DEFENSE

Protection of Information

Agreement Between the
UNITED STATES OF AMERICA
and GEORGIA

Signed at Washington May 9, 2017

with

Appendix

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."

GEORGIA

Defense: Protection of Information

Agreement signed at Washington
May 9, 2017;
Entered into force December 18, 2017.
With appendix.

AGREEMENT BETWEEN
THE GOVERNMENT OF THE UNITED STATES OF AMERICA
AND
THE GOVERNMENT OF GEORGIA
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 Georgia ("Georgia") (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 (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 safeguard Classified Information. Such a certification shall signify that Classified Information at the CONFIDENTIAL 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. In the case of the United States, an FSC is not required for a Contractor to undertake

Contracts that only require the receipt or production of Classified Information at the 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 state 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 function of the Party or Parties.

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. 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 Georgia: The State Security Service of Georgia.

2. The Parties shall inform each other of any subsequent changes to these Authorities.

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, to include programs involving 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	GEORGIA
TOP SECRET	განსაკუთრებული მნიშვნელობის (GANSAKUTREBULI MNISHVNELOBIS) / TOP SECRET
SECRET	სრულიად საიდუმლო (SRULIAD SAIDUMLO) / SECRET
CONFIDENTIAL	საიდუმლო (SAIDUMLO) / CONFIDENTIAL
NO EQUIVALENT	შეზღუდული სარგებლობისათვის (SHEZGUDULI SARGEBLOBISATVIS) / RESTRICTED

2. During the implementation of this Agreement, if Georgia in accordance with its domestic law provides Classified Information designated as 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 national 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 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 national 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 state 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 transmission: Classified Information that is classified at the CONFIDENTIAL 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 Tbilisi in the case of U.S. visitors, and by the Embassy of Georgia in Washington, D.C., in the case of Georgian visitors.

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

1. Reproduction, which includes translations or copies, of Classified Information shall be in accordance with the requirements of applicable national laws and regulations of the Party reproducing the Classified Information and this Article.

2. 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. Destruction of Classified Information shall be in accordance with the requirements of applicable national laws and regulations of the Party destroying the Classified Information and this Article.

2. 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.

3. 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 – AMENDMENTS

This Agreement shall be amended only by mutual agreement of the Parties. Any such amendments shall be concluded as a separate document, which shall enter into force in accordance with Paragraph 1 of Article 24 of this Agreement.

ARTICLE 24 – FINAL PROVISIONS

1. This Agreement and any amendments to this Agreement shall enter into force on the date of the later note in an exchange of diplomatic notes by which the Parties indicate 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 Washington this 9th day of May, 2017 in the English and Georgian 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 GEORGIA:

APPENDIX

PROCEDURES FOR PROTECTING RESTRICTED INFORMATION PROVIDED BY GEORGIA TO THE UNITED STATES

1. Upon receipt, Georgia Classified Information provided to the United States at the RESTRICTED level shall be protected by the United States in accordance with the following minimum procedures.

2. Information designated as RESTRICTED shall be stored in locked containers or closed areas that prevent access by unauthorized personnel.

3. The United States shall take all available steps short of classification to protect RESTRICTED information provided by Georgia from disclosure to unauthorized persons or entities without prior written approval of Georgia.

4. 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 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. 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 "GEORGIA 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 RESTRICTED information shall bear on the cover and the first page the marking "GEORGIA RESTRICTED." The portion of the documents containing RESTRICTED information also shall be identified with the marking "GEORGIA RESTRICTED."

7. RESTRICTED information may be transmitted or accessed electronically via a network like the Internet using government or commercial encryption devices mutually accepted by the Parties. Telephone conversations, video conferencing, or facsimile transmissions containing

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 RESTRICTED level.

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

შეთანხმება
ამერიკის შეერთებული შტატების მთავრობასა
და
საქართველოს მთავრობას შორის
საიდუმლო ინფორმაციის დაცვის უსაფრთხოების ზომების
შესახებ

პრეამბულა

ამერიკის შეერთებული შტატების („შეერთებული შტატები“) მთავრობა და საქართველოს („საქართველო“) მთავრობა (თითოეული - „მხარე“ და ერთობლივად - „მხარეები“),

ითვალისწინებენ რა, რომ მხარეები თანამშრომლობენ ისეთ საკითხებში, რომლებიც მოიცავს, თუმცა არ შემოიფარგლება საგარეო საქმეების, თავდაცვის, უსაფრთხოების, სამართალდაცვითი, სამეცნიერო, სამრეწველო და ტექნოლოგიური საკითხებით, და

აქვთ რა მხარეთა შორის კონფიდენციალურად გაცვლილი საიდუმლო ინფორმაციის დაცვის ორმხრივი ინტერესი,

შეთანხმდნენ შემდეგზე:

მუხლი 1 - ტერმინთა განმარტება

წინამდებარე შეთანხმების მიზნებისათვის:

1. <u>საიდუმლო ინფორმაცია</u>: ერთი მხარის მიერ მეორე მხარისთვის მიწოდებული ინფორმაცია, რომელიც, ეროვნული უსაფრთხოების მიზნებისთვის, მიმწოდებელი მხარის მიერ მიჩნეულია საიდუმლოდ და, შესაბამისად, საჭიროებს დაცვას არაუფლებამოსილი გამჟღავნებისგან. ეს ინფორმაცია შეიძლება არსებობდეს ზეპირი, ვიზუალური, ელექტრონული ან დოკუმენტის ფორმით, ან მასალის, მათ შორის აღჭურვილობის ან ტექნოლოგიის, ფორმით.

2. <u>საიდუმლო კონტრაქტი</u>: კონტრაქტი, რომელიც საჭიროებს ან სამომავლოდ მოითხოვს კონტრაქტორის ან მისი დასაქმებულების მიერ საიდუმლო ინფორმაციის გაცნობას ან მის შექმნას, კონტრაქტის შესრულების პროცესში.

3. <u>კონტრაქტორი</u>: ფიზიკური ან იურიდიული პირი, რომელიც ფლობს კონტრაქტების დადების უფლებამოსილებას და წარმოადგენს საიდუმლო კონტრაქტის მხარეს.

