MEMORANDUM OF COOPERATION
BETWEEN
THE DEPARTMENT OF HOMELAND SECURITY
OF THE UNITED STATES OF AMERICA
AND
THE MINISTRY OF THE INTERIOR
OF THE ORIENTAL REPUBLIC OF URUGUAY
ON ENHANCING BORDER SECURITY COOPERATION
THROUGH THE EXCHANGE OF INFORMATION

The Department of Homeland Security of the United States of America (the "U.S. Participant" or "DHS") and the Ministry of the Interior of the Oriental Republic of Uruguay (the "Uruguayan Participant" or "MOI"), herein collectively referred to as the "Participants",

Desiring to cooperate as partners to protect the safety and security of their States' territories by denying entry to such territories to persons who are not eligible for entry, including on terrorism, criminal, or security grounds;

Recognizing a need to have a technical arrangement for the exchange of biometric and associated data to verify the identity of travelers, migrants, or applicants for immigration benefits; to establish their citizenship and immigration status; and to determine whether they are suspected, investigated, accused or convicted of terrorism offenses, offenses linked to illegal immigration, or crimes rendering the individual inadmissible or removable, consistent with their respective national laws and policies;

Recognizing that the exchange of information occurs in a manner that complies with the Participants' respective human rights obligations and commitments, including those relating to privacy and civil liberties. Recognizing that the appropriate handling and Processing of Data that they acquire from each other is of critical importance to preserving confidence in the implementation of this Memorandum;

Recognizing existing efforts to provide mutual support in preventing potential threats to national security and detecting terrorist and criminal activities including the Memorandum of Cooperation and Understanding between the Department of Homeland Security of the United States of America and the Ministry of the Interior of the Oriental Republic of Uruguay Regarding Collaboration on the Use of Traveler Information, signed at Washington and Montevideo on September 21, 2020,

and

Having regard for United Nations Security Council Resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2322 (2016), and, in particular, 2396 (2017), which decided that Member States

are to develop and implement systems to collect biometric data to identify terrorists and to prevent the movement of terrorists or terrorist groups by effective national border controls and through measures for preventing fraudulent use of identity papers and travel documents, and also encourages Member States to share such information responsibly, as appropriate,

Have stated as follows:

Section 1

Purpose and scope

1. ***Scope.*** This Memorandum of Cooperation (herein referred to as "Memorandum") describes the general relationships, responsibilities, and understandings for the automated and manual sharing and use of appropriate Personal Data, in furtherance of the purposes identified in Section 1, paragraph 2 of this Memorandum.

2. ***Purposes for the Exchange and Handling of Data Between Participants.*** The Participants intend that this Memorandum support the administration and enforcement of the Participants' respective immigration and border security laws through the exchange and handling of appropriate Personal Data in the interest of national security, public safety, and public security, and describe the policies and processes through which such exchanges are intended to occur. Consistent with the Participants' respective domestic laws and policies, the Participants intend to exchange information to:

    a. Facilitate the screening and vetting, including establishing and verifying identity, of individuals seeking admission, entry, transit or departure at the Participants' respective national borders, or applying for visas, travel authorizations, or immigration benefits, including applications for trusted traveler programs, work-related credentials, or to seek asylum and refugee protection, or other forms of international protection;

    b. Facilitate the determination of whether there are grounds of inadmissibility or removability of an individual under the laws of the United States or Uruguay; or

    c. Further the prevention, detection, investigation, and prosecution of acts that would constitute serious crime, including terrorism, and other acts that would constitute a crime rendering an individual inadmissible or removable under the relevant laws of either Participant, or international law, as applicable.

Section 2

Definitions

For the purposes of this Memorandum, the following definitions apply:

1. ***"Applicable Database"*** means:

    a. With respect to DHS: IDENT, or its successor, including other U.S. datasets available to IDENT or its successor, and any data from which the U.S. Participant is authorized by applicable national law and policy to disclose to Uruguay.

    b. With respect to MOI: RAMM and AFIS, or their successors, including other Uruguayan datasets available to RAMM, AFIS, or their successors, whose data in

such database which the Uruguayan Participant is authorized to disclose under applicable national law and policy to disclose to the United States.

2. ***"Personal Data"*** means any information through which a natural person may be identified, directly or indirectly, and includes biometric information (such as fingerprints, face images, and iris images); associated reference numbers; surnames, first names, former names, other names, aliases, and alternative spelling of names; gender; date and place of birth; current and former nationalities; passport data; data from other identity documents; and criminal, police, and alien records.

