

DEFENSE

Protection of Information

**Agreement Between the
UNITED STATES OF AMERICA
and the SLOVAK REPUBLIC**

Signed at Bratislava May 13, 2022

With Appendix

Entered into force May 13, 2022



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.”

AGREEMENT BETWEEN
THE GOVERNMENT OF THE UNITED STATES OF AMERICA
AND
THE GOVERNMENT OF THE SLOVAK REPUBLIC
CONCERNING SECURITY MEASURES FOR THE PROTECTION OF
CLASSIFIED INFORMATION

PREAMBLE

The Government of the United States of America and the Government of the Slovak Republic (hereinafter a “Party,” and collectively the “Parties”);

Considering that the Parties cooperate in matters including, but not limited to, foreign affairs, defense, security, law enforcement, science, industry, and technology; and

Having a mutual interest in the protection of Classified Information exchanged between the Parties;

Have agreed as follows:

ARTICLE 1
DEFINITIONS

For the purpose of this Agreement:

1. Classified Information: Information provided by one Party to the other Party that is designated as classified by the releasing Party for national security purposes and therefore requires protection against unauthorized disclosure. The information may be in oral, visual, electronic, or documentary form, or in the form of material, including equipment or technology.
2. Classified Contract: A contract that requires, or will require, access to, or production of, Classified Information by a Contractor or by its employees in the performance of the contract.
3. Contractor: An individual or a legal entity, possessing the legal capacity to conclude contracts, who is a party to a Classified Contract.
4. Facility Security Clearance (FSC): A certification provided by the National Security Authority of a Party, as designated in Article 4, for a Contractor facility under the Party’s jurisdiction that indicates the facility is cleared to a specified level and also has suitable security safeguards in place at a specified level to protect Classified Information. Such a certification shall signify that Classified Information at the CONFIDENTIAL / DÔVERNÉ level or above shall be protected by the Contractor

for which the FSC is provided in accordance with the provisions of this Agreement and that compliance shall be monitored and enforced by the relevant National Security Authority.

5. Personnel Security Clearance (PSC):

a. A certification by the National Security Authority of a Party, as designated in Article 4 of this Agreement, that an individual who is employed by a government agency of that Party or a Contractor under the jurisdiction of that Party is authorized to access Classified Information up to a specified level.

b. A certification by the National Security Authority of a Party, as designated in Article 4, that an individual who is a citizen of one Party but is to be employed by the other Party or by one of the other Party's Contractors is authorized access to Classified Information up to a specified level.

6. Need-to-Know: A determination made by an authorized holder of Classified Information that a prospective recipient of Classified Information requires access to specific Classified Information in order to perform or assist in a lawful and authorized governmental function.

ARTICLE 2 LIMITATIONS ON SCOPE OF THE AGREEMENT

This Agreement shall not apply to Classified Information within the scope of the terms of another agreement or arrangement between the Parties or agencies thereof providing for the protection of a particular item or category of Classified Information exchanged between the Parties or agencies thereof, except to the extent that such other agreement or arrangement expressly makes this Agreement's terms applicable. This Agreement also shall not apply to the exchange of Restricted Data, as defined in the U.S. Atomic Energy Act of 1954, as amended (the "AEA"), or to Formerly Restricted Data, which is data removed from the Restricted Data category in accordance with the AEA but still considered to be defense information by the United States of America.

ARTICLE 3 COMMITMENT TO THE PROTECTION OF CLASSIFIED INFORMATION

1. Each Party shall protect Classified Information of the other Party according to the terms set forth herein.

2. Classified Information shall be protected by the recipient Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party.

3. Each Party shall promptly notify the other of any changes to its laws and regulations that would affect the protection of Classified Information under this Agreement. The obligations in this Agreement shall not be affected by such changes in domestic law. In such cases, the Parties shall consult regarding possible amendments to this Agreement or other measures that may be appropriate to maintain protection of Classified Information exchanged under this Agreement.

ARTICLE 4
NATIONAL SECURITY AUTHORITIES

1. The Parties shall inform each other of the National Security Authorities responsible for implementation of this Agreement and any subsequent changes to them.

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

a. for the Slovak Republic:
National Security Authority
Budatínska 30
851 06 Bratislava
Slovak Republic

b. for the United States of America:
Assistant Director, International Engagement Directorate
Defense Technology Security Administration
4800 Mark Center Drive
Alexandria, Virginia 22350-1600

3. The Parties may conclude supplemental implementing arrangements to this Agreement where additional technical security measures may be required to protect Classified Information transferred to the recipient Party through foreign military sales or cooperative programs for co-production or co-development of defense articles or services. Such implementing arrangements may include Special Security Agreements or Industrial Security Agreements.

ARTICLE 5
DESIGNATION OF CLASSIFIED INFORMATION

1. Classified Information shall be designated, by the releasing Party as classified at one of the following national security classification levels. For purposes of ensuring equivalent treatment, the Parties agree that the following security classification levels are equivalent:

UNITED STATES OF AMERICA	SLOVAK REPUBLIC
TOP SECRET	PRÍSNE TAJNÉ
SECRET	TAJNÉ
CONFIDENTIAL	DÔVERNÉ
CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED	VYHRADENÉ

2. The United States of America shall afford protection to Classified Information designated “VYHRADENÉ” as “CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED” in accordance with this Agreement unless specified otherwise in the Appendix to this Agreement.
3. Classified Information shall be designated, with the name of the releasing Party.

ARTICLE 6 RESPONSIBILITY FOR CLASSIFIED INFORMATION

The recipient Party shall be responsible for the protection of all Classified Information of the releasing Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party while the Classified Information is under its control. While in transit, the releasing Party shall be responsible for all Classified Information until custody of the Classified Information is formally transferred to the recipient Party.

ARTICLE 7 PROTECTION OF CLASSIFIED INFORMATION

1. No individual shall be entitled to have access to Classified Information solely by virtue of rank, position, appointment, or PSC. Access to such Classified Information shall be granted only to individuals who have a Need-to-Know and who have been granted the requisite PSC in accordance with the prescribed standards of the recipient Party.
2. Except as otherwise provided in this Agreement, the recipient Party shall not release Classified Information of the releasing Party to any third party, including any third-party government, individual, firm, institution, organization, or other entity, without the prior written authorization of the releasing Party.
3. The recipient Party shall not use or permit the use of Classified Information of the releasing Party for any other purpose than that for which it was provided without the prior written authorization of the releasing Party.
4. The recipient Party shall respect any private rights that are associated with Classified Information of the releasing Party, including those rights with respect to patents, copyrights, or trade secrets, and shall not release, use, exchange, or disclose such Classified Information in a manner inconsistent with those rights without the prior written authorization of the owner of those rights.
5. The recipient Party shall ensure that each facility that handles Classified Information covered by this Agreement maintains a list of individuals at the facility who are authorized to have access to such Classified Information.
6. Each Party shall develop accountability and control procedures to manage the dissemination of, and access to, Classified Information.
7. Each Party shall comply with any and all limitations on use, disclosure, release, and access to Classified Information as may be specified by the releasing Party when it discloses such Classified

Information. If a Party is unable to comply with the specified limitations, that Party shall immediately consult with the other Party and shall undertake all lawful measures to prevent or minimize any such use, disclosure, release, or access.

