

Memorandum of Understanding
between the
Government of the United States of America
and
the Government of Australia
On Enhancing Cooperation in
Preventing and Combating Crime

**Memorandum of Understanding between
the Government of the United States of America
and
the Government of Australia
On Enhancing Cooperation in
Preventing and Combating Crime**

The Government of the United States of America and the Government of Australia (herein "Participants"),

Prompted by the desire to cooperate as partners to prevent and combat crime, particularly terrorism, more effectively,

Recognizing that information sharing is an essential component in the fight against terrorism, while respecting fundamental rights and freedoms, notably privacy, and

Seeking to enhance and encourage cooperation between the Participants in the spirit of partnership,

Have reached the following understandings:

1. Definitions

For the purposes of this Memorandum,

1. DNA profiles (DNA identification patterns) means a letter or numerical code representing a number of identifying features of the non-coding part of an analyzed human DNA sample, i.e. of the specific chemical form at the various DNA loci.
2. Personal data means any information relating to an identified or identifiable natural person (the "data subject").
3. Processing of personal 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 supply, dissemination or otherwise making available, combination or alignment, blocking, or deleting through erasure or destruction of personal data.
4. Reference data means a DNA profile and the related reference (DNA reference data) or fingerprint data and the related reference (fingerprint reference data). Reference data should not contain any data from which the data subject can be directly identified. Reference data not traceable to any individual (untraceables) should be recognizable as such.

2. Purpose and Scope of this Memorandum

1. The purpose of this Memorandum is to enhance the cooperation between the United States and Australia in preventing and combating crime.
2. The querying powers provided for under this Memorandum are to be used only for prevention, detection and investigation of crime.
3. The scope of this Memorandum is to encompass crimes constituting an offense punishable under the laws of both Participants by a maximum deprivation of liberty of more than one year or a more serious penalty.
4. This Memorandum does not replace or limit the use of other legal assistance channels as required by the supplying Participant's laws.

3. Fingerprint data

For the purpose of implementing this Memorandum, the Participants are to ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offenses. Reference data are only to include fingerprint data and a reference.

4. Automated querying of fingerprint data

1. For the prevention and investigation of crime, and if permissible under the laws of both Participants, each Participant is to allow the other Participant's national contact points, as referred to in Paragraph 7, access to the reference data in the automated fingerprint identification system, which it has established for that purpose, with the power to conduct automated queries by comparing fingerprint data. Queries may be conducted only in individual cases and in compliance with the querying Participant's laws.
2. Comparison of fingerprint data with reference data held by the Participant in charge of the file is to be carried out by the querying national contact points by means of the automated supply of the reference data required for a clear match.
3. When needed, further analysis for the purpose of confirming a match of the fingerprint data with reference data held by the Participant in charge of the file is to be carried out by the requested national contact points.

5. Alternative means to query using identifying data

Until Australia has a fully operational and automated fingerprint identification system that links to individual criminal records and is prepared to provide the United States with automated access to such a system, it is to provide an alternative means to conduct a query using other identifying data to determine a clear match linking the individual to additional data. Query powers are to be exercised in the same manner as provided in Paragraph 4 and a clear match is to be treated the same as a firm match of fingerprint data to allow for the supply of additional data as provided for in Paragraph 6.

6. Supply of further personal and other data

Should the procedure referred to in Paragraph 4 show a match between fingerprint data, or should the procedure utilized pursuant to Paragraph 5 show a match, the supply of any available further personal data and other data relating to the reference data is to be governed by the laws, including those in relation to legal assistance, of the requested Participant, as well as the policies and guidelines based on essential interests of the requested Participant as understood in the context of the Treaty on Mutual Assistance in Criminal Matters between the United States and Australia. Further information provided under this paragraph is to be supplied in accordance with the procedures set forth in Paragraph 7.