4. <u>საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვება</u>: მხარის, მე-4 მუხლით განსაზღვრული, ეროვნული უსაფრთხოების ორგანოს მიერ მხარის იურისდიქციაში მყოფი კონტრაქტორის ობიექტისადმი გაცემული სერთიფიკატი, რომელიც მოწმობს, რომ ობიექტი შემოწმებულია საიდუმლოობის განსაზღვრულ ხარისხზე და, ასევე, ფლობს საიდუმლოობის განსაზღვრული ხარისხის სათანადო უსაფრთხოების გარანტიებს, რათა დაიცვას საიდუმლო ინფორმაცია. ასეთ სერთიფიკატში უნდა აღინიშნოს, რომ კონტრაქტორი დაიცავს CONFIDENTIAL ან უფრო მაღალი საიდუმლოობის ხარისხის მქონე საიდუმლო ინფორმაციას, რისთვისაც გაიცემა საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვება, წინამდებარე შეთანხმების დებულებების შესაბამისად, და რომ შესრულების მონიტორინგსა და აღსრულებას განახორციელებს შესაბამისი ეროვნული უსაფრთხოების ორგანო. შეერთებული შტატების შემთხვევაში, კონტრაქტორს არ მოეთხოვება საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვება ისეთი კონტრაქტების დასადებად, რომლებიც საჭიროებს მხოლოდ RESTRICTED საიდუმლოობის ხარისხის მქონე საიდუმლო ინფორმაციის მიღებას ან შექმნას.

5. <u>საიდუმლო ინფორმაციასთან ინდივიდუალური დაშვება</u>:

a. მხარის, მე-4 მუხლით განსაზღვრული, ეროვნული უსაფრთხოების ორგანოს გადაწყვეტილება, რომლის თანახმად, ამ მხარის სახელმწიფო ორგანოს მიერ, ან ამ მხარის იურისდიქციაში მყოფი კონტრაქტორის მიერ დასაქმებულ ფიზიკურ პირს აქვს საიდუმლოობის განსაზღვრულ ხარისხამდე საიდუმლო ინფორმაციის გაცნობის უფლება.

b. მხარის, მე-4 მუხლით განსაზღვრული, ეროვნული უსაფრთხოების ორგანოს გადაწყვეტილება, რომლის თანახმად, ფიზიკურ პირს, რომელიც ერთ-ერთი მხარის მოქალაქეა, მაგრამ უნდა დასაქმდეს მეორე მხარის მიერ, ან მეორე მხარის ერთ-ერთი კონტრაქტორის მიერ, აქვს საიდუმლოობის განსაზღვრულ ხარისხამდე საიდუმლო ინფორმაციის გაცნობის უფლება.

<u>ინფორმაციის გაცნობის საჭიროება</u>: საიდუმლო ინფორმაციის უფლებამოსილი მფლობელის მიერ მიღებული გადაწყვეტილება, რომლის თანახმად, საიდუმლო ინფორმაციის შესაძლო მიმღები საჭიროებს კონკრეტული საიდუმლო ინფორმაციის გაცნობას, რათა შეასრულოს ან ხელი შეუწყოს მხარის ან მხარეების კანონიერ და ნებადართულ საქმიანობას.

მუხლი 2 - შეთანხმების სამოქმედო სფეროს შეზღუდვები

წინამდებარე შეთანხმება არ გამოიყენება მხარეებს ან მათ ორგანოებს შორის დადებული იმ სხვა შეთანხმებების ან ხელშეკრულებების ფარგლებით გათვალისწინებული საიდუმლო ინფორმაციის მიმართ, რომლებიც ადგენენ მხარეებს ან მათ ორგანოებს შორის გაცვლილი საიდუმლო ინფორმაციის კონკრეტული კატეგორიის ან ნივთის დაცვას, გარდა იმ შემთხვევებისა, როცა ასეთი სხვა შეთანხმება ან ხელშეკრულება პირდაპირ მიუთითებს

წინამდებარე შეთანხმების პირობების გამოყენებაზე. წინამდებარე შეთანხმება, ასევე, არ გამოიყენება, „შეერთებული შტატების ატომური ენერგიის შესახებ“ 1954 წლის აქტითა და მისი ცვლილებებით („AEA“) განსაზღვრული, „შეზღუდული მონაცემების“ (Restricted Data) გაცვლის მიმართ, ან „ყოფილი შეზღუდული მონაცემების“ (Formerly Restricted Data) მიმართ, რომლებიც წარმოადგენს „შეზღუდული მონაცემების“ (Restricted Data) კატეგორიიდან, AEA-ს შესაბამისად, ამოღებულ მონაცემებს, თუმცა, შეერთებული შტატების მიერ, რომლებიც კვლავ მიიჩნევა თავდაცვით ინფორმაციად.

მუხლი 3 - საიდუმლო ინფორმაციის დაცვის ვალდებულება

1. თითოეულმა მხარემ უნდა დაიცვას მეორე მხარის საიდუმლო ინფორმაცია ქვემოთ მოცემული პირობების შესაბამისად.

2. მიმღებმა მხარემ იმგვარად უნდა დაიცვას საიდუმლო ინფორმაცია, რაც, სულ მცირე, ეკვივალენტური იქნება საიდუმლო ინფორმაციისთვის მიმწოდებელი მხარის მიერ მინიჭებული დაცვის.

3. თითოეულმა მხარემ დაუყოვნებლივ უნდა შეატყობინოს მეორე მხარეს საკუთარი შიდასახელმწიფოებრივი კანონმდებლობის ნებისმიერი ცვლილების შესახებ, რაც გავლენას მოახდენს წინამდებარე შეთანხმების ფარგლებში საიდუმლო ინფორმაციის დაცვაზე. შიდასახელმწიფოებრივ კანონმდებლობაში ასეთმა ცვლილებებმა გავლენა არ უნდა მოახდინოს წინამდებარე შეთანხმებით გათვალისწინებულ ვალდებულებებზე. ასეთ შემთხვევაში მხარეები კონსულტაციას გამართავენ წინამდებარე შეთანხმებაში შესაძლო ცვლილებების შეტანის ან სხვა ზომების შესახებ, რაც ადეკვატური იქნება წინამდებარე შეთანხმების ფარგლებში გაცვლილი საიდუმლო ინფორმაციის დაცვის შესანარჩუნებლად.