ARTICLE 8 PERSONNEL SECURITY CLEARANCES

1. The Parties shall ensure that all individuals who in the conduct of their official duties require access or whose duties or functions may afford access to Classified Information pursuant to this Agreement are granted an appropriate PSC before they are granted access to such Classified Information.
2. The Party granting the PSC shall conduct an appropriate investigation in sufficient detail to determine an individual's suitability for access to Classified Information. The grant of a PSC will be made in accordance with the national laws and regulations of the granting Party.
3. Before an official or representative of one Party releases Classified Information to an official or representative of the other Party, the recipient Party shall provide to the releasing Party an assurance that the official or representative has the necessary PSC level and a Need-to-Know and that the Classified Information will be protected by the recipient Party in accordance with this Agreement.

ARTICLE 9 RELEASE OF CLASSIFIED INFORMATION TO CONTRACTORS

1. Classified Information received by the recipient Party may be provided by the recipient Party to a Contractor or prospective Contractor whose duties require access to such Classified Information with the prior written authorization of the releasing Party. Prior to releasing any Classified Information to a Contractor or prospective Contractor, the recipient Party shall:
 - a. Confirm that such Contractor or prospective Contractor and the Contractor's facility have the capability to protect the Classified Information in accordance with the terms of this Agreement;
 - b. Confirm that such Contractor or prospective Contractor and the Contractor's facility have been granted appropriate PSCs and FSCs, as applicable;
 - c. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that all individuals having access to the Classified Information are informed of their responsibilities to protect the Classified Information in accordance with applicable laws and regulations; and
 - d. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that access to the Classified Information is limited to those individuals who have a Need-to-Know.
2. The recipient Party shall carry out periodic security inspections in cleared facilities to ensure that the Classified Information is protected as required by this Agreement.

**ARTICLE 10
CLASSIFIED CONTRACTS**

1. When a Party proposes to place, or authorizes a Contractor in its country to place, a Classified Contract, with a Contractor in the country of the other Party, the Party that is to place or authorize the Contractor to place such Classified Contract shall request an assurance that an FSC has been issued from the National Security Authority of the other Party. The National Security Authority of the requested Party shall monitor and take all appropriate steps to ensure the security conduct by the Contractor will be in accordance with the applicable laws and regulations.

2. The National Security Authority of a Party negotiating a Classified Contract to be performed in the country of the other Party, shall incorporate in the Classified Contract, request for proposal, or subcontract document, appropriate security clauses and other relevant provisions, including costs for security. This includes provisions requiring any Contractors to include appropriate security clauses in their subcontract documents.

**ARTICLE 11
RESPONSIBILITY FOR FACILITIES**

Each Party shall be responsible for the security of all government and private facilities where it stores Classified Information of the other Party and shall ensure that such facilities have qualified and appropriately cleared individuals appointed with the responsibility and authority for the control and protection of such Classified Information.

**ARTICLE 12
STORAGE OF CLASSIFIED INFORMATION**

Classified Information exchanged between the Parties shall be stored in a manner that ensures access only by those individuals who have been authorized access.

**ARTICLE 13
TRANSMISSION**

1. Classified Information shall be transmitted between the Parties through government-to-government channels or other channels mutually authorized in advance in writing.

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

a. Documents or other media:

(1) Documents or other media containing Classified Information shall be transmitted in double, sealed envelopes. The inner envelope shall indicate only the classification of the documents or other media and the organizational address of the intended recipient. The outer envelope shall

indicate the organizational address of the intended recipient, the organizational address of the sender, and the document control number, if applicable.

(2) No indication of the classification of the enclosed documents or other media shall be made on the outer envelope. The double sealed envelope shall be transmitted according to the prescribed procedures of the transmitting Party.

(3) Receipts shall be prepared by the sender for packages containing documents or other media containing Classified Information that are transmitted between the Parties, and such receipts shall be signed by the final recipient and returned to the sender.

b. Material:

(1) Material, including equipment, that contains Classified Information shall be transported in sealed, covered vehicles, or shall otherwise be securely packaged or protected in order to prevent identification of its shape, size, or contents, and kept under continuous control to prevent access by unauthorized individuals.

(2) Material, including equipment that contains Classified Information that must be stored temporarily awaiting shipment shall be placed in protected storage areas. Such areas shall be protected by intrusion detection equipment or guards with requisite PSCs who shall maintain continuous surveillance of those areas. Only authorized personnel with the requisite PSC shall have access to the protected storage areas.

(3) Receipts shall be obtained whenever material that contains Classified Information, including equipment, changes hands during transit, and a receipt for such material shall be signed by the final recipient and returned to the sender.

c. Electronic transmissions: Classified Information that is classified at the CONFIDENTIAL / DÔVERNÉ level or above that is to be transferred electronically shall be transmitted using secure means that have been authorized by each Party's National Security Authority.

ARTICLE 14

VISITS TO FACILITIES OF THE PARTIES

1. Visits by representatives of one Party to facilities of the other Party that require access to Classified Information, or visits for which a PSC is required to permit access, shall be limited to those necessary for official purposes. Authorization shall only be granted to representatives have been granted a valid PSC.

2. Authorization to visit such facilities shall be granted only by the Party in whose territory the facility to be visited is located. The visited Party, or its designated officials, shall be responsible for advising the facility of the proposed visit, and the scope and highest level of Classified Information that may be furnished to the visitor.

3. Requests for visits by representatives of the Parties shall be submitted by the Embassy of the United States of America in Bratislava in the case of visitors from the United States of America, and by the

Embassy of the Slovak Republic in Washington, District of Columbia in the case of visitors from the Slovak Republic.

