

DEFENSE

Protection of Information

Agreement Between the UNITED STATES OF AMERICA and NORTH MACEDONIA

With Appendix

Signed at Skopje December 21, 2021

Entered into force May 11, 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 REPUBLIC OF NORTH MACEDONIA
CONCERNING SECURITY MEASURES FOR THE PROTECTION OF
CLASSIFIED INFORMATION

PREAMBLE

The Government of the United States of America (the “United States”) and the Government of the Republic of North Macedonia (“North Macedonia”) (each 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 in confidence 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: 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 safeguard Classified Information. Such a certification shall signify

that Classified Information at the CONFIDENTIAL / ДООЕРПННО level or above shall be protected by the Contractor for which the Facility Security Clearance (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. An FSC is not required for a Contractor to undertake Contracts that only require the receipt or production of Classified Information at the ИНТЕРНО (RESTRICTED) level.

5. Personnel Security Clearance (PSC):

- a. A determination by the National Security Authority of a Party, as designated in Article 4, 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 determination 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.

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 these Authorities.

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

a. for the United States: Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy, U.S. Department of Defense

b. for North Macedonia: Director, Directorate for Security of Classified Information, Republic of North Macedonia

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, and stamped or marked where possible, 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	NORTH MACEDONIA
TOP SECRET	ДРЖАВНА ТАЈНА (TOP SECRET)
SECRET	СТРОГО ДОВЕРЛИВО (SECRET)
CONFIDENTIAL	ДОВЕРЛИВО (CONFIDENTIAL)
No equivalent	ИНТЕРНО (RESTRICTED)

2. During the implementation of this Agreement, if North Macedonia provides Classified Information designated as “ИНТЕРНО (RESTRICTED),” the United States shall handle it in accordance with the Appendix to this Agreement.

3. Classified Information shall be designated, and stamped or marked where possible, 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 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 consent 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 consent 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 or establishment that handles Classified Information covered by this Agreement maintains a list of individuals at the facility or establishment who are authorized to have access to such 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 receive an appropriate PSC before they are granted access to such 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 determination to grant 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 a recipient Party may be provided by the recipient Party to a Contractor or prospective Contractor whose duties require access to such information with the prior written consent 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 safeguard the 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 information are informed of their responsibilities to protect the information in accordance with applicable laws and regulations;
 - d. Carry out periodic security inspections of cleared facilities to ensure that the information is protected as required by this Agreement; and
 - e. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that access to the information is limited to those individuals who have a Need to Know.

ARTICLE 10 – CLASSIFIED CONTRACTS

1. When a Party proposes to place, or authorizes a Contractor in its country to place, a Classified Contract that is classified at the CONFIDENTIAL / ДОВЕРЛИВО level or above, 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 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 and establishments where it stores Classified Information of the other Party and shall ensure that such facilities or establishments have qualified and appropriately cleared individuals appointed with the responsibility and authority for the control and protection of such 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 approved 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 Parties.

(3) Receipts shall be prepared by the recipient 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 persons.

(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:

(1) Classified Information that is classified at the CONFIDENTIAL / ДОВЕРЛИВО level or above that is to be transferred electronically shall be transmitted using secure means that have been approved by each Party's National Security Authority.

ARTICLE 14 – VISITS TO FACILITIES AND ESTABLISHMENTS OF THE PARTIES

1. Visits by representatives of one Party to facilities and establishments 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 who possess a valid PSC.

2. Authorization to visit such facilities and establishments shall be granted only by the Party in whose territory the facility or establishment to be visited is located. The visited Party, or its designated officials, shall be responsible for advising the facility or establishment 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 in Skopje, North Macedonia, in the case of U.S. visitors, and by the Embassy of North Macedonia in Washington, D.C., in the case of visitors from North Macedonia.

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 safeguarding of Classified Information.

ARTICLE 17 – REPRODUCTION OF CLASSIFIED INFORMATION

When Classified Information is reproduced, all of the original security markings thereon shall also be reproduced, stamped, or marked on each reproduction of such information. Such reproductions shall be subject to the same controls as the original 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 information ceases to require that higher degree of protection or should be declassified as soon as the 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 consent 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 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 person 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.