მუხლი 4 - ეროვნული უსაფრთხოების ორგანოები

1. წინამდებარე შეთანხმების მიზნებისათვის, ეროვნული უსაფრთხოების ორგანოები არიან:

   a. შეერთებული შტატებისთვის: საერთაშორისო უსაფრთხოების პროგრამების დირექტორი, თავდაცვის ტექნოლოგიების უსაფრთხოების ადმინისტრაცია, თავდაცვის პოლიტიკის მდივნის მოადგილის ოფისი, შეერთებული შტატების თავდაცვის დეპარტამენტი;

   b. საქართველოსთვის: საქართველოს სახელმწიფო უსაფრთხოების სამსახური.

2. მხარეები ერთმანეთს აცნობებენ ამ ორგანოების ნებისმიერი შემდგომი ცვლილების შესახებ.

3. როდესაც უცხოური სამხედრო გაყიდვების, ან თანამშრომლობის პროგრამების საშუალებით, რომლებიც მოიცავს თავდაცვითი მასალის ან მომსახურების ერთობლივად შექმნის ან ერთობლივად განვითარების შემცველ პროგრამებს, მიმღები მხარისთვის გადაცემული საიდუმლო ინფორმაციის დასაცავად შეიძლება საჭირო გახდეს დამატებითი ტექნიკური უსაფრთხოების ზომების მიღება, მხარეებმა შეიძლება დადონ წინამდებარე შეთანხმების დამატებითი საიმპლემენტაციო წესები. ასეთი საიმპლემენტაციო წესები შეიძლება მოიცავდეს უსაფრთხოების სპეციალურ შეთანხმებებს ან სამეწარმეო უსაფრთხოების შეთანხმებებს.

მუხლი 5 - საიდუმლო ინფორმაციის განსაზღვრა

1. მიმწოდებელმა მხარემ უნდა განსაზღვროს და, შესაძლებლობის ფარგლებში, აღნიშნოს ან მიუთითოს, რომ საიდუმლო ინფორმაცია დასაიდუმლოებულია ეროვნული საიდუმლოობის ერთ-ერთი შემდეგი ხარისხით. ეკვივალენტური მოპყრობის უზრუნველყოფის მიზნით, მხარეები თანხმდებიან, რომ საიდუმლოობის შემდეგი ხარისხები ეკვივალენტურია:

შეერთებული შტატები	საქართველო
TOP SECRET	განსაკუთრებული მნიშვნელობის (GANSAKUTREBULI MNISHVNELOBIS) / TOP SECRET
SECRET	სრულიად საიდუმლო (SRULIAD SAIDUMLO) / (SECRET)
CONFIDENTIAL	საიდუმლო (SAIDUMLO) / (CONFIDENTIAL)
არ არსებობს ეკვივალენტური ხარისხი	შეზღუდული სარგებლობისათვის (SHEZGUDULI SARGEBLOBISATVIS) / (RESTRICTED)

2. წინამდებარე შეთანხმების შესრულების პროცესში, თუ საქართველო, საკუთარი შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად, გასცემს RESTRICTED საიდუმლოობის ხარისხით განსაზღვრულ საიდუმლო ინფორმაციას, შეერთებული შტატები მას უნდა მოეპყრას წინამდებარე შეთანხმების დანართის შესაბამისად.

3. საიდუმლო ინფორმაციაზე უნდა განისაზღვროს და, შესაძლებლობის ფარგლებში, აღინიშნოს ან მიეთითოს მიმწოდებელი მხარის სახელი.

მუხლი 6 - პასუხისმგებლობა საიდუმლო ინფორმაციაზე

მიმღები მხარე პასუხისმგებელია მიმწოდებელი მხარის ყველა საიდუმლო ინფორმაციის დაცვაზე იმგვარად, რაც, სულ მცირე, ეკვივალენტურია საიდუმლო ინფორმაციისთვის

მიმწოდებელი მხარის მიერ მინიჭებული დაცვის, როდესაც საიდუმლო ინფორმაცია მისი კონტროლის ქვეშ არის. ტრანზიტის დროს მიმწოდებელი მხარე პასუხისმგებელია ყველა საიდუმლო ინფორმაციაზე, სანამ საიდუმლო ინფორმაციაზე კონტროლი ფორმალურად არ გადავა მიმღებ მხარეზე.

მუხლი 7 - საიდუმლო ინფორმაციის დაცვა

1. არც ერთ ფიზიკურ პირს არ უნდა ჰქონდეს საიდუმლო ინფორმაციის გაცნობის უფლება მხოლოდ რანგის, პოზიციის, თანამდებობის ან საიდუმლო ინფორმაციასთან ინდივიდუალური დაშვების საფუძველზე. ასეთი ინფორმაციის გაცნობის უფლება უნდა მიენიჭოს მხოლოდ იმ ფიზიკურ პირებს, რომლებსაც აქვთ ინფორმაციის გაცნობის საჭიროება და რომლებსაც მინიჭებული აქვთ საიდუმლო ინფორმაციასთან აუცილებელი ინდივიდუალური დაშვება, მიმღები მხარის მიერ განსაზღვრული სტანდარტების შესაბამისად.

2. თუ წინამდებარე შეთანხმებით სხვაგვარად არ არის განსაზღვრული, მიმღებმა მხარემ მიმწოდებელი მხარის საიდუმლო ინფორმაცია არ უნდა გადასცეს ნებისმიერ მესამე მხარეს, მათ შორის, ნებისმიერი მესამე მხარის მთავრობას, ფიზიკურ პირს, ფირმას, ინსტიტუტს, ორგანიზაციას ან სხვა ერთეულს, მიმწოდებელი მხარის წინასწარი წერილობითი თანხმობის გარეშე.

3. მიმღებმა მხარემ მიმწოდებელი მხარის საიდუმლო ინფორმაცია არ უნდა გამოიყენოს ან არ უნდა დართოს ნება, რომ ის გამოყენებულ იქნას სხვა ნებისმიერი მიზნით, გარდა იმ მიზნებისა, რისთვისაც ის იქნა მიწოდებული, მიმწოდებელი მხარის წინასწარი წერილობითი თანხმობის გარეშე.

4. მიმღებმა მხარემ პატივი უნდა სცეს მიმწოდებელი მხარის საიდუმლო ინფორმაციასთან დაკავშირებულ ნებისმიერ კერძო უფლებას, მათ შორის, საპატენტო, საავტორო უფლებებთან ან სავაჭრო საიდუმლოებასთან დაკავშირებულ უფლებებს, და არ უნდა გასცეს, გამოიყენოს, გაცვალოს ან გაამჟღავნოს ასეთი საიდუმლო ინფორმაცია აღნიშნული უფლებების დარღვევით, ამ უფლებების მფლობელის წინასწარი წერილობითი ნებართვის გარეშე.