3. ***"Processing of Data" or "Process Data"*** means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, combination or alignment, blocking or deleting through erasure or destruction of Personal Data;

4. ***"Query" or "Queries"*** means an automated electronic search or searches by the Querying Participant of the Searched Participant's Applicable Database or Databases conducted under this Memorandum.

5. ***"Querying Participant"*** means the Participant that initiates the Query.

6. ***"Searched Participant"*** means the Participant that receives the Query from the Querying Participant.

7. ***"Serious Crime"*** means for purposes of implementing this MOU, conduct constituting an offense publishable under the domestic laws of their respective countries by a maximum deprivation of liberty of more than one year, or a more serious penalty

Section 3

Automated querying of biometric data

1. ***Information Exchange through Querying.*** For the purposes set forth in Section 1, paragraph 2 of this Memorandum, the Participants intend to allow for the automated submission of biometric Queries to each other's Applicable Databases to facilitate the lawful and appropriate exchange of other Personal Data and additional information.

2. ***Authority Required to Query.*** The Querying Participant is expected to conduct Queries only when it has authority to do so under its national law and for purposes described in Section 1, paragraph 2 of this Arrangement.

3. ***Query Information.*** When submitting Queries under this Section, the Querying Participant intends to send to the Searched Participant the following information:

   a. Biometric information consistent with Paragraph 6 of this Section;

   b. A unique reference number that identifies the individual and/or the Query; and when available and authorized by national law and policy:

      i. An indicator of the nature of the Querying Participant's encounter with the individual, including the reason for the Query and information collected or

generated during the encounter that motivated the Query;

ii. Query metadata, such as date and time stamp, and transaction number; and

iii. Additional Personal Data and additional information as may mutually be determined in writing by the Participants.

4. ***Responding to Queries.*** Upon receipt of the Query, the Searched Participant intends to, on an automated basis and consistent with its applicable national law, regulations, and policy:

   a. Compare the biometric information transmitted by the Querying Participant against the Searched Participant's Applicable Database;

   b. Notify the Querying Participant through an automated response whether the biometric information provided in the Query matches a record in the Searched Participant's Applicable Database (a positive match confirmation), consistent with applicable national laws and policies;

   c. Upon confirmation of a positive match, supply to the Querying Participant relevant Personal Data available through its Applicable Database, as appropriate and to the extent authorized by and consistent with applicable national law and policy;

   d. After supplying Personal Data to the Querying Participant, request through the automated querying system Personal Data associated with the matched biometric from the Querying Participant;

   e. If no match is found, give an automated notification to this effect to the Querying Participant; and

   f. Delete the biometric included in the Querying Participant's Query after it has determined it does not have a matching record or after it has determined it has a matching record available through its Applicable Database and shared the appropriate, associated Personal Data from its systems.

5. ***Reciprocal Exchange in Event of a Match.*** Should the procedure referred to in Section 3.4 of this Memorandum show a match to the biometric held by the Searched Participant, the Querying Participant intends to supply the Searched Participant with appropriate Personal Data about the individual that it has collected, or that was generated during the encounter that motivated its original Query, and that was not included in the original Query. The Personal Data supplied under this Paragraph may also include other biometric data when available.

6. ***Preferred Biometric Modality.*** The Participants intend to initially use fingerprints as the primary biometric modality for submitting Queries under this Memorandum. The Participants may submit Queries using other forms of biometric information where mutually decided in writing by the Participants and authorized through their respective domestic processes.

7. ***Comparison of Non-Biometric Personal Data.*** Where applicable and mutually decided in writing by the Participants, Queries, comparisons, and further analysis may also be made using forms of Personal Data other than the biometric information, for the purposes set

forth in Section 1, paragraph 2 of this Memorandum.

8. ***Availability of Personal Data.*** For purposes of Queries and responses to Queries under this Section, the Participants intend to make available appropriate Personal Data available through their Applicable Databases, to the extent authorized by their respective national laws and policies.

9. ***Personal Data, Litigation Proceedings.*** When a Participant requires the assistance of the disclosing Participant in order to introduce information exchanged under this Memorandum in judicial or administrative proceedings, the Participant may, in accordance with applicable mutual legal assistance instruments or rules, request the disclosing Participant to provide a copy of the biometric maintained in the disclosing Participant's Applicable Databases used to establish a positive match as well as any further Personal Data maintained with the biometric information.

10. ***Automated Exchange Intended.*** The Participants intend to conduct the exchange of Personal Data under this Section on an automated basis to the extent possible.