ARTICLE 23 – FINAL PROVISIONS

1. This Agreement shall enter into force on the date of receipt of the latest written notification by which the Parties have informed each other, through diplomatic channels, that each Party has completed its necessary internal procedures for the entry into force of this Agreement.
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 or otherwise provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

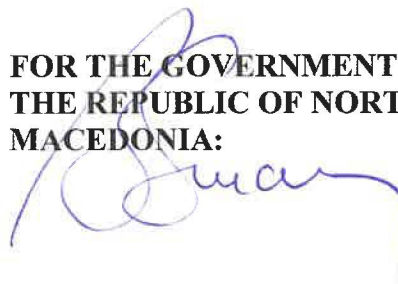
IN WITNESS WHEREOF, the undersigned, being duly authorized thereto by their respective Governments, have signed this Agreement.

Done in duplicate at Skopje this 21st day of December 2021, in the Macedonian and English languages, both texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

**FOR THE GOVERNMENT OF
THE UNITED STATES OF AMERICA:**



**FOR THE GOVERNMENT OF
THE REPUBLIC OF NORTH
MACEDONIA:**



APPENDIX

PROCEDURES FOR PROTECTING NORTH MACEDONIA ИНТЕPHO (RESTRICTED) CLASSIFIED INFORMATION PROVIDED TO THE UNITED STATES

1. Upon receipt, North Macedonia Classified Information provided to the United States and designated as “ИНТЕPHO (RESTRICTED)” shall be protected by the United States in accordance with the following procedures.
2. Information designated as “ИНТЕPHO (RESTRICTED)” shall be stored in locked containers or closed areas that prevent access by unauthorized personnel.
3. “ИНТЕPHO (RESTRICTED)” information shall not be disclosed to unauthorized persons or entities without the prior written approval of the Government of North Macedonia except as required by U.S. law, including the Freedom of Information Act.
4. “ИНТЕPHO (RESTRICTED)” 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 “ИНТЕPHO (RESTRICTED)” 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 U.S. Government establishments, 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. “ИНТЕPHO (RESTRICTED)” information shall be transmitted by first class mail within the United States in one sealed envelope. Transmission outside the United States shall be in double, sealed envelopes, with the inner envelope marked “North Macedonia ИНТЕPHO (RESTRICTED).” Transmission outside the United States shall be by traceable means such as commercial courier or other means agreed upon by the Parties in writing.
6. U.S. documents that contain “North Macedonia ИНТЕPHO (RESTRICTED)” information shall bear on the cover and the first page the marking “North Macedonia ИНТЕPHO (RESTRICTED).” The portion of the documents containing “North Macedonia ИНТЕPHO (RESTRICTED)” information also shall be identified with the same marking.
7. “ИНТЕPHO (RESTRICTED)” 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 “ИНТЕPHO (RESTRICTED)” information may be conducted if an encryption system is not available and subject to the approval of the releasing Party’s National Security Authority.

8. An FSC is not required for a Contractor to undertake contracts that require only the receipt or production of Classified Information at the “ИHTEPHO (RESTRICTED)” level.

9. Access to such “ИHTEPHO (RESTRICTED)” information shall be granted only to those individuals who have a Need to Know. A PSC is not required to access “ИHTEPHO (RESTRICTED)” information.

ДОГОВОР
МЕЃУ ВЛАДАТА НА СОЕДИНЕТИТЕ АМЕРИКАНСКИ ДРЖАВИ
И
ВЛАДАТА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
ЗА БЕЗБЕДНОСНИТЕ МЕРКИ ЗА ЗАШТИТА НА
КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

ПРЕАМБУЛА

Владата на Соединетите Американски Држави („Соединетите Држави“) и Владата на Република Северна Македонија („Северна Македонија“) (поединечно „Страна“, а колективно „Страните“);

Имајќи предвид дека Страните соработуваат во работи што вклучуваат, но не се ограничуваат на, надворешни работи, одбрана, безбедност, спроведување на законот, наука, индустрија и технологија; и

Имајќи заемен интерес во заштитата на класифицираните информации што се разменети во доверба меѓу Страните;

Се договорија за следното:

ЧЛЕН 1 - ДЕФИНИЦИИ

За целите на овој договор:

1. Класифицирана информација: Информација доставена од едната Страна на другата Страна што е означена како класифицирана од Страната испраќач за национални безбедносни цели и затоа е потребно да се заштити од неовластено откривање. Информацијата може да биде во усна, визуелна, електронска или документирана форма или во форма на материјал, вклучително опрема или технологија.
2. Класифициран договор: Договор за којшто е потребен или ќе биде потребен пристап до, или создавање на класифицирани информации од страна на контракторот или неговите вработени при реализацијата на договорот.
3. Контрактор: Поединец или правно лице што поседува правна способност да склучува договори и коешто е страна на класифициран договор.
4. Безбедносен сертификат за правно лице: Потврда издадена од Националниот безбедносен орган на една од Страните, како што е утврдено во член 4, за објектот на контракторот што е под надлежност на таа Страна во којашто е наведено дека објектот е проверен за одреден степен и има воспоставено соодветни безбедносни мерки за

одреден степен за чување класифицирани информации. Таквата потврда укажува дека контракторот за којшто е издаден безбедносен сертификат за правно лице ќе ги заштитува класифицираните информации со степен CONFIDENTIAL / ДОВЕРЛИВО или повисоко во согласност со одредбите на овој договор и дека придржувањето кон истиот ќе го следи и контролира релевантниот Национален безбедносен орган. Безбедносен сертификат за правно лице не е потребен за контрактор што реализира договори според коишто само се врши прием или создавање на класифицирани информации со степен ИНТЕРНО (RESTRICTED).

5. Безбедносен сертификат за физичко лице:

- a. Решение издадено од Националниот безбедносен орган на една од Страните, како што е утврдено во член 4, дека лицето што е вработено во владин орган на таа Страна или контрактор што е под надлежност на таа Страна има овластување за пристап до класифицирани информации до одреден степен.
 - б. Решение издадено од Националниот безбедносен орган на една од Страните, како што е утврдено во член 4, дека лицето што е државјанин на едната Страна но ќе биде вработено од другата Страна или од еден од контракторите што се под надлежност на другата Страна, има овластување за пристап до класифицирани информации до одреден степен.
6. Потребно е да знае: решение донесено од страна на овластен имател на класифицирана информација дека потенцијалниот примач на класифицираната информација има потреба од пристап до одредена класифицирана информација со цел да изврши или помага при извршувањето на законска и одобрена владина функција.

ЧЛЕН 2 – ОГРАНУВАЊЕ НА ОПСЕГОТ НА ДОГОВОРОТ

Овој договор не се применува за класифицирани информации што спаѓаат во опсегот на делување на друг договор или аранжман меѓу Страните или нивните органи којшто се однесува на заштитата на одреден производ или категорија на класифицирани информации што се разменети меѓу Страните или нивните органи, освен во случај доколку таквиот друг договор или аранжман јасно не се повика на примената на одредбите на овој договор. Овој договор исто така нема да се применува за размена на Податоци со степен на класификација, како што е дефинирано во Законот на Соединетите Држави за атомска енергија од 1954 година, и изменето („АЕА“), или на Податоци што порано имале степен на класификација коишто претставуваат податоци што се извадени од категоријата на Податоци со степен на класификација во согласност со АЕА но Соединетите Држави сè уште ги смета за податоци што се однесуваат на одбраната.

ЧЛЕН 3 – ПОСВЕТЕНОСТ НА ЗАШТИТАТА НА КЛАСИФИЦИРАНИТЕ ИНФОРМАЦИИ

1. Секоја Страна ги заштитува класифицираните информации на другата Страна во согласност со одредбите на овој договор.

2. Страната примач ги заштитува класифицираните информации на начин што е еквивалентен на заштитата што за тие класифицирани информации ја обезбедила Страната испраќач.

3. Секоја Страна брзо ја известува другата за сите промени на нејзините закони и прописи што би влијаеле на заштитата на класифицираните информации согласно овој договор. Таквите измени во националниот закон нема да влијаат на обврските што се уредени во овој договор. Во таков случај, Страните се консултираат за можните измени на овој договор или за други мерки што може да бидат соодветни за одржување на заштитата на класифицираните информации што се разменети согласно овој договор.

ЧЛЕН 4 – НАЦИОНАЛНИ БЕЗБЕДНОСНИ ОРГАНИ

1. Страните заемно се информираат за Националните безбедносни органи што се одговорни за примената на овој договор и за сите последователни промени во однос на тие органи.