7. National contact points and implementing arrangements

1. For the purpose of the supply of data as referred to in Paragraphs 4 and 5, and the subsequent supply of further personal data as referred to in Paragraph 6, each Participant is to designate one or more national contact points. The contact point is to supply such data in accordance with the laws of the Participant designating the contact point.
2. The technical and procedural details for the queries conducted pursuant to Paragraphs 4 and 5 are to be set forth in one or more implementing arrangements.

8. Automated querying of DNA profiles

1. If permissible under the laws of both Participants and on the basis of reciprocity, the Participants may allow each other's national contact point, as referred to in Paragraph 11, access to the reference data in their DNA analysis files, with the power to conduct automated queries by comparing DNA profiles for the investigation of crime. Queries may be made only in individual cases and in compliance with the querying Participant's laws.
2. Should an automated query show that a DNA profile supplied matches a DNA profile entered in the other Participant's file, the querying national contact point is to receive by automated notification the reference data for which a match has been found. If no match can be found, automated notification of this is to be given.

9. Alternative means to query DNA databases

Until such time that the laws and technical arrangements of both Participants permit the type of DNA queries contemplated by Paragraph 8, a Participant is to conduct a search of its own DNA databases, in accordance with its laws, at the request of the other Participant.

10. Supply of further personal and other data

Should the procedure referred to in Paragraph 8 show a match between DNA profiles, the supply of any available further personal and other data relating to the reference data is to be governed by the laws, including those in relation to legal assistance, of the requested Participant, as well as the policies and guidelines based on essential interests of the requested Participant as understood in the context of the Treaty on Mutual Assistance in Criminal Matters between the United States and Australia. Further information provided under this paragraph is to be supplied in accordance with Paragraph 11.

11. National contact point and implementing arrangements

1. For the purposes of the supply of data as set forth in Paragraph 8, each Participant is to designate a national contact point. The contact point is to supply such data in accordance with the laws of the Participant designating the contact point.
2. The technical and procedural details for the queries conducted under Paragraph 8 are to be set forth in one or more implementing arrangements.

12. Supply of personal and other data in order to prevent serious criminal and terrorist offences

1. For the prevention of serious criminal and terrorist offenses, the Participants may, in compliance with their respective laws, in individual cases, even without being requested to do so, supply the other Participant's relevant national contact point, as referred to in paragraph 7, with the personal data specified in subparagraph 12.2, in so far as is necessary because particular circumstances indicate that the data subject(s):
 - (a) will commit or has committed terrorist or terrorism related offenses, or offenses related to a terrorist group or association, as those offenses are defined under the supplying Participant's laws; or
 - (b) is undergoing or has undergone training to commit the offenses referred to in subparagraph 12.1(a); or
 - (c) will commit or has committed a serious criminal offense, or participates in an organized criminal group or association.
2. The personal data to be supplied are to include, if available, surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, current and former nationalities, passport number, numbers from other identity documents, and fingerprint data, as well as a description of any conviction or of the circumstances giving rise to the belief referred to in paragraph 1.
3. A Participant may impose conditions on the other Participant before supplying data pursuant to this article. The participants intend to abide by any conditions that they accept in order to receive data.
4. Generic restrictions with respect to the legal standards of the receiving Participant for processing personal data should not be imposed by the transmitting Participant as a condition under subparagraph 12.3 to providing data.
5. In addition to the personal data referred to in subparagraph 12.2, the Participants may provide each other with non-personal data related to the offenses set forth in subparagraph 12.1.
6. Each Participant is to designate one or more national contact points for the exchange of personal and other data under this Paragraph with the other Participant's contact points. The powers of the national contact points are to be governed by the laws applicable.