Section 4

Procedures for the manual exchange of

Personal Data

1. ***Non-Automated Exchange Available.*** Should the procedure for responding to Queries described in Section 3, paragraph 4 of this Memorandum show a match to the biometric information held by the Searched Participant, the Participants intend to exchange, as appropriate, Personal Data. This includes Personal Data that is not available through the Applicable Database, cannot be transmitted automatically, is not immediately available for automated exchange, or has not been approved for automated exchange through existing communication channels or through other means of communication, including the connection established to implement this Memorandum. The Participants intend that any such exchange be conducted under this Memorandum, applicable national law and policy, and any additional specific terms mutually decided upon by both Participants in writing. The Participants intend to inform each other's contact points of such specific terms.

2. ***Exchange through Contact Points.*** The Participants intend to implement the exchange of Personal Data under this Section through their respective contact points designated in Section 6.1 of this Memorandum.

Section 5

Supply of Personal Data in order to protect public safety and security

1. ***Unrequested Sharing of Personal Data.*** Where necessary for the protection of public safety and security, a Participant may, in individual cases and in accordance with its national laws and policies, supply the other Participant with Personal Data through established channels, even without being requested to do so.

2. ***Imposition of Conditions.*** In addition to the understandings in this Memorandum, the Participants intend, as appropriate and in accordance with their respective national laws

and international obligations, to impose conditions in writing on the use that may be made of the Personal Data exchanged under this Section. The Participants do not intend that such conditions include generic data protection conditions, that is, conditions imposed that are unrelated to the specific facts of the case. If the other Participant accepts Personal Data where such additional conditions have been imposed, that Participant is expected to abide by all those conditions and to notify the providing Participant if it cannot comply with such conditions.

3. ***Separate Agreement or Arrangement for Recurring Sharing.*** Any exchange of Personal Data under this Section done on a recurring basis or not otherwise tied to an individual case is expected to be set forth in a separate agreement or arrangement that details the specific purposes for which such biometric information and other Personal Data is supplied, processed, handled, and safeguarded.

Section 6

Contact point responsibilities

1. ***U.S. Contact Point:*** DHS is responsible for maintaining the Personal Data available through the Applicable Database and ensuring appropriate Processing of Personal Data.

2. ***Uruguayan Contact Point:*** The MOI is responsible for maintaining the availability of Personal Data through the Applicable Database and ensuring appropriate Processing of Personal Data.

3. ***Updates to Contact Points.*** The Participants intend to update each other in writing of changes in their contact point responsibilities in paragraph 1 of this Section.

4. ***Technical and Procedural Details.*** The Participants may decide the technical and procedural details for the implementation of this Memorandum and, when necessary, establish one or more implementing arrangements.

Section 7

Privacy and Personal Data protection

1. ***Data Handling.*** The Participants intend to handle and Process Data consistent with this Memorandum and their respective laws and policies, and further intend to:

   a. Supply only Personal Data that are necessary and relevant in relation to the specific purpose of the exchange;

   b. Take reasonable steps to ensure accuracy completeness, and reliability of the Personal Data processed, including notifying contact points in a timely manner of possibly significant errors, inaccuracies, or other indicia of unreliability, as further explained in Section 8 of this Memorandum; and

   c. Retain all Personal Data exchanged after a match has been established under this Memorandum only so long as necessary for the purpose for which the Personal Data were exchanged or further processed, to assist in the effective administration and enforcement of the Participants' respective laws, including where necessary to prevent, detect, investigate, or prosecute immigration or criminal offenses. In any case, the

Participants do not intend to retain Personal Data beyond the time limits and rules established by the Participants' respective applicable national laws and policies.

2. ***Appropriate Safeguards.*** The Participants intend to implement appropriate safeguards and security measures to protect all Personal Data exchanged under this Memorandum.

3. ***No Rights Conferred.*** Nothing in this Memorandum is intended to give rise to rights on the part of any individual, including to obtain, suppress, or exclude any evidence, or to impede the sharing of Personal Data.

4. ***Existing Rights Unaffected.*** Nothing in this Memorandum is intended to interfere with any individual's rights to information nor to appeal to an administrative or judicial body of the Participants in accordance with the Participants' respective national laws, if that individual believes that Personal Data pertaining to them are being processed incorrectly.

5. ***Notification of Retention Periods.*** The Participants intend to inform each other's contact points of their respective retention periods and any changes to retention practices relevant to this Section.