ARTICLE 15 SECURITY VISITS

Implementation of security requirements set out in this Agreement may be verified through reciprocal visits by security personnel of the Parties. The security representatives of each Party, after prior consultation, shall be permitted to visit the other Party to discuss and observe the implementing procedures of the other Party in the interest of achieving reasonable comparability of security systems. The host Party shall assist the visiting security representatives in determining whether Classified Information received from the other Party is being adequately protected.

ARTICLE 16 SECURITY STANDARDS

On request, each Party shall provide the other Party with information about its security standards, practices, and procedures for protection of Classified Information.

ARTICLE 17 REPRODUCTION OF CLASSIFIED INFORMATION

When Classified Information is reproduced, including when it is translated, all of the original security designations thereon shall also be reproduced on each reproduction, including each translation of such Classified Information. Such reproductions, including translations, shall be subject to the same controls as the original Classified Information. The number of reproductions shall be limited to the minimum number required for official purposes.

ARTICLE 18 DESTRUCTION OF CLASSIFIED INFORMATION

1. Documents and other media containing Classified Information shall be destroyed by burning, shredding, pulping, or other means that prevent reconstruction of the Classified Information contained therein.
2. Material, including equipment, containing Classified Information shall be destroyed through means that render it no longer recognizable so as to preclude reconstruction of the Classified Information in whole or in part.

ARTICLE 19
DOWNGRADING AND DECLASSIFICATION

1. The Parties agree that Classified Information should be downgraded in classification as soon as the Classified Information ceases to require that higher degree of protection or should be declassified as soon as the Classified Information no longer requires protection against unauthorized disclosure.
2. The releasing Party has complete discretion concerning downgrading or declassification of its Classified Information. The recipient Party shall not downgrade the security classification or declassify Classified Information received from the releasing Party, notwithstanding any apparent declassification instructions on the document, without the prior written authorization of the releasing Party.

ARTICLE 20
LOSS OR COMPROMISE

The recipient Party shall inform the releasing Party immediately upon discovery of all losses or compromises, as well as possible losses or compromises, of Classified Information of the releasing Party. In the event of an actual or possible loss or compromise of such Classified Information, the recipient Party shall initiate an investigation immediately to determine the circumstances of the actual or possible loss or compromise. The results of the investigation and information regarding measures taken to prevent recurrence shall be provided to the releasing Party.

ARTICLE 21
DISPUTES

Disagreements between the Parties arising under or relating to this Agreement shall be settled solely through consultations between the Parties and shall not be referred to a national court, an international tribunal, or any other individual or entity for settlement.

ARTICLE 22
COSTS

Each Party shall be responsible for bearing its own costs incurred in implementing this Agreement. All obligations of the Parties under this Agreement shall be subject to the availability of funds. Notwithstanding the availability of funds, each Party shall, in accordance with applicable laws and regulations, continue to protect Classified Information in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party.

ARTICLE 23
FINAL PROVISIONS

1. This Agreement shall enter into force upon the date of the last signature by the Parties.

2. Either Party may terminate this Agreement by notifying the other Party in writing through diplomatic channels ninety days in advance of its intention to terminate the Agreement.

3. Notwithstanding the termination of this Agreement, all Classified Information exchanged, produced, or otherwise provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

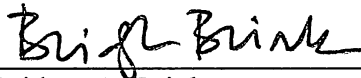
4. Upon entry into force of this Agreement, this Agreement shall supersede the Agreement between the Government of the Slovak Republic and the Government of the United States of America Concerning Security Measures for the Protection of Classified Military Information, signed at Washington, April 11, 1995 (the "Security Agreement"). This Agreement shall apply to classified military information to which the Security Agreement had applied prior to the entry into force of this Agreement.

IN WITNESS WHEREOF, the undersigned, being duly authorized thereto by their respective Governments, have signed this Agreement.

Done in duplicate at Bratislava this 13th day of May 2022, in the English and Slovak languages, both texts being equally authentic.

FOR THE GOVERNMENT OF
THE UNITED STATES OF AMERICA

FOR THE GOVERNMENT OF
THE SLOVAK REPUBLIC



Bridget A. Brink
Ambassador



Roman Konečný
Director, National Security Authority

APPENDIX

PROCEDURES FOR PROTECTING SLOVAK REPUBLIC "VYHRADENÉ" CLASSIFIED INFORMATION PROVIDED TO THE UNITED STATES OF AMERICA

1. Slovak Republic Classified Information provided to the United States of America and designated as "VYHRADENÉ" shall be protected by the United States of America as "CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED" in accordance with the following procedures.
2. Classified Information designated as "VYHRADENÉ" shall be stored in locked containers or secured areas so that access by unauthorized individuals is prevented.
3. "VYHRADENÉ" Classified Information shall not be disclosed to unauthorized individuals or entities without the prior written approval of the Slovak Republic.
4. "VYHRADENÉ" Classified Information shall, as applicable, be stored, processed, or transmitted electronically using government- or Contractor-accredited systems. In particular, before any system is used to store, process, or transmit "VYHRADENÉ" Classified Information, it must receive security approval, known as Accreditation. An Accreditation is a formal statement by the appropriate accrediting authority confirming that the use of a system meets the appropriate security requirements and does not present an unacceptable risk. Security Standard Operating Procedures are technical procedures to implement security policies and requirements unique to a specific facility to protect automated information systems processing Classified Information. For stand-alone automated information systems such as desktop and laptop computers utilized in United States of America government facilities the system registration document together with the Security Standard Operating Procedures shall fulfill the role of the required Accreditation. For Contractors, guidance on the use of communications and information systems shall be incorporated into the Restricted Conditions Requirements Clause in the Contract.
5. "VYHRADENÉ" Classified Information shall be transmitted by first class mail within the United States of America in double sealed envelope. Transmission outside the United States of America shall be in double, sealed envelopes, with the inner envelope designated "VYHRADENÉ/ CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED." Transmission outside the United States of America shall be by traceable means such as commercial courier or other means agreed upon by the Parties in writing.
6. United States of America documents that contain "VYHRADENÉ/ CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED" Classified Information shall bear on the cover and the first page the designation "SLOVAK REPUBLIC VYHRADENÉ." The portion of the documents containing "VYHRADENÉ" Classified Information also shall be identified with the same designation.
7. "VYHRADENÉ" Classified Information may be transmitted or accessed electronically via a public network like the Internet using government or commercial encryption devices mutually accepted by the Parties. Telephone conversations, video conferencing, or facsimile transmissions containing "VYHRADENÉ" Classified Information may be conducted if an encryption system is not available and subject to the approval of the Slovak Republic's National Security Authority.