2. За целите на овој договор, Национални безбедносни органи се:

а. За Соединетите Држави: Директор, Програми за меѓународна безбедност, Управа за одбранбена технологија и безбедност, Канцеларија на Потсекретарот за одбрана и политика, Министерство за одбрана на Соединетите Држави

б. За Северна Македонија: Директор, Дирекција за безбедност на класифицирани информации, Република Северна Македонија

3. Страните можат да склучуваат дополнителни аранжмани за примена на овој договор каде што можат да бидат потребни дополнителни технички безбедносни мерки за заштита на класифицираните информации што се пренесени на Страната примач преку странска воена продажба или програми за соработка за заедничко производство или заеднички развој на одбранбени средства или услуги. Таквите аранжмани за имплементација можат да вклучат Специјални безбедносни договори или Договори за индустриска безбедност.

ЧЛЕН 5 – ОПРЕДЕЛУВАЊЕ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

1. Страната испраќач ги определува, им става печат или ги обележува класифицираните информации каде за тоа постои можност како класифицирани со еден од следните национални степени за безбедносна класификација. Со цел обезбедување подеднаков третман, Страните се согласни дека следните степени за безбедносна класификација се еквивалентни:

СОЕДИНЕТИ ДРЖАВИ	СЕВЕРНА МАКЕДОНИЈА
TOP SECRET	ДРЖАВНА ТАЈНА (TOP SECRET)
SECRET	СТРОГО ДОВЕРЛИВО (SECRET)
CONFIDENTIAL	ДОВЕРЛИВО (CONFIDENTIAL)
Нема еквивалент	ИНТЕРНО (RESTRICTED)

2. За време на примената на овој договор, ако Северна Македонија достави класифицирана информација определена со степенот ИНТЕРНО (RESTRICTED) Соединетите Држави со нив ќе ракуваат во согласност со Додатокот на овој договор.

3. Класифицираните информации се определуваат, им се става печат или се обележуваат каде за тоа постои можност со името на Страната испраќач.

ЧЛЕН 6 – ОДГОВОРНОСТ ЗА КЛАСИФИЦИРАНИТЕ ИНФОРМАЦИИ

Страната примач е одговорна за заштита на сите класифицирани информации на Страната испраќач на начин којшто најмалку е еквивалентен на заштитата на класифицираните информации што ја дава Страната испраќач додека класифицираните информации се под нејзина контрола. За време на транзит, Страната испраќач е одговорна за сите класифицирани информации додека надлежноста за чување на класифицираните информации формално да биде префрлена на Страната примач.

ЧЛЕН 7 – ЗАШТИТА НА КЛАСИФИЦИРАНИТЕ ИНФОРМАЦИИ

1. Ниеден поединец нема право на пристап до класифицирани информации само по основ на чин, позиција, именување или безбедносен сертификат за физичко лице. Пристап до таквите информации се дава само на лицата коишто го исполнуваат принципот „потребно е да знае“ и коишто го поседуваат потребниот безбедносен сертификат за физичко лице во согласност со пропишаните стандарди на Страната примач.

2. Освен ако поинаку не е обезбедено со овој договор, Страната примач нема да ги отстапи класифицираните информации на Страната испраќач на која било трета страна, вклучувајќи влада, поединец, компанија, институција, организација или друг субјект на трета страна без претходна писмена согласност од Страната испраќач.

3. Страната примач нема да ги користи или да дозволи класифицираните информации на Страната испраќач да се користат за друга цел освен за онаа за којашто тие информации биле доставени без претходна писмена согласност од Страната испраќач.

4. Страната примач ги почитува приватните права што се поврзани со класифицираните информации на Страната испраќач, вклучувајќи ги правата што се однесуваат на патенти, авторски права или трговски тајни и нема да ги отстапи на користење, користи, разменува или открива таквите класифицирани информации на начин што не соодветствува на тие права без претходно писмено овластување од сопственикот на тие права.

5. Страната примач обезбедува секој објект или установа каде што се ракува со класифицирани информации согласно овој договор да води евиденција на лицата во тој објект или установа коишто имаат право на пристап до таквите информации.

6. Секоја Страна развива процедури за одговорност и контрола со цел менаџирање на дисеминацијата и пристапот до класифицирани информации.

7. Секоја Страна се придржува кон сите ограничувања за користење, откривање, отстапување на користење и пристап до класифицирани информации што можат да бидат наведени од страна на Страната испраќач кога таа ги открива класифицираните информации. Ако некоја Страна не може да се придржува кон наведените ограничувања, таа Страна веднаш се консултира со другата Страна и ги презема сите законски мерки за спречување или минимизирање на таквото користење, откривање, отстапување на користење или пристап.

