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

PREAMBLE

The Government of the Republic of Estonia ("Estonia") and the Government of the United States of America (the "United States") (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 these terms mean the following:

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): An assurance provided by the National Security Authority of a Party, as designated in Article 4, that a Contractor´s facility under the Party's jurisdiction is cleared in accordance with its national laws and regulations to a specified level and also has suitable security safeguards in place at a specified level to safeguard Classified

Information. Such a determination shall signify that Classified Information at the KONFIDENTSIAALNE / 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.

5. 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.

6. Personnel Security Clearance (PSC):

a. An assurance provided 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 in accordance with its national laws and regulations to access Classified Information up to a specified level.

b. An assurance provided 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 in accordance with its national laws and regulations to access Classified Information up to a specified level.

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 released by one Party to the other Party shall be protected by the recipient Party in a manner that is at least equivalent to the protection afforded to Classified Information of equivalent classification level of the recipient 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 national 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 Estonia: National Security Authority, Estonian Foreign Intelligence Service.

b. for the United States: Assistant Director, International Engagement Directorate, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy, U.S. Department of Defense.

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:

ESTONIA	**UNITED STATES**
TÄIESTI SALAJANE	TOP SECRET
SALAJANE	SECRET
KONFIDENTSIAALNE	CONFIDENTIAL
PIIRATUD (RESTRICTED)	No equivalent (see paragraph 2)

2. During the implementation of this Agreement, if Estonia provides Classified Information designated as PIIRATUD (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. Classified Information released by one Party to the other Party shall be protected
by the recipient Party in a manner that is at least equivalent to the protection afforded to Classified Information of equivalent classification level of the recipient 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, who have been briefed in accordance with their national laws and regulations on their responsibilities and obligations to protect Classified Information, and who are 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 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 KONFIDENTSIAALNE / 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 from the National Security Authority of the other Party that an FSC corresponding to the required security classification level has been issued. 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 releasing Party 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 KONFIDENTSIAALNE / 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 Estonia in Washington, D.C., in the case of Estonian visitors and by the Embassy of the United States in Tallinn in the case of U.S. 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

When Classified Information is reproduced (including translation), 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 in whole or in part 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 the last signature by the Parties.

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

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

4. The Agreement between the Government of the Republic of Estonia and the Government of the United States Concerning Security Measures for the Protection of Classified Military Information (the "Security Agreement"), signed February 23, 2000, shall terminate on the date that this Agreement enters into force.

5. Any reference in any other existing agreement or arrangement between the Parties to the Security Agreement shall be considered to be a reference to this Agreement.

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

Done, in duplicate, at Washington D.C this 20-th day of November 2023, in the English language.

FOR THE GOVERNMENT OF THE REPUBLIC OF ESTONIA	**FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA**
Kristjan Prikk	**Micheal R. Laychak**

APPENDIX

PROCEDURES FOR PROTECTING ESTONIAN PIIRATUD (RESTRICTED) CLASSIFIED INFORMATION PROVIDED TO THE UNITED STATES

1. Upon receipt, Estonian Classified Information provided to the United States and designated as PIIRATUD (RESTRICTED) shall be protected by the United States in accordance with the following procedures.

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

3. PIIRATUD (RESTRICTED) information shall not be disclosed to unauthorized persons or entities without the prior written approval of the Estonian National Security Authority except as required by U.S. law, including the Freedom of Information Act.

4. PIIRATUD (RESTRICTED) information shall, as applicable, be stored, processed, or transmitted electronically by using government- or Contractor-accredited systems. In particular, before any system is used to store, process, or transmit PIIRATUD (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 used 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. PIIRATUD (RESTRICTED) information (documents or other media) shall be transmitted by Priority Mail. Transmission within and outside the United States will be in double, sealed envelopes with the inner envelope marked “Estonian PIIRATUD (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 Estonian PIIRATUD (RESTRICTED) information shall bear on the cover and the first page the marking “Estonian PIIRATUD (RESTRICTED)”. The portion of the documents containing Estonian PIIRATUD (RESTRICTED) information also shall be identified with the same marking.

7. PIIRATUD (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 PIIRATUD (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 and PSC are not required for a Contractor to undertake contracts that require only the receipt or production of Classified Information at the PIIRATUD (RESTRICTED) level.

   Access to PIIRATUD (RESTRICTED) information shall be granted only to those individuals who have a Need-to-Know and who have been appropriately briefed on their responsibilities and obligations to protect Classified Information. A United States' PSC is not required to access PIIRATUD (RESTRICTED) Classified Information