13. Privacy and Data Protection

1. The Participants recognize that the handling and processing of personal data that they acquire from each other is of critical importance to preserving confidence in the implementation of this Memorandum.
2. The Participants dedicate themselves to processing personal data fairly and in accord with their respective laws and:
 - (a) ensuring that the personal data provided are adequate and relevant in relation to the specific purpose of the transfer;
 - (b) retaining personal data only so long as necessary for the specific purpose for which the data were provided or further processed in accordance with this Memorandum; and
 - (c) ensuring that possibly inaccurate personal data are timely brought to the attention of the receiving Participant in order that appropriate corrective action is taken.
3. Nothing in this Memorandum is intended to give rise to rights on the part of any private person, including to obtain, suppress, or exclude any evidence, or to impede the sharing of personal data. Rights existing independently of this Memorandum, however, are not to be affected.
4. Responsibility and powers for enforcing legal requirements that apply to the supply, receipt, processing, and recording of personal data lie with relevant data protection authorities or, where applicable, privacy officers and judicial authorities of the respective Participants as determined by their laws.

14. Additional Protection for Transmission of Special Categories of Personal Data

1. Personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, trade union membership or concerning health and sexual life should only be provided if they are particularly relevant to the purposes of this Memorandum.
2. The Participants, recognizing the special sensitivity of the above categories of personal data, are to take suitable safeguards, in particular appropriate security measures, in order to protect such data.

15. Limitation on processing to protect personal and other data

1. Without prejudice to subparagraph 2.3, and in accordance with subparagraph 2.2, each Participant may process data obtained under this Memorandum:
 - (a) for the purpose of its criminal investigations;
 - (b) for preventing a serious threat to its public security;
 - (c) in its non-criminal judicial or administrative proceedings directly related to investigations set forth in subparagraph 15.1(a); or
 - (d) for any other purpose, only with the prior consent of the Participant which has transmitted the data.

2. The Participants are not to communicate data provided under this Memorandum to any third State, international body or private entity without the prior consent of the Participant that provided the data and without the safeguards required by that Participant.
3. A Participant may conduct an automated query of the other Participant's fingerprint or DNA files under Paragraphs 4 or 8, and process data received in response to such a query, including the communication whether or not a hit exists, solely in order to:
 - (a) establish whether the compared DNA profiles or fingerprint data match;
 - (b) prepare and submit a follow-up request for assistance in compliance with the its laws, including those in relation to legal assistance, if those data match; or
 - (c) conduct record-keeping, as required or permitted by its laws. Record keeping refers to keeping a record of the query, and the response following a query if there is a match.

The Participant administering the file may process the data supplied to it by the querying Participant during the course of an automated query in accordance with Paragraphs 4 and 8 solely where this is necessary for the purposes of comparison, providing automated replies to the query or record-keeping pursuant to Paragraph 17. The data supplied for comparison are to be deleted immediately following data comparison or automated replies to queries unless further processing is necessary for the purposes mentioned under subparagraphs 15(3)(b) or (c).

16. Correction, blockage and deletion of data

1. At the request of the supplying Participant, the receiving Participant is to correct, block, or delete, consistent with its laws, data received under this Memorandum that are incorrect or incomplete or if its collection or further processing is inconsistent with this Memorandum or the measures applicable to the supplying Participant.
2. Where a Participant becomes aware that data it has received from the other Participant under this Memorandum are not accurate, it is to take all appropriate measures to safeguard against erroneous reliance on such data, which is to include in particular supplementation, deletion, or correction of such data.
3. Each Participant is to notify the other if it becomes aware that material data it has transmitted to the other Participant or received from the other Participant under this Memorandum are inaccurate or unreliable or are subject to significant doubt.

17. Documentation

1. Each Participant is to maintain a record of the transmission and receipt of data communicated to the other Participant under this Memorandum. This record is to serve to:

- (a) ensure effective monitoring of data protection in accordance with the laws of the respective Participant;
 - (b) enable the Participants to effectively make use of the rights granted to them according to Paragraphs 15 and 19; and
 - (c) ensure data security.
2. The record is to include:
 - (a) information on the data supplied;
 - (b) the date of supply; and
 - (c) the recipient of the data in case the data are supplied to other entities.
3. The recorded data are to be protected against inappropriate use and other forms of improper use and are to be kept for two years. After the conservation period the recorded data are to be deleted immediately, unless this is inconsistent with laws of the receiving Participant, including applicable data protection and retention rules.