5. მიმღებმა მხარემ უნდა უზრუნველყოს, რომ თითოეული ობიექტი ან დაწესებულება, რომელიც ახორციელებს წინამდებარე შეთანხმებით გათვალისწინებულ საიდუმლო ინფორმაციასთან მოპყრობას, აწარმოებს ობიექტის ან დაწესებულების იმ ფიზიკურ პირთა ნუსხას, რომლებსაც აქვთ ასეთი ინფორმაციის გაცნობის უფლება.

6. თითოეულმა მხარემ უნდა შეიმუშავოს პასუხისმგებლობისა და კონტროლის პროცედურები, რათა მართოს საიდუმლო ინფორმაციის გავრცელება და მისი გაცნობა.

7. თითოეულმა მხარემ უნდა დაიცვას საიდუმლო ინფორმაციის გამოყენების, გამჟღავნების, გაცემისა და გაცნობის ნებისმიერი და ყველა შეზღუდვა, რაც შეიძლება განისაზღვროს მიმწოდებელი მხარის მიერ, მის მიერ ასეთი საიდუმლო ინფორმაციის გამჟღავნებისას. თუ მხარეს არ შეუძლია მოცემული შეზღუდვების დაცვა, ამ მხარემ დაუყოვნებლივ კონსულტაცია უნდა გაიაროს მეორე მხარესთან და უნდა მიიღოს ყველა კანონიერი ზომა, რათა თავიდან აიცილოს ან შეამციროს ნებისმიერი ასეთი გამოყენება, გამჟღავნება, გაცემა ან გაცნობა.

მუხლი 8 - საიდუმლო ინფორმაციასთან ინდივიდუალური დაშვება

1. მხარეებმა უნდა უზრუნველყონ, რომ ყველა ფიზიკური პირი, რომელიც თავისი ოფიციალური საქმიანობის განხორციელებისას საჭიროებს, ან რომლის საქმიანობამ ან ფუნქციებმა შეიძლება განაპირობოს საიდუმლო ინფორმაციის გაცნობა წინამდებარე შეთანხმების შესაბამისად, მიიღებს საიდუმლო ინფორმაციასთან შესაბამის ინდივიდუალურ დაშვებას, სანამ მათ მიენიჭებათ ასეთი ინფორმაციის გაცნობის უფლება.

2. მხარემ, რომელიც ანიჭებს საიდუმლო ინფორმაციასთან ინდივიდუალურ დაშვებას, უნდა ჩაატაროს სათანადო და საკმარისად დეტალური შემოწმება, რათა განსაზღვროს ფიზიკური პირის შესაბამისობა საიდუმლო ინფორმაციის გასაცნობად. საიდუმლო ინფორმაციასთან ინდივიდუალური დაშვების მინიჭების საკითხი გადაწყდება მიმნიჭებელი მხარის შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად.

3. სანამ ერთი მხარის ოფიციალური პირი ან წარმომადგენელი საიდუმლო ინფორმაციას გადასცემს მეორე მხარის ოფიციალურ პირს ან წარმომადგენელს, მიმღებმა მხარემ მიმწოდებელ მხარეს უნდა წარუდგინოს დადასტურება, რომ ოფიციალური პირი ან წარმომადგენელი ფლობს საიდუმლო ინფორმაციასთან აუცილებელი საიდუმლოობის ხარისხის მქონე ინდივიდუალურ დაშვებას და აქვს ინფორმაციის გაცნობის საჭიროება, და რომ საიდუმლო ინფორმაცია დაცული იქნება მიმღები მხარის მიერ, წინამდებარე შეთანხმების შესაბამისად.

მუხლი 9 - საიდუმლო ინფორმაციის გადაცემა კონტრაქტორებისთვის

1. მიმღები მხარის მიერ მიღებული საიდუმლო ინფორმაცია, მიმწოდებელი მხარის წინასწარი წერილობითი თანხმობით, მიმღებმა მხარემ შეიძლება გადასცეს კონტრაქტორს ან შესაძლო კონტრაქტორს, რომლის საქმიანობა საჭიროებს ასეთი ინფორმაციის გაცნობას. კონტრაქტორისთვის ან შესაძლო კონტრაქტორისთვის ნებისმიერი საიდუმლო ინფორმაციის გადაცემამდე, მიმღებმა მხარემ უნდა:

a. დაადასტუროს, რომ ასეთ კონტრაქტორს ან შესაძლო კონტრაქტორს და კონტრაქტორის ობიექტს აქვს ინფორმაციის დაცვის შესაძლებლობა, წინამდებარე შეთანხმების პირობების შესაბამისად;

b. დაადასტუროს, რომ ასეთ კონტრაქტორს ან შესაძლო კონტრაქტორს და კონტრაქტორის ობიექტს მინიჭებული აქვს საიდუმლო ინფორმაციასთან შესაბამისი ინდივიდუალური დაშვება და იურიდიული პირის დაშვება, საჭიროების მიხედვით;

c. დაადასტუროს, რომ კონტრაქტორს ან შესაძლო კონტრაქტორს აქვს პროცედურები, უზრუნველყოს, რომ ყველა ფიზიკური პირი, რომელსაც აქვს ინფორმაციის გაცნობის უფლება, ინფორმირებულია, მოქმედი შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად, ინფორმაციის დაცვის საკუთარი პასუხისმგებლობის შესახებ;

d. განახორციელოს შემოწმებული ობიექტების უსაფრთხოების პერიოდული შემოწმებები, რათა უზრუნველყოს, რომ ინფორმაცია დაცულია წინამდებარე შეთანხმების მოთხოვნების შესაბამისად; და

e. დაადასტუროს, რომ კონტრაქტორს ან შესაძლო კონტრაქტორს აქვს პროცედურები, უზრუნველყოს, რომ ინფორმაციის გაცნობის უფლება შეზღუდულია იმ ფიზიკური პირებით, რომლებსაც აქვთ ინფორმაციის გაცნობის საჭიროება.