6. ***Use by Other Government Agencies and Political Subdivisions.*** A Participant may permit other agencies and political subdivisions of its government to use Personal Data received from the other Participant for purposes consistent with Section 1 provided their processing of Personal Data respects the provisions of this MOU.

7. ***Third Party Sharing.*** The Participants do not intend to disseminate or otherwise make available any Personal Data supplied under this Memorandum to any third State, international body, or private person or entity. In those exceptional cases where it is critical for such information to be disclosed for public safety and security reasons or to comply with domestic law, the disclosing Participant intends to notify the Participant that provided the information as soon as practicable.

Section 8

Correction, blockage and deletion of Personal Data

1. ***Notification of Significant Inaccuracies.*** The Participants intend to notify each other of possibly significant inaccurate Personal Data as soon as practicable, preferably within 48 hours of determining that inaccurate information was transferred, so that appropriate corrective action can be taken. The Participants intend to make such notifications only in cases of possibly significant errors, inaccuracies, or other indicia of unreliability.

2. ***Resolving Inaccuracies***. The Participant that received inaccurate or incomplete Personal Data intends to annotate, correct, block, or delete such Personal Data, as appropriate and consistent with its national laws. If requested to take such action by the Participant that sent the data, the Participant that received the data is expected to take corrective action, as appropriate and consistent with its national law.

3. ***Blocking Unauthorized Data.*** The Participants further intend to correct, block, or delete Personal Data if the exchange or further Processing of Data is inconsistent with this Memorandum or their national laws. The Participants intend to notify each other in the

event of such correction, blocking, or deletion of Personal Data.

4. ***Preventing Reliance on Inaccurate Data.*** When a Participant becomes aware of significant doubts as to the accuracy or reliability of the Personal Data exchanged under this Memorandum, as described in paragraph 1 of this Section, the Participants intend to take all appropriate measures to safeguard against erroneous reliance on such Personal Data.

Section 9

Personal Data security

1. ***Security Measures.*** The Participants intend to utilize technical measures and internal organizational arrangements to protect Personal Data against accidental or unlawful loss or destruction, and accidental or unauthorized disclosure, alteration, access, or use, or any unauthorized form of processing. The Participants, in particular, intend to take reasonable measures to allow only those authorized to access the Personal Data to have access to such Personal Data.

2. ***Security Best Practices.*** The procedures for the automated and manual handling of Personal Data under Sections 3, 4, and 5 of this Memorandum are expected to include:

   a. the appropriate use of technology that is designed to support data protection, security, confidentiality, and integrity;

   b. the use of encryption, authorization, and other data security best practices and procedures for accessing or using the information sharing procedures outlined in this Memorandum or data supplied under it; and

   c. the employment of an appropriate mechanism to prevent unauthorized Queries.

3. ***Data Breach Notifications.*** As appropriate and consistent with their national laws, the Participants intend to promptly notify each other's contact points no later than forty-eight (48) hours after becoming aware of any incident involving accidental loss or destruction, or unauthorized access, disclosure, or alteration of Personal Data exchanged under this Memorandum, and they intend to furnish all necessary and appropriate details regarding the incident.

Section 10

Record keeping

1. ***Purpose of Record Keeping.*** The Participants are expected to maintain a record of the transmission and receipt of Personal Data exchanged with the other Participant under this Memorandum, as well as a record of the transmission of Personal Data to any other agency or department belonging to a Participant's government, under this Memorandum. The Participants intend to maintain such records to:

   a. facilitate the exchange of Personal Data outlined in this Memorandum;

   b. facilitate effective monitoring of data protection in accordance with the respective national laws, regulations, and policies of the Participants;

c. enable the Participants to effectively implement Sections 7, 8, and 9 of this Memorandum; and

d. facilitate cybersecurity.

2. ***Record Keeping Contents.*** The Participants intend for the record of the exchange and receipt of Personal Data to include:

   a. description of the type of data exchanged;

   b. the date of exchange;

   c. the recipient of the Personal Data in case the Personal Data are exchanged with other governmental entities; and

   d. any applicable Query metadata, including the unique reference number referred to in Section 3, paragraph 3(b) of this Memorandum.

3. ***Retention of Record.*** To the extent consistent with applicable national laws, the Participants intend to maintain data recorded under this Section for a period of two (2) years. After this retention period, the Participants intend to immediately delete such recorded data, unless doing so is inconsistent with their national laws and policies, including applicable data protection and retention rules.