8. An FSC is required for a Contractor to undertake contracts at the “VYHRADENÉ” level.

9. Access to such “VYHRADENÉ” Classified Information shall be granted only to those individuals who have a Need-to-Know. A PSC is not required to access “VYHRADENÉ” Classified Information.

DOHODA MEDZI VLÁDOU SPOJENÝCH ŠTÁTOV AMERICKÝCH

A

VLÁDOU SLOVENSKEJ REPUBLIKY

O BEZPEČNOSTNÝCH OPATRENIACH NA OCHRANU UTAJOVANÝCH SKUTOČNOSTÍ

PREAMBULA

Vláda Spojených štátov amerických a vláda Slovenskej republiky (ďalej len „zmluvná strana“ a spoločne „zmluvné strany“),

berúc do úvahy, že zmluvné strany spolupracujú v záležitostiach vrátane, no nie výlučne, zahraničných záležitostí, obrany, bezpečnosti, presadzovania práva, vedy, priemyslu a technológií a

majúc spoločný záujem na ochrane utajovaných skutočností vymieňaných medzi zmluvnými stranami,

sa dohodli takto:

ČLÁNOK 1 VYMEDZENIE POJMOV

Na účely tejto dohody:

1. Utajované skutočnosti: Informácie poskytnuté jednou zmluvnou stranou druhej zmluvnej strane, označené ako utajené odovzdávajúcou zmluvnou stranou z dôvodov národnej bezpečnosti, ktoré si preto vyžadujú ochranu pred neoprávneným poskytnutím. Informácie môžu byť v písomnej, vizuálnej, elektronickej alebo dokumentárnej podobe alebo v podobe materiálu, vrátane zariadenia alebo technológie.
2. Utajovaný kontrakt: Kontrakt, ktorý si vyžaduje alebo si bude vyžadovať prístup k utajovaným skutočnostiam alebo ich tvorbu kontrahentom alebo jeho zamestnancami počas výkonu kontraktu.
3. Kontrahent: Fyzická osoba alebo právnická osoba právne spôsobilá uzatvárať utajované kontrakty, ktorá je zmluvnou stranou utajovaného kontraktu.
4. Previerka priemyselnej bezpečnosti (FSC): Potvrdenie poskytnuté národným bezpečnostným orgánom zmluvnej strany v súlade s článkom 4, pre kontrahentský podnik v pôsobnosti zmluvnej strany, ktoré označuje, že podnik je preverený na určitý stupeň a má tiež zavedené vhodné bezpečnostné záruky pre konkrétny stupeň ochrany utajovaných skutočností. Takéto potvrdenie znamená, že utajované skutočnosti stupňa DÔVERNÉ/CONFIDENTIAL alebo vyššie kontrahent ochráni na stupni, na ktorý je previerka priemyselnej bezpečnosti poskytnutá v súlade s ustanoveniami tejto dohody, pričom tento súlad monitoruje a presadzuje národný bezpečnostný orgán.

5. Preverka personálnej bezpečnosti (PSC):

a. Potvrdenie národného bezpečnostného orgánu zmluvnej strany v súlade s článkom 4 tejto dohody, že fyzická osoba zamestnaná štátnym orgánom zmluvnej strany alebo kontrahentom v pôsobnosti zmluvnej strany je oprávnená na prístup k utajovaným skutočnostiam konkrétneho stupňa.

b. Potvrdenie národného bezpečnostného orgánu zmluvnej strany v súlade s článkom 4, že fyzická osoba, ktorá je štátnym príslušníkom jednej zmluvnej strany, ale má sa zamestnať v druhej zmluvnej strane alebo u kontrahenta druhej zmluvnej strany, je oprávnená na prístup k utajovaným skutočnostiam konkrétneho stupňa.

6. Need-to-know: Zistenie urobené oprávneným držiteľom utajovaných skutočností, že potenciálny príjemca utajovaných skutočností vyžaduje prístup ku konkrétnym utajovaným skutočnostiam pre výkon alebo súčinnosť vo funkcii v štátnom orgáne v súlade s právom a oprávnením.

ČLÁNOK 2 OBMEDZENIA ROZSAHU POUŽITIA TEJTO DOHODY

Táto dohoda sa neuplatní na utajované skutočnosti v rámci podmienok inej dohody alebo dojednania medzi zmluvnými stranami alebo ich štátnymi orgánmi ohľadom ochrany konkrétnych utajovaných skutočností alebo nejakej ich kategórie, vymieňaných medzi zmluvnými stranami alebo ich štátnymi orgánmi, s výnimkou prípadu, kedy sa taká dohoda alebo dojednanie podmienky tejto dohody výslovne uplatní. Táto dohoda sa tiež neuplatní na výmenu informácií označených „Restricted Data“ podľa Zákona Spojených štátov amerických o atómovej energii z r. 1954 v znení neskorších predpisov (ďalej len „AEA“), alebo na informácie označené „Formerly Restricted Data“, teda informácie vyňaté z kategórie „Restricted Data“ v súlade s AEA, no naďalej považované za obranné informácie Spojenými štátmi americkými.

ČLÁNOK 3 ZÁVÄZOK OCHRANY UTAJOVANÝCH SKUTOČNOSTÍ

1. Každá zmluvná strana chráni utajované skutočnosti druhej zmluvnej strany podľa podmienok uvedených v tejto dohode.

2. Prijímajúca zmluvná strana chráni utajované skutočnosti spôsobom, ktorý je prinajmenšom rovnocenný ochrane poskytnutej utajovaným skutočnostiam odovzdávajúcou zmluvnou stranou.

3. Každá zmluvná strana bezodkladne oboznámi druhú zmluvnú stranu o akýchkoľvek zmenách vlastných vnútroštátnych právnych predpisov, ktoré by mali vplyv na ochranu utajovaných skutočností podľa tejto dohody. Povinnosti v tejto dohode nebudú ovplyvnené takými zmenami vo vnútroštátnom práve. V takých prípadoch sa uskutočnia medzi zmluvnými stranami konzultácie ohľadom prípadných zmien tejto dohody alebo iných opatrení vhodných pre zachovanie ochrany utajovaných skutočností vymieňaných podľa tejto dohody.

ČLÁNOK 4 NÁRODNÉ BEZPEČNOSTNÉ ORGÁNY

1. Zmluvné strany sa navzájom informujú o národných bezpečnostných orgánoch zodpovedných za vykonávanie tejto dohody a o ich prípadných následných zmenách.