მუხლი 10 - საიდუმლო კონტრაქტები

1. როდესაც მხარე გამოდის ინიციატივით, ან უფლებას ანიჭებს მის ქვეყანაში არსებულ კონტრაქტორს, მეორე მხარის ქვეყანაში არსებულ კონტრაქტორთან დადოს CONFIDENTIAL ან უფრო მაღალი საიდუმლოობის ხარისხით დასაიდუმლოებული საიდუმლო კონტრაქტი, მხარემ, რომელიც დებს ან კონტრაქტორს ანიჭებს ასეთი საიდუმლო კონტრაქტის დადების უფლებას, უნდა მოითხოვოს დადასტურება, რომ მეორე მხარის ეროვნული უსაფრთხოების ორგანოს მიერ გაცემულ იქნა საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვება. მოთხოვნის მიმღები მხარის ეროვნულმა უსაფრთხოების ორგანომ მონიტორინგი უნდა გაუწიოს და მიიღოს ყველა სათანადო ზომა, რათა უზრუნველყოს, რომ კონტრაქტორის მიერ უსაფრთხოების განხორციელება მოხდეს მოქმედი შიდასახელმწიფოებრივი კანონმდებლობის შესაბამისად.

2. იმ მხარის ეროვნულმა უსაფრთხოების ორგანომ, რომელიც მოლაპარაკებებს აწარმოებს მეორე მხარის ქვეყანაში საიდუმლო კონტრაქტის შესრულების თაობაზე, საიდუმლო კონტრაქტში, ინიციატივის შესახებ მოთხოვნაში ან ქვეკონტრაქტის დოკუმენტში უნდა გაითვალისწინოს უსაფრთხოების შესაბამისი პუნქტები და სხვა სათანადო დებულებები, მათ შორის, ხარჯები უსაფრთხოებისთვის. ეს მოიცავს დებულებებს, რომლებიც ნებისმიერ კონტრაქტორს ავალდებულებს, რომ თავისი ქვეკონტრაქტის დოკუმენტებში გაითვალისწინოს უსაფრთხოების შესაბამისი პუნქტები.

მუხლი 11 - პასუხისმგებლობა ობიექტებზე

თითოეული მხარე პასუხისმგებელია ყველა იმ სახელმწიფო და კერძო ობიექტისა და დაწესებულების უსაფრთხოებაზე, სადაც ის ინახავს მეორე მხარის საიდუმლო ინფორმაციას, და უზრუნველყოფს, რომ ასეთ ობიექტებსა თუ დაწესებულებებში დანიშნულნი იყვნენ კვალიფიციური და სათანადოდ შემოწმებული ფიზიკური პირები, რომელთა პასუხისმგელობას და უფლებამოსილებას წარმოადგენს ასეთი ინფორმაციის კონტროლი და დაცვა.

მუხლი 12 - საიდუმლო ინფორმაციის შენახვა

მხარეთა შორის გაცვლილი საიდუმლო ინფორმაცია შენახული უნდა იქნას იმგვარად, რაც უზრუნველყოფს მის გაცნობას მხოლოდ იმ ფიზიკური პირების მიერ, რომლებსაც მინიჭებული აქვთ გაცნობის უფლება.

მუხლი 13 - მიწოდება

1. მხარეთა შორის საიდუმლო ინფორმაციის მიწოდება უნდა განხორციელდეს მთავრობათაშორისი არხების ან წინასწარ, ორმხრივად, წერილობით შეთანხმებული სხვა არხების საშუალებით.

2. მიწოდების დროს საიდუმლო ინფორმაციის უსაფრთხოების მიმართ არსებული მინიმალური მოთხოვნები შემდეგია:

a. დოკუმენტები ან ინფორმაციის მატარებელი სხვა საშუალებები:

(1) საიდუმლო ინფორმაციის შემცველი დოკუმენტების ან ინფორმაციის მატარებელი სხვა საშუალებების მიწოდება უნდა მოხდეს ორმაგი, დალუქული კონვერტით. შიდა კონვერტზე უნდა აღინიშნოს მხოლოდ დოკუმენტების ან ინფორმაციის მატარებელი სხვა საშუალებების საიდუმლოობის ხარისხი და განსაზღვრული მიმღების ორგანიზაციის მისამართი. გარე კონვერტზე უნდა აღინიშნოს განსაზღვრული მიმღების ორგანიზაციის მისამართი, გამგზავნის ორგანიზაციის მისამართი და დოკუმენტის საკონტროლო ნომერი, ასეთის არსებობის შემთხვევაში.

(2) გარე კონვერტზე არანაირი აღნიშვნა არ უნდა გაკეთდეს მასში არსებული დოკუმენტების ან ინფორმაციის მატარებელი სხვა საშუალებების საიდუმლოობის ხარისხის შესახებ. ორმაგი დალუქული კონვერტის მიწოდება უნდა განხორციელდეს მხარეთა მიერ დადგენილი პროცედურების შესაბამისად.

(3) ამანათებისთვის, რომლებიც მოიცავს მხარეთა შორის გადაცემული საიდუმლო ინფორმაციის შემცველ დოკუმენტებს ან ინფორმაციის მატარებელ სხვა საშუალებებს, მიმღებმა უნდა მოამზადოს მიღების დამადასტურებელი ჩანაწერები, მიღების

დამადასტურებელ ამგვარ ჩანაწერებს ხელი უნდა მოაწეროს საბოლოო მიმღებმა და ისინი უნდა დაუბრუნდეს გამგზავნს.

b. მასალა:

(1) საიდუმლო ინფორმაციის შემცველი მასალის, მათ შორის აღჭურვილობის, ტრანსპორტირება უნდა განხორციელდეს დალუქული, დახურული სატრანსპორტო საშუალებებით, ან სხვაგვარად უსაფრთხოდ უნდა შეიფუთოს ან იქნეს დაცული, რათა მოხდეს მისი ფორმის, ზომის ან შემადგენლობის იდენტიფიცირების თავიდან აცილება, და უნდა იმყოფებოდეს მუდმივი კონტროლის ქვეშ, რათა მოხდეს არაუფლებამოსილი პირების მიერ მასზე წვდომის პრევენცია.