ЧЛЕН 8 – БЕЗБЕДНОСНИ СЕРТИФИКАТИ ЗА ФИЗИЧКИ ЛИЦА

1. Страните обезбедуваат сите лица коишто за извршување на своите должности имаат потреба за пристап или чиишто должности или функции можат да дозволат пристап до класифицирани информации согласно овој договор да добијат соодветен безбедносен сертификат за физичко лице пред да добијат пристап до таквите информации.

2. Страната што го издава безбедносниот сертификат за физичко лице спроведува соодветна и доволно детална истрага со цел да се утврди соодветноста на лицето за пристап до класифицирани информации. Одлуката за издавање безбедносен сертификат за физичко лице ќе биде донесена во согласност на националните закони и регулативи на Страната што го издава безбедносниот сертификат.

3. Пред некое службено лице или претставник на една од Страните да отстапи на користење класифицирани информации на службено лице или претставник на другата Страна, Страната примач доставува гаранција до Страната испраќач дека тоа службено лице или претставник поседува безбедносен сертификат за физичко лице со соодветен степен на класификација и има потреба да ги знае информациите и дека Страната примач ќе ги штити тие класифицирани информации во согласност со овој договор.

ЧЛЕН 9 – ОТСТАПУВАЊЕ НА КОРИСТЕЊЕ КЛАСИФИЦИРАНИ ИНФОРМАЦИИ НА КОНТРАКТОРИ

1. Класифицираните информации што ги примила Страната примач може да ги отстапи на користење на контрактор или можен контрактор чиишто должности бараат пристап до таквите информации со претходна писмена согласност на Страната испраќач. Пред отстапувањето на користење какви било класифицирани информации на контрактор или можен контрактор, Страната примач:

а. потврдува дека таквиот контрактор или можен контрактор и објектот на контракторот имаат способност за заштита на информациите во согласност со условите на овој договор;

б. потврдува дека на таквиот контрактор или можен контрактор и на објектот на контракторот се издадени соодветни безбедносни сертификати за физичко и за правно лице, како што одговара;

в. потврдува дека таквиот контрактор или можен контрактор има воспоставено процедури што обезбедуваат сите лица што имаат пристап до информациите да бидат известени за нивните одговорности за заштита на информациите во согласност со важечките закони и регулативи;

г. спроведува периодични безбедносни инспекции на проверените објекти со цел да осигура дека информациите се штитат како што се бара со овој договор и

д. потврдува дека контракторот или можниот контрактор има воспоставено процедури што обезбедуваат дека пристапот до информациите е ограничен само на тие лица што имаат потреба да ги знаат информациите.

ЧЛЕН 10 – КЛАСИФИЦИРАНИ ДОГОВОРИ

1. Кога едната Страна предлага да склучи или овластува контрактор во нејзината држава да склучи класифициран договор со степен CONFIDENTIAL / ДОВЕРЛИВО или повисоко со контрактор во државата на другата Страна, Страната што ќе го склучи или ќе го овласти контракторот да склучи таков класифициран договор бара гаранција дека е издаден безбедносен сертификат за правно лице од страна на Националниот безбедносен орган на другата Страна. Националниот безбедносен орган на Страната од којашто се бара гаранцијата го следи безбедносното однесување на контракторот и ги презема сите потребни чекори за да обезбеди дека истото е во согласност со важечките закони и регулативи.

2. Националниот безбедносен орган на Страната којашто преговара за класифициран договор што ќе се изведува во државата на другата Страна, во класифицираниот договор ќе вклучи, ќе бара предлог или ќе договора документ со соодветни безбедносни клаузули и други релевантни одредби, вклучувајќи и трошоци за безбедноста. Ова вклучува и одредби со коишто контракторите ќе бидат обврзани да вклучат соодветни безбедносни клаузули во нивите под-договорни документи.

ЧЛЕН 11 – ОДГОВОРНОСТ ЗА ОБЈЕКТИТЕ

Секоја Страна е одговорна за безбедноста на сите владини и приватни објекти и установи каде што се чуваат класифицирани информации на другата Страна и обезбедува дека тие објекти и установи имаат квалификувани и соодветно проверени лица на коишто им е доделена одговорност и овластување да вршат контрола и заштита на таквите информации.