2. Na účely tejto dohody sú národnými bezpečnostnými orgánmi:

a. pre Spojené štáty americké:

námestník riaditeľa Riaditeľstva pre medzinárodné angažovanie sa
Správa bezpečnosti obranných technológií
4800 Mark Center Drive
Alexandria, Virginia 22350-1600
Spojené štáty americké

b. pre Slovenskú republiku:

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava
Slovenská republika

3. Zmluvné strany môžu uzatvárať dodatočné vykonávacie dojednania k tejto dohode, kde možno požadovať dodatočné technické bezpečnostné opatrenia pre ochranu utajovaných skutočností postúpených prijímajúcej zmluvnej strane prostredníctvom zahraničného vojenského predaja alebo programov spolupráce v spoločnej tvorbe alebo spoločnom vývoji obranných položiek alebo služieb. Tieto vykonávacie dojednania môžu obsahovať dohody o priemyselnej bezpečnosti alebo dohody o zvláštnej bezpečnosti.

ČLÁNOK 5 OZNAČOVANIE UTAJOVANÝCH SKUTOČNOSTÍ

1. Utajované skutočnosti označí odovzdávajúca zmluvná strana ako utajované jedným z nasledujúcich národných bezpečnostných stupňov utajenia. Na účely zabezpečenia rovnocenného zaobchádzania zmluvné strany súhlasia, že nasledujúce bezpečnostné stupne utajenia sú rovnocenné:

Spojené štáty americké	Slovenská republika
TOP SECRET	PRÍSNE TAJNÉ
SECRET	TAJNÉ
CONFIDENTIAL	DÔVERNÉ
CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED	VYHRADENÉ

2. Spojené štáty americké poskytnú utajovaným skutočnostiam označeným „VYHRADENÉ” ochranu ako „CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED” v súlade s touto dohodou, ak v prílohe k tejto dohode nie je uvedené inak.

3. Utajované skutočnosti sa označia názvom odovzdávajúcej zmluvnej strany.

ČLÁNOK 6 ZODPOVEDNOSŤ ZA UTAJOVANÉ SKUTOČNOSTI

Prijímajúca zmluvná strana je zodpovedná za ochranu všetkých utajovaných skutočností odovzdávajúcej zmluvnej strany spôsobom, ktorý je prinajmenšom rovnocenný ochrane priznanej utajovaným skutočnostiam odovzdávajúcou zmluvnou stranou, kým sú utajované skutočnosti pod jej kontrolou. Počas prepravy odovzdávajúca zmluvná strana je zodpovedná za všetky utajované skutočnosti, kým nebudú formálne prevedené do držby prijímajúcej zmluvnej strane.

ČLÁNOK 7 OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

1. Žiadna fyzická osoba nezíska prístup k utajovaným skutočnostiam výlučne na základe hodnosti, pozície, ustanovenia do funkcie alebo previerky personálnej bezpečnosti. Prístup k utajovaným skutočnostiam sa povolí iba fyzickým osobám s need-to-know a s príslušnou previerkou personálnej bezpečnosti v súlade s predpísanými štandardmi prijímajúcej zmluvnej strany.
2. Ak v tejto dohode nie je uvedené inak, bez predchádzajúceho písomného súhlasu odovzdávajúcej zmluvnej strany prijímajúca zmluvná strana neposkytne utajované skutočnosti odovzdávajúcej zmluvnej strany akejkoľvek tretej strane, vrátane vlády, fyzických osôb, firiem, inštitúcií, organizácií alebo iných entít tretej strany.
3. Bez predchádzajúceho písomného súhlasu odovzdávajúcej zmluvnej strany prijímajúca zmluvná strana nepoužije ani nepovolí použitie utajovaných skutočností odovzdávajúcej zmluvnej strany na akýkoľvek iný účel ako na ten, na ktorý boli poskytnuté.
4. Prijímajúca zmluvná strana rešpektuje všetky súkromné práva týkajúce sa utajovaných skutočností odovzdávajúcej zmluvnej strany, vrátane práv ohľadom patentov, autorských práv alebo obchodných tajomstiev a neposkytne, nepoužije, nevymení ani neodovzdá takéto utajované skutočnosti spôsobom nezlučiteľným s týmito právami bez predchádzajúceho písomného súhlasu vlastníka týchto práv.
5. Prijímajúca zmluvná strana zabezpečí, že každý podnik, ktorý manipuluje s utajovanými skutočnosťami podľa tejto dohody, udržiava zoznam fyzických osôb v podniku, ktoré sú oprávnené mať prístup k týmto utajovaným skutočnostiam.
6. Každá zmluvná strana vytvorí systém zodpovednosti a postupov riadenia pre zabezpečenie rozširovania a prístupu k utajovaným skutočnostiam.
7. Každá zmluvná strana vyhovie všetkým obmedzeniam použitia, odovzdania, postúpenia a prístupu k utajovaným skutočnostiam, ako boli konkretizované odovzdávajúcou zmluvnou stranou pri odovzdaní týchto utajovaných skutočností. Ak zmluvná strana nemôže vyhovieť takýmto konkrétnym obmedzeniam, táto zmluvná strana sa bezodkladne poradí s druhou zmluvnou stranou a podnikne všetky opatrenia v súlade s právom, aby predišla alebo obmedzila takéto použitie, odovzdanie, postúpenie alebo prístup.

ČLÁNOK 8 PREVIERKY PERSONÁLNEJ BEZPEČNOSTI

1. Zmluvné strany zabezpečia, že všetky fyzické osoby, ktoré v rámci svojich úradných povinností vyžadujú prístup alebo povinnosti alebo postavenie ktorých môže vyžadovať prístup k utajovaným skutočnostiam podľa tejto dohody, majú udelenú príslušnú previerku personálnej bezpečnosti pred poskytnutím prístupu k takýmto utajovaným skutočnostiam.
2. Zmluvná strana udeľujúca previerku personálnej bezpečnosti vykoná príslušné dostatočne podrobné vyšetrovanie, aby sa zistilo, či je prístup fyzickej osoby k utajovaným skutočnostiam vhodný. Udelenie previerky personálnej bezpečnosti sa vykoná v súlade s vnútroštátnymi právnymi predpismi udeľujúcej zmluvnej strany.
3. Predtým, ako úradník alebo predstaviteľ jednej zmluvnej strany postúpi utajované skutočnosti úradníkovi alebo predstaviteľovi druhej zmluvnej strany, prijímajúca zmluvná strana poskytne odovzdávajúcej zmluvnej strane uistenie, že daný úradník alebo predstaviteľ má previerku personálnej bezpečnosti príslušného stupňa a need-to-know a že utajované skutočnosti budú chránené prijímajúcou zmluvnou stranou v súlade s touto dohodou.

