie zewnętrznej nie umieszcza się informacji o klauzuli tajności załączonych dokumentów lub innych nośników. Zapieczętowana koperta jest następnie przekazywana zgodnie z procedurami obowiązującymi daną Stronę. W przypadku paczek zawierających niejawne dokumenty lub inne nośniki przekazywane między Stronami, przygotowuje się potwierdzenia odbioru. Odbiór załączonych dokumentów lub innych nośników jest potwierdzany pisemnie przez ostatniego odbiorcę i przekazywany nadawcy;

2) sprzęt objęty klauzulą tajności jest transportowany w zapieczętowanych, zakrytych pojazdach, lub bezpiecznie pakowany bądź zabezpieczany w celu uniemożliwienia jego szczegółowej identyfikacji. Znajduje się on także pod stałą kontrolą w celu uniemożliwienia dostępu osobom nieupoważnionym;

3) sprzęt objęty klauzulą tajności, który musi być tymczasowo przechowywany w oczekiwaniu na wysłanie, umieszcza się w miejscu objętym ochroną. Miejsce to jest chronione za pomocą urządzeń zabezpieczających przed wtargnięciem osób trzecich lub pracowników ochrony posiadających poświadczenia bezpieczeństwa prowadzących stały nadzór. Dostęp do takiego miejsca mogą mieć wyłącznie członkowie upoważnionego personelu posiadający wymagane poświadczenia bezpieczeństwa;

4) w przypadku, kiedy podczas transportu zmieniają się osoby odpowiedzialne za sprzęt objęty klauzulą tajności, należy każdorazowo wystawiać potwierdzenie, które jest później podpisywane przez ostatniego odbiorcę i przekazywane nadawcy, oraz

5) informacje niejawne mogą być przekazywane za pośrednictwem bezpiecznych systemów i sieci teleinformatycznych dopuszczonych do użytku zgodnie z prawem krajowym Stron. Informacje niejawne przekazywane drogą elektroniczną są szyfrowane.

ROZDZIAŁ IX

NISZCZENIE, POWIELANIE I TŁUMACZENIE

ARTYKUŁ 14

Dokumenty oraz inne nośniki zawierające informacje niejawne są niszczone w sposób uniemożliwiający rekonstrukcję informacji niejawnych w nich zawartych.

ARTYKUŁ 15

Sprzęt objęty klauzulą tajności jest niszczony w sposób uniemożliwiający jego rozpoznanie lub modyfikowany w sposób wykluczający częściową lub całkowitą rekonstrukcję informacji niejawnych.

ARTYKUŁ 16

Informacje niejawne o klauzuli ŚCIŚLE TAJNE lub TAJNE, które nie mogą być powielane są w tym celu odpowiednio oznaczane zgodnie z prawem krajowym Strony wytwarzającej.

ARTYKUŁ 17

W przypadku powielania niejawnych dokumentów lub innych nośników, wszystkie znajdujące się na nich oryginalne klauzule tajności są powielane bądź umieszczane na każdej kopii. Powielone w ten sposób dokumenty lub inne nośniki podlegają takiej samej kontroli, jak oryginały. Liczba kopii jest ograniczona do liczby wymaganej dla celów służbowych.

ARTYKUŁ 18

Wszelkie tłumaczenia informacji niejawnych są dokonywane przez osoby posiadające poświadczenia bezpieczeństwa, zgodnie z postanowieniami rozdziału V. Liczba kopii jest ograniczona do niezbędnego minimum, a ich udostępnianie podlega kontroli. Wykonane w ten sposób tłumaczenia są oznaczane odpowiednią klauzulą tajności oraz odpowiednim oznaczeniem w języku, na który dokonano przekładu, wskazującym, że dokument lub nośnik zawiera informacje niejawne pochodzące od Strony wytwarzającej.

ROZDZIAŁ X

UDOSTĘPNIANIE KONTRAHENTOM

ARTYKUŁ 19

Przed udostępnieniem jakichkolwiek informacji niejawnych otrzymanych od drugiej Strony kontrahentowi lub ewentualnemu kontrahentowi, Strona otrzymująca udziela zapewnienia, że:

1) kontrahent lub ewentualny kontrahent, oraz jego zakład posiadają możliwości ochrony informacji niejawnych;

2) wydane zostało odpowiednie świadectwo bezpieczeństwa przemysłowego;

3) wydane zostały odpowiednie poświadczenia bezpieczeństwa wszystkim osobom fizycznym, których obowiązki wymagają dostępu do informacji niejawnych;

4) wszystkie osoby fizyczne mające dostęp do informacji niejawnych są poinformowane o odpowiedzialności za ochronę informacji niejawnych zgodnie z obowiązującym prawem Stron;

5) przeprowadzane są okresowe inspekcje zakładów, którym wydano świadectwa bezpieczeństwa przemysłowego, w celu zapewnienia, że informacje niejawne są chronione zgodnie z postanowieniami niniejszej Umowy, oraz

6) dostęp do informacji jest ograniczony do tych osób, których zadania służbowe wymagają zapoznania się z nimi.

ROZDZIAŁ XI

EWIDENCJA I KONTROLA

ARTYKUŁ 20

1. Strony zapewniają prowadzenie niezbędnej ewidencji i kontroli informacji niejawnych.

2. Zgodnie z postanowieniami niniejszej Umowy oraz swoim prawem krajowym, Strony stosują odpowiednie środki w celu ochrony informacji niejawnych, które są przekazywane lub powstają w wyniku wspólnej działalności obu Stron, w tym także informacji niejawnych wytworzonych w związku z realizacją kontraktu.