(2) გასაგზავნად გამზადებული საიდუმლო ინფორმაციის შემცველი მასალის, მათ შორის აღჭურვილობის, დროებითი შენახვა უნდა მოხდეს შესანახად დაცულ ტერიტორიაზე. ასეთი ტერიტორია დაცული უნდა იყოს ტერიტორიაზე შეღწევის გამომვლენი აღჭურვილობით ან საიდუმლო ინფორმაციასთან აუცილებელი ინდივიდუალური დაშვების მქონე მცველების მიერ, რომლებიც განახორციელებენ აღნიშნული ტერიტორიის მუდმივ მეთვალყურეობას. შესანახად დაცულ ტერიტორიაზე წვდომა ექნება მხოლოდ საიდუმლო ინფორმაციასთან აუცილებელი ინდივიდუალური დაშვების მქონე უფლებამოსილ პერსონალს.

(3) ტრანზიტის დროს ყოველ ჯერზე, როდესაც საიდუმლო ინფორმაციის შემცველი მასალა, მათ შორის აღჭურვილობა, გადადის ხელიდან ხელში, უნდა მოხდეს მიღების დამადასტურებელი ჩანაწერების მოპოვება, და ამგვარი მასალის მიღების დამადასტურებელ ჩანაწერს ხელი უნდა მოაწეროს საბოლოო მიმღებმა და ის უნდა დაუბრუნდეს გამგზავნს.

c. ელექტრონული მიწოდება: CONFIDENTIAL ან უფრო მაღალი საიდუმლოობის ხარისხით დასაიდუმლოებული საიდუმლო ინფორმაცია, რომელიც ელექტრონულად გადაიცემა, მიწოდებული უნდა იქნას თითოეული მხარის ეროვნული უსაფრთხოების ორგანოს მიერ დამტკიცებული უსაფრთხო საშუალებების გამოყენებით.

მუხლი 14 - ვიზიტები მხარეთა ობიექტებსა და დაწესებულებებში

1. ერთი მხარის წარმომადგენლების ვიზიტები მეორე მხარის ობიექტებსა და დაწესებულებებში, რომლებიც საჭიროებს საიდუმლო ინფორმაციის გაცნობას, ან ვიზიტები, რომლებისთვისაც საჭიროა საიდუმლო ინფორმაციასთან ინდივიდუალური დაშვება საიდუმლო ინფორმაციის გაცნობის უფლების მისანიჭებლად, შეზღუდული უნდა იყოს იმდენად, რამდენადაც ეს აუცილებელია ოფიციალური მიზნებისათვის. ნებართვა უნდა

მიენიჭოს მხოლოდ იმ წარმომადგენლებს, რომლებიც ფლობენ საიდუმლო ინფორმაციასთან ძალაში მყოფ ინდივიდუალურ დაშვებას.

2. ასეთ ობიექტებსა და დაწესებულებებში ვიზიტის ნებართვა უნდა გაიცეს მხოლოდ იმ მხარის მიერ, რომლის ტერიტორიაზეც მდებარეობს ეს ობიექტი ან დაწესებულება, სადაც ვიზიტი უნდა განხორციელდეს. მხარე, სადაც ვიზიტი ხორციელდება, ან მის მიერ განსაზღვრული ოფიციალური პირები პასუხისმგებელნი არიან რჩევის მიწოდებაზე შესაძლო ვიზიტის ობიექტის ან დაწესებულების შესახებ, და საიდუმლო ინფორმაციის ფარგლებისა და უმაღლესი საიდუმლოობის ხარისხის შესახებ, რომელიც შესაძლოა მიეწოდოს ვიზიტორს.

3. ვიზიტის შესახებ მხარეთა წარმომადგენლების მოთხოვნა, შეერთებული შტატების ვიზიტორების შემთხვევაში, წარდგენილ უნდა იქნას თბილისში შეერთებული შტატების საელჩოს მიერ, და ქართველი ვიზიტორების შემთხვევაში - ვაშინგტონში, კოლუმბიის ოლქში, საქართველოს საელჩოს მიერ.

მუხლი 15 - უსაფრთხოების ვიზიტები

წინამდებარე შეთანხმებით განსაზღვრული უსაფრთხოების მოთხოვნების განხორციელება შეიძლება შემოწმდეს ნაცვალგებაზე დაფუძნებული ვიზიტების საშუალებით, მხარეთა უსაფრთხოების პერსონალის მიერ. წინასწარი კონსულტაციის შემდეგ, თითოეული მხარის უსაფრთხოების წარმომადგენლებს უფლება უნდა მიეცეთ, ვიზიტით ეწვიონ მეორე მხარეს, რათა, უსაფრთხოების სისტემებს შორის გონივრული შესაბამისობის მიღწევის მიზნით, განიხილონ და დააკვირდნენ მეორე მხარის საიმპლემენტაციო პროცედურებს. მასპინძელი მხარე უნდა დაეხმაროს ვიზიტით მყოფ უსაფრთხოების წარმომადგენლებს იმის განსაზღვრაში, მეორე მხარისგან მიღებული საიდუმლო ინფორმაცია არის თუ არა სათანადოდ დაცული.

მუხლი 16 - უსაფრთხოების სტანდარტები

მოთხოვნის საფუძველზე, თითოეულმა მხარემ მეორე მხარეს უნდა მიაწოდოს ინფორმაცია საიდუმლო ინფორმაციის დაცვის საკუთარი უსაფრთხოების სტანდარტების, პრაქტიკისა და პროცედურების შესახებ.

მუხლი 17 - საიდუმლო ინფორმაციის რეპროდუქცია

1. საიდუმლო ინფორმაციის რეპროდუქცია, რომელიც მოიცავს თარგმანს ან ასლების გადაღებას, უნდა განხორციელდეს საიდუმლო ინფორმაციის რეპროდუქციის განმახორციელებელი მხარის შესაბამისი შიდასახელმწიფოებრივი კანონმდებლობის მოთხოვნებისა და ამ მუხლის თანახმად.

2. საიდუმლო ინფორმაციის რეპროდუქციისას მასზე არსებული საიდუმლოობის ყველა დედანი გრიფი, ასევე, უნდა დაექვემდებაროს რეპროდუქციას, აღინიშნოს ან მიეთითოს ასეთი ინფორმაციის თითოეულ რეპროდუქციაზე. ასეთი რეპროდუქციები უნდა დაექვემდებაროს იგივე კონტროლს, რაც მოქმედებს თავდაპირველი ინფორმაციის მიმართ. რეპროდუქციების რაოდენობა უნდა შეიზღუდოს ოფიციალური მიზნებისთვის საჭირო მინიმალური რაოდენობით.