ČLÁNOK 9 POSTÚPENIE UTAJOVANÝCH SKUTOČNOSTÍ KONTRAHENTOM

1. Utajované skutočnosti prijaté prijímajúcou zmluvnou stranou môže prijímajúca zmluvná strana s predchádzajúcim písomným súhlasom odovzdávajúcej zmluvnej strany poskytnúť kontrahentovi alebo potenciálnemu kontrahentovi, povinnosti ktorého vyžadujú prístup k takýmto utajovaným skutočnostiam. Pred postúpením akýchkoľvek utajovaných skutočností kontrahentovi alebo potenciálnemu kontrahentovi prijímajúca zmluvná strana:
 - a. potvrdí, že takýto kontrahent alebo potenciálny kontrahent a kontrahentov podnik majú spôsobilosť chrániť utajované skutočnosti v súlade s podmienkami tejto dohody;
 - b. potvrdí, že takémuto kontrahentovi alebo potenciálnemu kontrahentovi a kontrahentovmu podniku boli podľa potreby udelené príslušné previerky personálnej bezpečnosti a previerky priemyselnej bezpečnosti;
 - c. potvrdí, že kontrahent alebo potenciálny kontrahent má zavedené postupy zabezpečujúce, že všetky fyzické osoby majúce prístup k utajovaným skutočnostiam sú oboznámené so svojou zodpovednosťou pri ochrane utajovaných skutočností v súlade s príslušnými právnymi predpismi; a
 - d. potvrdí, že kontrahent alebo potenciálny kontrahent má zavedené postupy zabezpečujúce, že prístup k utajovaným skutočnostiam je obmedzený na fyzické osoby s need-to-know.
2. Prijímajúca zmluvná strana vykoná pravidelné bezpečnostné kontroly v preverených podnikoch pre zabezpečenie ochrany utajovaných skutočností v súlade s požiadavkami tejto dohody.

ČLÁNOK 10 UTAJOVANÉ KONTRAKTY

1. Keď jedna zmluvná strana navrhne uzavretie alebo oprávni kontrahenta svojho štátu uzavrieť utajovaný kontrakt s kontrahentom štátu druhej zmluvnej strany, zmluvná strana, ktorá má uzavrieť alebo oprávniť kontrahenta uzavrieť takýto utajovaný kontrakt, požiada o uistenie, že národný bezpečnostný orgán druhej zmluvnej strany vydal previerku priemyselnej bezpečnosti. Národný bezpečnostný orgán dožadanej zmluvnej strany monitoruje a vykoná potrebné kroky pre zabezpečenie bezpečnostného správania sa kontrahenta v súlade s príslušnými právnymi predpismi.

2. Národný bezpečnostný orgán zmluvnej strany, ktorá vyjednáva utajovaný kontrakt, ktorý sa má vykonať v štáte druhej zmluvnej strany, zahrnie do utajovaného kontraktu, žiadosti o návrh alebo dokumentu subkontraktu príslušné bezpečnostné klauzuly a iné relevantné ustanovenia, vrátane bezpečnostných nákladov. To zahŕňa aj ustanovenia vyžadujúce od akýchkoľvek kontrahentov, aby zahrnuli príslušné bezpečnostné klauzuly do svojich dokumentov subkontraktov.

ČLÁNOK 11 ZODPOVEDNOSŤ ZA PODNIKY

Každá zmluvná strana je zodpovedná za bezpečnosť všetkých podnikov štátnej správy aj súkromných podnikov, kde uchováva utajované skutočnosti druhej zmluvnej strany a zabezpečí, že tieto podniky majú určené kvalifikované a príslušne preverené fyzické osoby so zodpovednosťou a právomocou pre riadenie a ochranu takýchto utajovaných skutočností.

ČLÁNOK 12 UCHOVÁVANIE UTAJOVANÝCH SKUTOČNOSTÍ

Utajované skutočnosti vymieňané medzi zmluvnými stranami sa uchovávajú spôsobom, ktorý zabezpečí prístup k nim iba fyzickým osobám, ktoré boli na prístup oprávnené.

ČLÁNOK 13 POSTUPOVANIE

1. Utajované skutočnosti si postúpia zmluvné strany prostredníctvom vládnych kanálov alebo iných kanálov, na ktorých sa vzájomne vopred písomne dohodnú.

2. Minimálne požiadavky pre bezpečnosť utajovaných skutočností počas postupovania sú nasledujúce:

a. Dokumenty a iné médiá:

(1) Dokumenty a iné médiá obsahujúce utajované skutočnosti sa postupujú v dvojitych zapečatených obálkach. Vnútorňa obálka nesie len označenie utajenia dokumentov alebo iných médií a adresu organizácie adresáta, ktorému je to určené. Vonkajšia obálka nesie označenie adresy organizácie adresáta, ktorý je určeným príjemcom, adresy organizácie odosielateľa a podľa potreby evidenčného čísla dokumentu.

(2) Na vonkajšej obálke sa nenachádza označenie utajenia priložených písomností alebo iných médií. Dvojitá zapečatená obálka sa postúpi v súlade s platnými zákonmi, vyhláškami alebo postupmi postupujúcej zmluvnej strany.

(3) Odosielateľ pripraví potvrdenia o prijatí pre zásielky obsahujúce dokumenty alebo iné médiá obsahujúce utajované skutočnosti, postupované medzi zmluvnými stranami a tieto potvrdenia o prijatí prijímateľ podpíše a vráti ich odosielateľovi.

b. Veci:

(1) Veci, vrátane zariadenia, ktoré obsahujú utajované skutočnosti, sa prevádzajú v zapečatených, krytých vozidlách alebo sa inak bezpečne zabalia a chránia pred identifikáciou ich tvaru, veľkosti alebo obsahu a udržiavajú sa pod nepretržitou kontrolou, aby sa predišlo prístupu neoprávnených osôb.

(2) Veci, vrátane zariadenia, ktoré obsahujú utajované skutočnosti, ktoré musia byť dočasne uskladnené pred prepravou, sa uskladnia v chránených skladovacích priestoroch. Takéto priestory sú chránené zariadeniami na detekciu vniknutia alebo strážnikmi s príslušnými previerkami personálnej bezpečnosti, ktorí zabezpečujú nepretržité sledovanie týchto priestorov. Len oprávnený personál s príslušnou previerkou personálnej bezpečnosti má prístup do chránených skladovacích priestorov.