ROZDZIAŁ XII

PROCEDURA W PRZYPADKU UTRATY LUB NIEUPRAWNIONEGO UJAWNIENIA BĄDŹ DOMNIEMANIA UTRATY LUB NIEUPRAWNIONEGO UJAWNIENIA

ARTYKUŁ 21

Strona wytwarzająca jest natychmiast informowana o utracie lub nieuprawnionym ujawnieniu, a także o domniemaniu utraty lub nieuprawnionego ujawnienia należących do niej informacji niejawnych, natomiast Strona otrzymująca rozpoczyna postępowanie wyjaśniające oraz, jeśli jest to zasadne – dochodzenie, w celu wyjaśnienia okoliczności. Wyniki postępowania lub dochodzenia, wraz z informacją na temat środków podjętych w celu uniknięcia powtórzenia się takiej sytuacji, są przekazywane Stronie wytwarzającej przez Stronę przeprowadzającą postępowanie lub dochodzenie.

ROZDZIAŁ XIII
KONSULTACJE I PRZEGLĄD SYSTEMÓW BEZPIECZEŃSTWA

ARTYKUŁ 22

1. Krajowe władze bezpieczeństwa Stron informują się o wszelkich zmianach w swoim prawie krajowym w zakresie dotyczącym ochrony informacji niejawnych.

2. W celu zapewnienia ścisłej współpracy przy realizacji postanowień niniejszej Umowy, krajowe władze bezpieczeństwa Stron konsultują się na wniosek jednej z nich.

3. Realizacja określonych w niniejszej Umowie wymogów bezpieczeństwa może być wspierana poprzez obustronne wizyty przedstawicieli krajowych władz bezpieczeństwa Stron, którzy po wcześniejszych konsultacjach, otrzymają zgodę na złożenie wizyty drugiej Stronie w celu omówienia oraz dokonania bezpośredniego przeglądu realizacji procedur przez drugą Stronę, co pozwoli na uzyskanie porównywalnych systemów bezpieczeństwa. Każda ze Stron pomaga przedstawicielom krajowych władz bezpieczeństwa drugiej Strony w oszacowaniu, czy informacje niejawne przekazane przez drugą Stronę są właściwie chronione.

ROZDZIAŁ XIV
KOSZTY

ARTYKUŁ 23

Każda ze Stron pokrywa swoje własne koszty poniesione w związku z realizacją niniejszej Umowy.

ROZDZIAŁ XV
ROZSTRZYGANIE SPORÓW

ARTYKUŁ 24

1. Wszelkie kwestie sporne dotyczące niniejszej Umowy są rozstrzygane w drodze bezpośrednich negocjacji między krajowymi władzami bezpieczeństwa.

2. Jeżeli rozstrzygnięcie sporu w sposób, o którym mowa w ustępie 1, jest niemożliwe, będzie on rozwiązany drogą dyplomatyczną i nie będzie przedkładany do rozstrzygnięcia sądowi krajowemu, trybunałowi międzynarodowemu, czy też innej osobie lub podmiotowi.

ROZDZIAŁ XVI
POSTANOWIENIA KOŃCOWE

ARTYKUŁ 25

1. Z chwilą wejścia w życie niniejszej Umowy, wygasa Porozumienie między Rządem Stanów Zjednoczonych Ameryki a Rządem Rzeczypospolitej Polskiej w sprawie ochrony wojskowych informacji niejawnych, podpisane w Waszyngtonie D.C. 17 lutego 1995 roku (zwane dalej „Porozumieniem z 1995 roku").

2. Informacje niejawne, które zostały wcześniej wymienione przez Strony na podstawie Porozumienia z 1995 roku, zostają objęte ochroną zgodnie z postanowieniami niniejszej Umowy.

ARTYKUŁ 26

1. Niniejsza Umowa wchodzi w życie z dniem późniejszej z not wymienionych między Stronami informujących o zakończeniu wszystkich procedur wewnętrznych niezbędnych do wejścia Umowy w życie.

2. Zmiany do niniejszej Umowy są wprowadzane na podstawie obustronnej zgody Stron i wchodzą w życie zgodnie z postanowieniami ustępu 1.

3. Niniejsza Umowa zawarta jest na okres pięciu lat, po którym będzie automatycznie przedłużana na kolejne okresy jednoroczne, chyba że którakolwiek ze Stron, poinformuje drugą Stronę o zamiarze wypowiedzenia i dokona tego pisemnie, drogą dyplomatyczną z dziewięćdziesięciodniowym wyprzedzeniem.

4. Bez względu na wypowiedzenie niniejszej Umowy, wszystkie informacje niejawne przekazane na jej podstawie będą nadal chronione zgodnie z jej postanowieniami.

SPORZĄDZONO w Warszawie dnia 8 marca 2007 roku, w językach angielskim i polskim, przy czym obydwa teksty posiadają jednakową moc.

Z UPOWAŻNIENIA RZĄDU STANÓW ZJEDNOCZONYCH AMERYKI	Z UPOWAŻNIENIA RZĄDU RZECZYPOSPOLITEJ POLSKIEJ