მუხლი 18 - საიდუმლო ინფორმაციის განადგურება

1. საიდუმლო ინფორმაციის განადგურება უნდა განხორციელდეს საიდუმლო ინფორმაციის განადგურების განმახორციელებელი მხარის შესაბამისი შიდასახელმწიფოებრივი კანონმდებლობის მოთხოვნებისა და ამ მუხლის თანახმად.

2. საიდუმლო ინფორმაციის შემცველი დოკუმენტები და ინფორმაციის მატარებელი სხვა საშუალებები უნდა განადგურდეს დაწვის, დაჭუცმაცების, რბილ მასად ქცევის ან სხვა მეთოდების გამოყენებით, რაც უზრუნველყოფს მათში მოცემული საიდუმლო ინფორმაციის აღდგენის პრევენციას.

3. საიდუმლო ინფორმაციის შემცველი მასალა, მათ შორის აღჭურვილობა, უნდა განადგურდეს ისეთი საშუალებებით, რაც შეუძლებელს გახდის მის ამოცნობას, რათა გამოირიცხოს საიდუმლო ინფორმაციის სრულად ან ნაწილობრივ აღდგენა.

მუხლი 19 - საიდუმლოობის ხარისხის დადაბლება და განსაიდუმლოება

1. მხარეები თანხმდებიან, რომ საიდუმლო ინფორმაციის საიდუმლოობის ხარისხი უნდა დადაბლდეს მაშინვე მას შემდეგ, რაც ეს ინფორმაცია აღარ მოითხოვს დაცვის უფრო მაღალ ხარისხს, ან განსაიდუმლოებული უნდა იქნას მაშინვე მას შემდეგ, რაც ეს ინფორმაცია აღარ მოითხოვს დაცვას არაუფლებამოსილი გამჟღავნებისგან.

2. მიმწოდებელ მხარეს აქვს საკუთარი საიდუმლო ინფორმაციის საიდუმლოობის ხარისხის დადაბლების ან განსაიდუმლოების სრული დისკრეცია. მიმღებმა მხარემ, მიმწოდებელი მხარის წინასწარი წერილობითი თანხმობის გარეშე, არ უნდა დაადაბლოს მიმწოდებელი მხარისგან მიღებული საიდუმლო ინფორმაციის საიდუმლოობის ხარისხი ან მოახდინოს მისი განსაიდუმლოება, იმ შემთხვევაშიც კი, თუ დოკუმენტზე მითითებულია განსაიდუმლოების ნებისმიერი აშკარა ინსტრუქცია.

მუხლი 20 - დაკარგვა ან გამჟღავნება

მიმღებმა მხარემ დაუყოვნებლივ უნდა შეატყობინოს მიმწოდებელ მხარეს, მიმწოდებელი მხარის საიდუმლო ინფორმაციის ყველა დაკარგვის ან გამჟღავნების გამოვლენის, აგრეთვე, შესაძლო დაკარგვის ან გამჟღავნების შესახებ. ასეთი ინფორმაციის რეალური ან შესაძლო

დაკარგვის ან გამჟღავნების შემთხვევაში, მიმღებმა მხარემ დაუყოვნებლივ უნდა დაიწყოს გამოძიება, რათა დაადგინოს რეალური ან შესაძლო დაკარგვის ან გამჟღავნების გარემოებები. მიმწოდებელ მხარეს უნდა მიეწოდოს გამოძიების შედეგები და ინფორმაცია იმ ზომების შესახებ, რომლებიც მიღებულ იქნა განმეორებით მოხდენის პრევენციის მიზნით.

მუხლი 21 - დავები

მხარეთა შორის უთანხმოება, რომელიც წარმოიშვება წინამდებარე შეთანხმების ფარგლებში ან მასთან დაკავშირებით, უნდა გადაწყდეს მხოლოდ მხარეთა შორის კონსულტაციების გზით და გადასაწყვეტად არ უნდა გადაეცეს ეროვნულ სასამართლოს, საერთაშორისო ტრიბუნალს ან ნებისმიერ სხვა პირს ან ერთეულს.

მუხლი 22 - ხარჯები

თითოეული მხარე პასუხისმგებელია წინამდებარე შეთანხმების შესრულებისას წარმოშობილ საკუთარ ხარჯებზე. წინამდებარე შეთანხმების ფარგლებში მხარეთა ყველა ვალდებულება უნდა დაექვემდებაროს ფინანსური სახსრების ხელმისაწვდომობას.

მუხლი 23 - ცვლილებები

წინამდებარე შეთანხმებაში ცვლილებები შედის მხოლოდ მხარეთა ურთიერთშეთანხმების საფუძველზე. ნებისმიერი ამგვარი ცვლილება გაფორმდება ცალკე დოკუმენტის სახით, რომელიც ძალაში შევა წინამდებარე შეთანხმების 24-ე მუხლის პირველი პუნქტის შესაბამისად.

მუხლი 24 - დასკვნითი დებულებები

1. წინამდებარე შეთანხმება და წინამდებარე შეთანხმების ნებისმიერი ცვლილება ძალაში შედის დიპლომატიური ნოტების გაცვლისას ბოლო შეტყობინების თარიღიდან, რომლითაც მხარეები ადასტურებენ, რომ თითოეულმა მხარემ დაასრულა წინამდებარე შეთანხმების ძალაში შესვლისთვის საჭირო საკუთარი შიდასახელმწიფოებრივი პროცედურები.

2. თითოეულ მხარეს შეუძლია შეწყვიტოს წინამდებარე შეთანხმება, წინამდებარე შეთანხმების შეწყვეტის შესახებ საკუთარი განზრახვის მეორე მხარისთვის, ოთხმოცდაათი დღით ადრე, დიპლომატიური არხებით, წერილობითი შეტყობინების გაგზავნის გზით.

3. წინამდებარე შეთანხმების შეწყვეტის მიუხედავად, უნდა გაგრძელდეს წინამდებარე შეთანხმების შესაბამისად გაცვლილი ან სხვაგვარად მიწოდებული ყველა საიდუმლო ინფორმაციის დაცვა, აქ მოცემული დებულებების შესაბამისად.

რის დასტურადაც, შესაბამისი მთავრობების მიერ სათანადოდ უფლებამოსილმა, ქვემორე ხელმომწერებმა ხელი მოაწერეს წინამდებარე შეთანხმებას.