(3) Konečný prijímateľ podpíše a vráti odosielateľovi potvrdenie o prijatí vždy, keď sú veci, obsahujúce utajované skutočnosti, počas dopravy odovzdané.

c. Elektronické postupovanie: Utajované skutočnosti stupňa utajenia DÔVERNÉ /CONFIDENTIAL alebo vyššie, ktoré majú byť postúpené elektronicky, sa postúpia s použitím bezpečných prostriedkov odsúhlasených národnými bezpečnostnými orgánmi každej zmluvnej strany.

ČLÁNOK 14 NÁVŠTEVY PODNIKOV ZMLUVNÝCH STRÁN

1. Návštevy predstaviteľov jednej zmluvnej strany v podnikoch druhej zmluvnej strany, ktoré si vyžadujú prístup k utajovaným skutočnostiam, alebo návštevy, na ktoré sa vyžaduje previerka personálnej bezpečnosti pre povolenie prístupu, sa obmedzia na tie, ktoré sú nevyhnutné na úradné účely. Oprávnenie sa udelí len predstaviteľom, ktorým bola udelená platná previerka personálnej bezpečnosti.

2. Oprávnenie na návštevu takýchto podnikov sa udelí len zmluvnou stranou, na území ktorej sa nachádza podnik, ktorý má byť navštívený. Navštívená zmluvná strana alebo jej určený úradník sú zodpovední za upovedomenie podniku o navrhovanej návšteve a o rozsahu a najvyššom stupni utajovaných skutočností, ktoré môžu byť návštevníkom poskytnuté.

3. Žiadosti o návštevy predstaviteľov jednej zmluvnej strany postúpi Veľvyslanectvo Spojených štátov amerických v Bratislave v prípade návštevníkov zo Spojených štátov amerických a Veľvyslanectvo Slovenskej republiky vo Washingtone, District of Columbia v prípade návštevníkov zo Slovenskej republiky.

ČLÁNOK 15 BEZPEČNOSTNÉ NÁVŠTEVY

Uskutočňovanie bezpečnostných požiadaviek uvedených v tejto dohode sa môže overiť vzájomnými návštevami bezpečnostného personálu zmluvných strán. Bezpečnostným predstaviteľom každej zmluvnej strany sa po predchádzajúcej konzultácii povolí navštíviť druhú zmluvnú stranu s cieľom prediskutovať a pozorovať uskutočňované postupy druhej zmluvnej strany v záujme dosiahnutia primeranej porovnateľnosti bezpečnostných systémov. Hostiteľská zmluvná strana poskytne navštevujúcim bezpečnostným predstaviteľom asistenciu pri určení, či sú utajované skutočnosti prijaté z druhej zmluvnej strany dostatočne chránené.

ČLÁNOK 16 BEZPEČNOSTNÉ ŠTANDARDY

Na základe žiadosti poskytne každá zmluvná strana druhej zmluvnej strane informácie o bezpečnostných štandardoch, praxi a postupoch na ochranu utajovaných skutočností.

ČLÁNOK 17 ROZMNOŽOVANIE UTAJOVANÝCH SKUTOČNOSTÍ

Pri rozmnožovaní utajovaných skutočností, vrátane ich prekladu, sa rozmnožia všetky pôvodné bezpečnostné označenia na každej rozmnoženine, vrátane každého prekladu takýchto utajovaných skutočností. Takéto rozmnoženiny, vrátane prekladov, sú predmetom rovnakej kontroly ako pôvodné utajované skutočnosti. Počet rozmnožením sa obmedzí na minimum, ktoré je nevyhnutné na úradné účely.

ČLÁNOK 18 ZNIČENIE UTAJOVANÝCH SKUTOČNOSTÍ

1. Dokumenty a iné médiá obsahujúce utajované skutočnosti sa zničia spálením, skartovaním, rozdrvením alebo iným spôsobom, ktorý zabráni obnoveniu utajovaných skutočností v nich obsiahnutých.
2. Veci, vrátane zariadenia, obsahujúce utajované skutočnosti, sa zničia spôsobom, ktorý spôsobí, že sa už nebudú dať rozoznať, aby sa predišlo obnoveniu utajovaných skutočností sčasti alebo v celku.

ČLÁNOK 19 ZNÍŽENIE A ZRUŠENIE STUPŇA UTAJENIA

1. Zmluvné strany súhlasia, že utajované skutočnosti by mali mať znížený stupeň utajenia, akonáhle utajované skutočnosti prestanú vyžadovať vyšší stupeň utajenia alebo by mali mať zrušený stupeň utajenia, akonáhle utajované skutočnosti prestanú vyžadovať ochranu pred neoprávneným poskytnutím.
2. Odovzdávajúca zmluvná strana má plnú právomoc rozhodnúť o znížení alebo zrušení stupňa utajenia svojich utajovaných informácií. Prijímajúca zmluvná strana nezníži ani nezruší stupeň utajenia utajovaných skutočností prijatých od odovzdávajúcej zmluvnej strany, bez ohľadu na

akékoľvek zjavné pokyny na zrušenie stupňa utajenia na dokumente, bez predchádzajúceho písomného súhlasu odovzdávajúcej zmluvnej strany.

ČLÁNOK 20 STRATA ALEBO OHROZENIE

Prijímajúca zmluvná strana bezodkladne informuje odovzdávajúcu zmluvnú stranu o zistení akejkoľvek straty alebo ohrozenia, alebo o zistení potenciálnej straty alebo potenciálneho ohrozenia utajovaných skutočností odovzdávajúcej zmluvnej strany. V prípade skutočnej alebo potenciálnej straty alebo ohrozenia takýchto utajovaných skutočností prijímajúca zmluvná strana iniciuje bezodkladne vyšetrovanie na zistenie okolností skutočnej alebo potenciálnej straty alebo ohrozenia. Výsledky vyšetrovania a informácia ohľadom opatrení prijatých na predídenie opätovnému výskytu sa oznámia odovzdávajúcej zmluvnej strane.

ČLÁNOK 21 SPORY

Rozdielne názory medzi zmluvnými stranami vyplývajúce z tejto dohody alebo v súvislosti s touto dohodou sa riešia výlučne konzultáciami medzi zmluvnými stranami a nie sú predložené národnému súdu, medzinárodnému tribunálu alebo akejkoľvek inej fyzickej osobe alebo právnickej osobe na urovanie.

ČLÁNOK 22 NÁKLADY

Každá zmluvná strana zodpovedá za vlastné náklady vzniknuté uplatňovaním tejto dohody. Všetky povinnosti zmluvných strán podľa tejto dohody závisia od dostupnosti financií.