ЧЛЕН 12 – ЧУВАЊЕ КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Класифицираните информации што се разменети меѓу Страните се чуваат на начин што обезбедува пристап само за лицата што имаат овластен пристап.

ЧЛЕН 13 – ПРЕНОС

1. Класифицираните информации се пренесуваат меѓу Страните преку владини канали или на друг начин што однапред заемно писмено е одобрен.

2. Минималните барања за безбедност на класифицираните информации за време на преносот се:

а. Документи или други медиуми:

(1) Документите или другите медиуми што содржат класифицирани информации се пренесуваат во дупли запечатени коверти. Внатрешниот коверт ја носи само ознаката за степенот на класификација на документите или другите медиуми и службената адреса на примачот. Надворешниот коверт ја носи службената адреса на примачот, службената адреса на испраќачот и евиденцискиот број на документот, ако се применува.

(2) На надворешниот коверт не стои ознака за степенот на класификација на спакуваните документи или другите медиуми. Запечатениот дупли коверт потоа се пренесува во согласност со пропишаните процедури на Страните.

(3) Примачот подготвува потврди за прием на пратките што содржат документи или други медиуми со класифицирани информации што се разменуваат меѓу Страните, и таквите потврди ги потпишува крајниот примач и истите се враќаат до испраќачот.

б. Материјал:

(1) Материјал, вклучувајќи опрема, што содржи класифицирани информации се транспортира во запечатени, затворени возила, или се пакува на друг безбедносен начин или заштитува со цел да се спречи откривање на неговата форма, големина или содржина, и се чува под постојана контрола за да се спречи пристап од страна на неовластени лица.

(2) Материјал, вклучувајќи опрема, што содржи класифицирани информации што привремено мора да се чува заради чекање за испорака, се чува во заштитен простор за складирање. Таквиот простор се заштитува со опрема за откривање неовластен упад или со чувари со потребните безбедносни сертификати за физичко лице коишто вршат постојан надзор на тој простор. Само овластен персонал со потребниот безбедносен сертификат за физичко лице има пристап до заштитениот просторот за складирање.

(3) Потврди за прием се обезбедуваат секогаш кога материјал што содржи класифицирани информации, вклучувајќи и опрема, се примо-предава за време на транзит, а потврда за прием на таков материјал потпишува крајниот примач и истата се враќа до испраќачот.

в. Електронски пренос:

(1) Класифицираните информации што се класифицирани со степенот CONFIDENTIAL/ДОВЕРЛИВО и повисоко и што треба да пренесат по електронски пат, се пренесуваат преку заштитени средства што се одобрени на Националниот безбедносен орган на секоја од Страните.

ЧЛЕН 14 – ПОСЕТИ НА ОБЈЕКТИ И УСТАНОВИ НА СТРАНИТЕ

1. Посетите на претставници на едната Страна на објекти и установи на другата Страна за коишто е потребен пристап до класифицирани информации, или посети за коишто е потребен безбедносен сертификат за физичко лице со цел да се дозволи пристап, се

ограничуваат само на тие што се потребни за службени цели. Овластување се дава само на претставниците што поседуваат важечки безбедносен сертификат за физичко лице.

2. Овластување за посета на такви објекти и установи дава само Страната на чијашто територија е лоциран објектот или установата што се посетува. Страната што се посетува, или нејзините назначени службени лица, имаат одговорност да го советуваат објектот или установата за предложената посета и за опсегот и највисокиот степен на класифицирани информации што можат да се отстапат на користење на посетителот.

3. Барањата за посети претставниците на Страните ги доставуваат преку Амбасадата на Соединетите Држави во Скопје, Северна Македонија кога станува збор за посетители од Соединетите Држави, и преку Амбасадата на Северна Македонија во Вашингтон, Д.Ц, во случај на посетители од Северна Македонија.

ЧЛЕН 15 – БЕЗБЕДНОСНИ ПОСЕТИ

Примената на безбедносните барања што се уредени со овој договор може да се верификува преку реципрочни посети на безбедносниот персонал на Страните. На безбедносните претставници на секоја Страна, по претходна консултација, ќе им биде дозволено да ја посетат другата Страна за да дискутираат и да ги следат процедурите за имплементација на другата Страна во интерес на постигнување разумна компатибилност на безбедносните системи. Страната домаќин им помага на безбедносните претставници што се дојдени во посета при утврдувањето дали соодветно се заштитени класифицираните информации што се добиени од другата Страна.