შესრულებულია ორ დედნად, ქ. ვაშინგტონში, 2017 წ. 9 ივლისს, ინგლისურ და ქართულ ენებზე, ორივე ტექსტი თანაბრად ავთენტურია. განმარტებისას ნებისმიერი განსხვავების შემთხვევაში, უპირატესობა ენიჭება ინგლისურ ტექსტს.

ამერიკის შეერთებული შტატების მთავრობის სახელით:	**საქართველოს მთავრობის სახელით:**

დანართი

საქართველოს მიერ შეერთებული შტატებისთვის მიწოდებული RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაციის დაცვის პროცედურები

1. შეერთებული შტატებისთვის მიწოდებული RESTRICTED საიდუმლოობის ხარისხის მქონე საქართველოს საიდუმლო ინფორმაცია შეერთებულმა შტატებმა, მიღების შემთხვევაში, უნდა დაიცვას ქვემოთ მოცემული მინიმალური პროცედურების შესაბამისად.

2. RESTRICTED საიდუმლოობის ხარისხით განსაზღვრული ინფორმაციის შენახვა უნდა მოხდეს დალუქულ კონტეინერებში ან დახურულ ტერიტორიაზე, რაც უზრუნველყოფს არაუფლებამოსილი პერსონალის მიერ მისი გაცნობის პრევენციას.

3. შეერთებული შტატები მიიღებს დასაიდუმლოების მიღმა ყველა შესაძლო ზომას, რათა დაიცვას საქართველოს მიერ მიწოდებული RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაცია არაუფლებამოსილი პირების ან ერთეულებისათვის მისი გამჟღავნებისგან, საქართველოს წინასწარი წერილობითი ნებართვის გარეშე.

4. RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაციის ელექტრონული შენახვა, დამუშავება ან მიწოდება, საჭიროების მიხედვით, უნდა განხორციელდეს მთავრობის ან კონტრაქტორის მიერ აკრედიტებული სისტემების გამოყენებით. კერძოდ, RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაციის შენახვის, დამუშავების ან გადაცემის მიზნით ნებისმიერი სისტემის გამოყენებამდე, მან უნდა მიიღოს უსაფრთხოების დადასტურება, რომელიც ცნობილია, როგორც „აკრედიტაცია". „აკრედიტაცია" არის შესაბამისი მააკრედიტებელი ორგანოს მიერ გაკეთებული ოფიციალური განაცხადი, რითაც დასტურდება, რომ სისტემის გამოყენება აკმაყოფილებს უსაფრთხოების შესაბამის მოთხოვნებს და არ ქმნის გაუმართლებელ რისკს. „უსაფრთხოების სტანდარტული ოპერაციული პროცედურები" არის ტექნიკური პროცედურები, რითაც, საიდუმლო ინფორმაციის დამმუშავებელი ავტომატიზებული საინფორმაციო სისტემების დაცვის მიზნით, ხორციელდება კონკრეტული ობიექტისთვის დამახასიათებელი უსაფრთხოების პოლიტიკა და მოთხოვნები. იზოლირებული ავტომატიზებული საინფორმაციო სისტემების შემთხვევაში, როგორიცაა შეერთებული შტატების სამთავრობო დაწესებულებებში გამოყენებული სტაციონალური და პორტატული კომპიუტერები, მოთხოვნილი „აკრედიტაციის" ფუნქციას შეასრულებს სისტემის რეგისტრაციის დოკუმენტი, „უსაფრთხოების სტანდარტულ ოპერაციულ პროცედურებთან" ერთად. კონტრაქტორების შემთხვევაში, კონტრაქტში არსებულ „შეზღუდული პირობების მოთხოვნების პუნქტში" უნდა ჩაიდოს საკომუნიკაციო და საინფორმაციო სისტემების გამოყენების სახელმძღვანელო წესი.

5. RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაციის მიწოდება შეერთებული შტატების ფარგლებში უნდა განხორციელდეს პირველი კლასის ფოსტით, ერთი დალუქული ამანათით. შეერთებული შტატების ფარგლებს გარეთ მიწოდება უნდა განხორციელდეს

ორმაგი, დალუქული ამანათით, სადაც შიდა კონვერტზე გაკეთდება აღნიშვნა: „GEORGIA RESTRICTED“. შეერთებულ შტატების ფარგლებს გარეთ მიწოდება უნდა განხორციელდეს კონტროლირებადი საშუალებებით, როგორიცაა კომერციული კურიერი ან მხარეთა მიერ წერილობით შეთანხმებული სხვა საშუალებები.

6. შეერთებული შტატების დოკუმენტებს, რომელიც შეიცავს RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაციას, შეფუთვასა და პირველ გვერდზე უნდა მიეთითოს აღნიშვნა: „GEORGIA RESTRICTED“. დოკუმენტების ნაწილზე, რომელიც შეიცავს RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაციას, ასევე, უნდა მიეთითოს აღნიშვნა: „GEORGIA RESTRICTED“.

7. RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაციის მიწოდება ან მისი გაცნობა შესაძლებელია განხორციელდეს ელექტრონულად, ისეთი ქსელის მეშვეობით, როგორიცაა ინტერნეტი, მხარეთა მიერ ორმხრივად აღიარებული სამთავრობო ან კომერციული დაშიფვრის მოწყობილობების გამოყენებით. თუ დაშიფვრის სისტემა ხელმისაწვდომი არ არის და არსებობს მიმწოდებელი მხარის ეროვნული უსაფრთხოების ორგანოს დასტური, შესაძლებელია განხორციელდეს RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაციის შემცველი სატელეფონო საუბარი, ვიდეო კონფერენცია ან ფაქსის მეშვეობით მიწოდება.

8. კონტრაქტორს არ მოეთხოვება საიდუმლო ინფორმაციასთან იურიდიული პირის დაშვება ისეთი კონტრაქტების დასადებად, რომლებიც საჭიროებს მხოლოდ RESTRICTED საიდუმლოობის ხარისხის მქონე საიდუმლო ინფორმაციის მიღებას ან შექმნას.

9. RESTRICTED საიდუმლოობის ხარისხის მქონე ასეთი ინფორმაციის გაცნობის უფლება შეიძლება მიენიჭოს მხოლოდ იმ ფიზიკურ პირებს, რომლებსაც აქვთ ინფორმაციის გაცნობის საჭიროება. RESTRICTED საიდუმლოობის ხარისხის მქონე ინფორმაციის გაცნობა არ საჭიროებს საიდუმლო ინფორმაციასთან ინდივიდუალურ დაშვებას.