18. Data Security

1. The Participants are to ensure that the necessary technical measures and organizational arrangements are utilized to protect personal data against accidental or unlawful destruction, accidental loss or unauthorized disclosure, alteration, access or any unauthorized form of processing. The Participants in particular are to take reasonable measures to ensure that only those authorized to access personal data can have access to such data.
2. The implementing arrangements that govern the procedures for automated querying of fingerprint and DNA files pursuant to Paragraphs 4 and 8 are to provide:
 - (a) that appropriate use is made of modern technology to ensure data protection, security, confidentiality and integrity;
 - (b) that encryption and authorization procedures recognized by the competent authorities are used when having recourse to generally accessible networks; and
 - (c) for a mechanism to ensure that only permissible queries are conducted.

19. Transparency – Providing information to the data subjects

1. Nothing in this Memorandum is to be interpreted to interfere with the Participants' legal obligations, as set forth by their respective laws, to provide data subjects with information as to the purposes of the processing and the identity of the data controller, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him or her and any further information such as the legal basis of the processing operation for which the data are intended, the time limits for storing the data and the right of recourse, in so far as such further information is necessary, having regard for the purposes and the specific circumstances in which the data are processed, to guarantee fair processing with respect to data subjects.

2. Such information may be denied in accordance with the respective laws of the Participants, including if providing this information may jeopardize:
 - (a) the purposes of the processing;
 - (b) investigations or prosecutions conducted by the competent authorities in the United States or by the competent authorities in Australia; or
 - (c) the rights and freedoms of third parties.

20. Information

Upon request, the receiving Participant is to inform the supplying Participant of the processing of supplied data and the result obtained. The receiving Participant is to ensure that its answer is communicated to the supplying Participant in a timely manner.

21. Relation to Other Arrangements

Nothing in this Memorandum is to be construed to limit or prejudice the provisions of any treaty, other arrangement, working law enforcement relationship, or laws allowing for information sharing between the United States and Australia.

22. Consultations

1. The Participants are to consult each other regularly on the implementation of the provisions of this Memorandum.
2. In the event of any dispute regarding the interpretation or application of this Memorandum, the Participants are to consult each other in order to facilitate its resolution.

23. Expenses

Each Participant is to bear the expenses incurred by its authorities in implementing this Memorandum. In special cases, the Participants may mutually consent to different arrangements.

24. Discontinuance of the Memorandum

Cooperation under this Memorandum may be discontinued by either Participant. The Participants intend the Participant discontinuing cooperation to give three months' notice in writing to the other Participant. The Participants intend to continue to apply the terms of this Memorandum to data supplied prior to such discontinuation.

25. Revisions

1. The Participants are to enter into consultations with respect to revisions to this Memorandum at the request of either Participant.
2. This Memorandum may be revised by the mutually written consent of the Participants at any time.

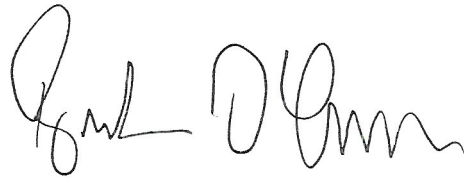
26. Commencement

1. The Participants intend to begin cooperation under this Memorandum, with the exception of Paragraphs 8, 10 and 11, on the date of signature by both Participants.
2. The Participants intend to begin cooperation under Paragraphs 8 and 10 through 11 of this Memorandum following the completion of the implementing arrangement(s) referred to in Paragraph 11 if the laws of both Participants permit the type of DNA screening contemplated by Paragraphs 8, 10 and 11.

Signed at Canberra, this ^{16TH}.....day of November 2011, in duplicate.



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



**FOR THE GOVERNMENT OF
AUSTRALIA:**