ЧЛЕН 16 – БЕЗБЕДНОСНИ СТАНДАРДИ

На барање, секоја Страна доставува информации на другата Страна за нејзините безбедносни стандарди, практики и процедури за заштита на класифицирани информации.

ЧЛЕН 17 – РЕПРОДУКЦИЈА НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Кога се репродуцира класифицирана информација, на секоја копија на таквата информација се репродуцираат, се става печат или се обележуваат сите нејзини оригинални безбедносни ознаки. Таквите репродуцирани информации се ставаат под иста заштита како и оригиналната информација. Бројот на копии се ограничува на минималниот број потребен за службени цели.

ЧЛЕН 18 - УНИШТУВАЊЕ КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

1. Документи и други материјали што содржат класифицирани информации се уништуваат со палење, сечење со шрединг машина, гмечење или на друг начин којшто оневозможува обновување на класифицираните информации што се содржани во нив.

2. Материјал, вклучувајќи и опрема, што содржи класифицирани информации се уништува до степен на непрепознавање со цел да се исклучи можноста за обновување на класифицираните информации во целина или делумно.

ЧЛЕН 19 – РЕКЛАСИФИКАЦИЈА И ДЕКЛАСИФИКАЦИЈА

1. Страните се согласуваат дека класифицираните информации треба да се рекласифицираат веднаш штом престане потребата за повисока заштита на информацијата или треба да се декласифицираат веднаш штом престане потребата за нејзина заштита од неовластено откривање.

2. Страната испраќач има потполно дискреционо право во однос на рекласификацијата или декласификацијата на нејзините класифицирани информации. Страната примач нема да ги рекласифицира или декласифицира класифицираните информации што ги примила од Страната испраќач, без разлика на постоењето видливи насоки за декласификација на документот, без претходна писмена согласност од Страната испраќач.

ЧЛЕН 20 – ГУБЕЊЕ ИЛИ КОМПРОМИТИРАЊЕ

Страната примач веднаш ја известува Страната испраќач за секое откриено губење или компромитирање, како и за секое можно губење или компромитирање на класифицираните информации на Страната испраќач. Во случај на реално или можно губење или компромитирање на таквите информации, Страната примач веднаш започнува истрага за утврдување на околностите на настанот или можното губење или компромитирање. Резултатите од истрагата и информација за преземените мерки за спречување повторно да се случи такво нешто се доставуваат до Страната испраќач.

ЧЛЕН 21 – СПОРОВИ

Несогласувањата меѓу Страните што настануваат или се во врска со овој договор се решаваат единствено преку консултации меѓу Страните и нема да се изнесуваат пред национален суд, меѓународен трибунал или друго трето лице или субјект за решавање.

ЧЛЕН 22 – ТРОШОЦИ

Секоја Страна е одговорна за покривање на своите трошоци настанати со примената на овој договор. Сите обврски на Страните согласно овој договор се предмет на расположливоста на средства.

ЧЛЕН 23 – ФИНАЛНИ ОДРЕДБИ

1. Овој договор влегува во сила на датумот на приемот на последното писмено известување со кое Страните взаемно по дипломатски пат се известуваат дека секоја Страна ги завршила потребните внатрешни процедури за влегување во сила на овој договор.

2. Секоја од Страните може да го раскине овој договор преку писмено известување на другата Страна по дипломатски пат деведесет дена однапред за својата намера да го раскине Договорот.

3. Без оглед на раскинувањето на овој договор, сите класифицирани информации што се разменети или отстапени на користење на друг начин согласно овој договор продолжуваат да се заштитуваат во согласност со одредбите што се содржани во него.

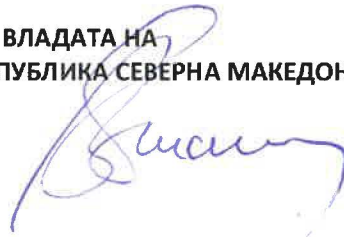
ЗА ПОТВРДА НА ТОА долупотпишаните, соодветно овластени од страна на нивните влади, го потпишаа овој договор.

Потпишан во дупликат во Скопје на 21-иот ден од месец декември, 2021-та година на англиски и на македонски јазик, од коишто и двата јазици се подеднакво веродостојни. Во случај на разлики во толкувањето, ќе преовлада текстот на англиски јазик.