Bez ohľadu na dostupnosť financií každá zmluvná strana v súlade s príslušnými vnútroštátnymi právnymi predpismi naďalej ochráni utajované skutočnosti spôsobom, ktorý je prinajmenšom rovnocenný ochrane poskytnutej utajovaným skutočnostiam odovzdávajúcou zmluvnou stranou.

ČLÁNOK 23 ZÁVEREČNÉ USTANOVENIA

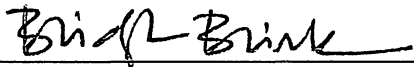
1. Táto dohoda nadobudne platnosť dňom posledného podpisu jednou zo zmluvných strán.
2. Ktorákoľvek zmluvná strana môže ukončiť platnosť tejto dohody písomným oznámením svojho úmyslu ukončiť jej platnosť druhej zmluvnej strane diplomatickou cestou 90 dní vopred.
3. Bez ohľadu na ukončenie platnosti tejto dohody všetky utajované skutočnosti vymenené, vytvorené alebo inak poskytnuté podľa tejto dohody sa naďalej chránia podľa tejto dohody v súlade s jej ustanoveniami.
4. Nadobudnutím platnosti tejto dohody táto dohoda nahradí Dohodu medzi vládou Spojených štátov amerických a vládou Slovenskej republiky o bezpečnostných opatreniach na ochranu utajovaných vojenských informácií, podpísanú vo Washingtone dňa 11. apríla 1995 („Bezpečnostná dohoda“).

Táto dohoda sa vzťahuje na vojenské utajované informácie, na ktoré sa vzťahovala Bezpečnostná dohoda pred nadobudnutím platnosti tejto dohody.

NA DÔKAZ TOHO splnomocnení, riadne na to poverení svojimi vládami, podpísali túto dohodu.

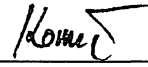
Dané v Bratislave, dňa 13. mája 2022 v dvoch pôvodných vyhotoveniach, v slovenskom a anglickom jazyku, pričom obe znenia majú rovnakú platnosť.

ZA VLÁDU
SPOJENÝCH ŠTÁTOV AMERICKÝCH



Bridget A. Brink
Veľvyslankyňa

ZA VLÁDU
SLOVENSKEJ REPUBLIKY



Roman Konečný
Riaditeľ, Národný bezpečnostný úrad

PRÍLOHA

POSTUPY PRE OCHRANU UTAJOVANÝCH SKUTOČNOSTÍ SLOVENSKEJ REPUBLIKY „VYHRADENÉ“ POSKYTNUTÝCH SPOJENÝM ŠTÁTOM AMERICKÝM

1. Utajované skutočnosti Slovenskej republiky poskytnuté Spojeným štátom americkým a označené „VYHRADENÉ“ chránia Spojené štáty americké ako „CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED“ v súlade s nasledujúcimi postupmi.
2. Utajované skutočnosti označené „VYHRADENÉ“ sa uchovávajú v uzamknutých schránkach alebo zabezpečených priestoroch tak, aby sa predišlo prístupu neoprávnených fyzických osôb.
3. Utajované skutočnosti označené „VYHRADENÉ“ sa nepostúpia neoprávneným fyzickým osobám alebo právnickým osobám bez predchádzajúceho písomného súhlasu Slovenskej republiky.
4. Utajované skutočnosti označené „VYHRADENÉ“ sa podľa vhodnosti uchovávajú, spracúvajú alebo elektronicky postupujú s použitím systémov akreditovaných štátnym orgánom alebo kontrahentom. Konkrétne, skôr, ako sa systém použije na uchovávanie, spracovávanie alebo prenos utajovaných skutočností označených „VYHRADENÉ“, musí získať bezpečnostný súhlas, známy ako akreditácia. Akreditácia je formálne vyhlásenie príslušného akreditačného orgánu, potvrdzujúce, že použitie systému spĺňa príslušné bezpečnostné požiadavky a nepredstavuje neprijateľné riziko. Bezpečnostné štandardné prevádzkové postupy sú technické postupy na vykonanie bezpečnostných zásad a požiadaviek pre konkrétny podnik na ochranu automatizovaných informačných systémov spracúvajúcich utajované skutočnosti. Pre samostatné automatizované informačné systémy ako stolové počítače a laptopy používané v podnikoch štátnych orgánov Spojených štátov amerických plní dokument o systémovej registrácii spolu s bezpečnostnými štandardnými prevádzkovými postupmi úlohu požadovanej akreditácie. Pre kontrahentov sa metodika k používaniu komunikačných a informačných systémov zahrnie do dokumentu s názvom Restricted Conditions Requirements Clause in the Contract.
5. Utajované skutočnosti označené „VYHRADENÉ“ sa v Spojených štátoch amerických prepravujú poštou prvej triedy v dvojitych zapečatených obáľkach. Preprava mimo Spojených štátov amerických sa uskutoční v dvojitych, zapečatených obáľkach, pričom vnútorná obálka sa označí „VYHRADENÉ/ CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED“. Preprava mimo Spojených štátov amerických sa uskutoční vystopovateľným spôsobom ako komerčným kuriérom alebo iným spôsobom, na ktorom sa zmluvné strany písomne dohodnú.
6. Dokumenty Spojených štátov amerických, ktoré obsahujú utajované skutočnosti označené „VYHRADENÉ/ CONFIDENTIAL, MODIFIED HANDLING AUTHORIZED“, majú na obale a na prvej strane označenie „SLOVAK REPUBLIC VYHRADENÉ.“ Časti dokumentov obsahujúce utajované skutočnosti „VYHRADENÉ“ sa tiež označia tým istým označením.
7. Utajované skutočnosti označené „VYHRADENÉ“ možno elektronicky postúpiť alebo sprístupniť prostredníctvom verejnej siete ako internet za podmienky použitia šifrovacích prostriedkov štátnych orgánov alebo súkromných, ak s nimi súhlasia obe zmluvné strany. Telefónne rozhovory, videokonferencie alebo faxové prenosy obsahujúce utajované skutočnosti označené

„VYHRADENÉ” môžu byť uskutočnené, ak nie je k dispozícii šifrovací systém, len so súhlasom národného bezpečnostného orgánu Slovenskej republiky.

8. Na prevzatie kontraktov na stupni „VYHRADENÉ“ sa vyžaduje preverka priemyselnej bezpečnosti.

9. Prístup k takýmto utajovaným skutočnostiam označeným „VYHRADENÉ” sa udelí len fyzickým osobám s need-to-know. Preverka personálnej bezpečnosti sa pre prístup k utajovaným skutočnostiam „VYHRADENÉ” nevyžaduje.