Section 11

Transparency

Notwithstanding Sections 7, 8, and 9 of this Memorandum, the Participants do not intend for anything in this Memorandum to be interpreted to interfere with the Participants' obligations under their respective national laws or other applicable arrangements or agreements pertaining to data protection and privacy, which may include obligations to provide individuals with rights and privileges regarding Personal Data.

Section 12

Review

The Participants intend to review the implementation of this Memorandum periodically, including within the first year of operation. As part of such review, the Participants intend to examine the following subjects:

1. ***Effectiveness Review.*** The Participants intend to evaluate the effectiveness of the exchange conducted under this Memorandum in protecting security and public safety as well as the effectiveness of the privacy safeguards applicable to protect the Personal Data exchanged;

2. ***Query Review.*** The Participants intend to review the number and nature of Queries, the number and percentage of matches, and the timeliness of responses;

3. ***Case Study Review.*** The Participants intend to share, to the extent practicable, additional statistics and case studies demonstrating how the exchange of Personal Data under this Memorandum has assisted in identifying criminals, including known or suspected terrorists or other threats to security and public safety, and actions taken as a

result of that identification, including denial of entry or immigration benefits, removals, or prosecutions; and

4. ***Privacy Review.*** As appropriate and consistent with their respective national laws, the Participants intend to discuss any possibly significant inaccuracies notified under Section 8, paragraph 1 of this Memorandum, and any data breaches notified under Section 10, paragraph 3 of this Memorandum, including accidental or unauthorized access or disclosure of Personal Data, that occur during the implementation of this Memorandum and any corrective actions taken in response to any such incidents.

Section 13

Expenses

Each Participant is expected to be responsible for its own costs incurred in the implementation of this Memorandum which will be subject to the availability of appropriated funds and other resources at the time of implementation.

Section 14

Consultations and modifications

1. ***Modifications.*** The Participants intend that this Memorandum may be modified with their mutual written approval.
2. ***Interpretation.*** The Participants intend to consult each other if there is a discrepancy in the interpretation or implementation of this Memorandum. In the event of a discrepancy between the English and Spanish versions of this Memorandum, the Participants intend to clarify such discrepancies in a collaborative manner, but in the event of an irreconcilable discrepancy, the Participants intend that the English version will control.
3. ***Discrepancies.*** In the event of a discrepancy under this Memorandum, the Participants do not intend to refer any matters under this Memorandum to any third parties for resolution.

Section 15

General provisions

1. ***Relation to Other Instruments.*** The Participants do not intend for the provisions of this Memorandum to be construed to limit or prejudice the provisions of any treaty, agreement, arrangement, law enforcement relationship, or other mechanisms allowing for information sharing between the Participants, between their respective governments, or between other agencies within their respective governments.
2. ***Inability to Share.*** Either Participant may refuse to supply data and information to the other Participant, including if the request is not consistent with this Memorandum, if the response would prejudice its sovereignty, national security, important public policy, public order, or other essential public interest, be contrary to applicable national law, regulation, or policy or is inconsistent with any of its international obligations or commitments.
3. ***Compliance with Law.*** In carrying out the activities described in this Memorandum, the Participants intend to abide by their respective national laws, policies, and international

obligations, including under international human rights law, international refugee law, and international humanitarian law.

4. ***Notification of Changes to Law.*** The Participants intend to inform each other of any changes to their national laws and policies that may materially affect their cooperation under this Memorandum.

5. ***Commencement.*** Participation under this Memorandum commences upon signing and is to continue indefinitely unless discontinued.

6. ***Discontinuation.*** Either Participant may discontinue cooperation under this Memorandum at any time, but is expected to endeavor to provide at least six (6) months' written notice to the other Participant.

7. ***Data Privacy after Discontinuation***. In the event of discontinuation of this Memorandum, the Participants are expected to continue to protect all Personal Data exchanged under this Memorandum consistent with Sections 7 through 11 of this Memorandum.

8. ***No Obligations or Rights Created.*** Nothing in this Memorandum is intended to give rise to rights or obligations under international law.

Signed in Montevideo, Uruguay, the 3rd of January of 2024, in two originals in the English and Spanish languages.

FOR THE DEPARTMENT OF HOMELAND SECURITY OF THE UNITED STATES OF AMERICA:

United States Ambassador to the
Oriental Republic of Uruguay
Heide B. Fulton

FOR THE MINISTRY OF THE INTERIOR OF THE ORIENTAL REPUBLIC OF URUGUAY:

Minister of Interior of the
Oriental Republic of Uruguay
Nicolas Martinelli