**ЗА ВЛАДАТА НА
СОЕДИНЕНИТЕ АМЕРИКАНСКИ ДРЖАВИ:**



**ЗА ВЛАДАТА НА
РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА:**



ДОДАТОК

ПРОЦЕДУРИ ЗА ЗАШТИТА НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ НА СЕВЕРНА МАКЕДОНИЈА СО СТЕПЕН ИНТЕРНО (RESTRICTED) ДОСТАВЕНИ ДО СОЕДИНЕТИТЕ ДРЖАВИ

1. При прием, Соединетите Држави ги заштитуваат класифицираните информации на Северна Македонија со степен „ИНТЕРНО (RESTRICTED)“ согласно следните процедури.
2. Информациите со степен „ИНТЕРНО (RESTRICTED)“ се чуваат во заклучени ормари или затворени зони коишто спречуваат пристап од неовластен персонал.
3. Информации со степен „ИНТЕРНО (RESTRICTED)“ не се откриваат на неовластени лица или субјекти без претходно писмено одобрение од Владата на Северна Македонија освен како што се бара со закон на Соединетите Држави, вклучувајќи го и Законот за слобода на информациите.
4. Информациите со степен „ИНТЕРНО (RESTRICTED)“ се чуваат, обработуваат или пренесуваат електронски преку користење владини системи или системи акредитирани од страна на контрактор, онака што е применливо. Особено, пред некој систем да се користи за чување, обработка или пренесување информации со степен „ИНТЕРНО (RESTRICTED)“ претходно мора да добие безбедносно одобрение, познато како акредитација. Акредитацијата е формална изјава на соодветно тело за акредитација со којашто се потврдува дека за користење на системот се исполнети соодветни безбедносни барања и истото не претставува неприфатлив ризик. Безбедносните стандардни оперативни процедури претставуваат технички процедури за имплементација на безбедносните политики и барања што се специфични за објектот за заштита на автоматизирани информации системи низ коишто се обработуваат класифицирани информации. За самостојни автоматизирани информациски системи како што се десктоп и лаптоп компјутерите што се користат во владините установи на Соединетите Држави, документот за регистрирање на системот заедно со Безбедносните стандардни оперативни процедури имаат улога на потребната акредитација. За контракторите, во клаузулата за потребите за ограничени услови во договорот се вклучуваат насоки за користењето комуникациски и информациски системи.
5. Информациите со степен „ИНТЕРНО (RESTRICTED)“ во Соединетите Држави се пренесуваат со пошта од прва класа во еден запечатен коверт. Преносот надвор од Соединетите Држави се врши во дупли, запечатени коверти, при што на внатрешниот коверт стои ознаката „Северна Македонија ИНТЕРНО (RESTRICTED)“. Преносот надвор од Соединетите Држави се врши на начин што може да се следи како што е комерцијален доставувач или на друг начин писмено договорен меѓу Страните.
6. Документите на Соединетите Држави што содржат информации означени „Северна Македонија ИНТЕРНО (RESTRICTED)“ на пропратното писмо и на првата страна ја носат ознаката „Северна Македонија ИНТЕРНО (RESTRICTED)“. Делот од документите што содржат информации „Северна Македонија ИНТЕРНО (RESTRICTED)“ се идентификува со истата ознака.

7. Информациите со степен „ИНТЕРНО (RESTRICTED)“ можат електронски да се пренесуваат или до нив да се пристапи преку јавна мрежа како што е Интернетот со користење владини или комерцијални уреди за енкрипција коишто заемно се договорени меѓу Страните. Телефонски разговори, видео конференции или пренос на факсови што содржат информации со степен „ИНТЕРНО (RESTRICTED)“ може да се реализираат ако нема систем за енкрипција по одобрение на Националниот безбедносен орган на Страната испраќач.

8. Безбедносен сертификат за правно лице не е потребен за контрактор да реализира договори според коишто само се врши прием или создавање на класифицирани информации со степен „ИНТЕРНО (RESTRICTED)“.

9. Пристап до таквите информации со степен „ИНТЕРНО (RESTRICTED)“ се дава само на лица согласно принципот „потребно да знае“. Безбедносен сертификат за физичко лице не е потребен за пристап до информации со степен „ИНТЕРНО (RESTRICTED)“.