

MEMORANDUM OF UNDERSTANDING
BETWEEN THE
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
AND THE
DEPARTMENT OF DEFENSE
BIOMETRICS TASK FORCE
CONCERNING THE
CHANNELING OF CIVIL FINGERPRINT SUBMISSIONS

I. PARTIES

This Memorandum of Understanding (MOU) is entered into by the FBI Criminal Justice Information Services (CJIS) Division and the Department of Defense (DoD) Biometrics Task Force (BTF), hereinafter referred to as the parties.

II. PURPOSE

This MOU documents the responsibilities and functions of each party with respect to the submission and processing of fingerprint-based criminal history record check requests pursuant to the DoD's Identification-based Decision Process to Enable Confident Transactions (IDProTECT) pilot project. Fingerprint submissions will be limited to employment, credentialing, or security clearance investigations of DoD personnel, and the pilot is expected to be run for ten (10) months.

III. AUTHORITIES

The FBI, on behalf of the Attorney General, may exchange records and information with, and for the official use of, authorized officials of the Federal Government under Title 28, United States Code (U.S.C.), Section 534. The DoD enters into this MOU, pursuant to 5 U.S.C. §§552a, 3571, 7532, and 9101; 50 U.S.C. §§831, 832, and 834; Executive Orders 10450, 12333, 12958, and 13467; and Title 5, Code of Federal Regulations, Part 732.

IV. BACKGROUND INFORMATION

The DoD expects to channel fingerprints to the FBI for noncriminal justice criminal history record check requests as part of the IDProTECT pilot project.

The fingerprint-based check results will be in support of employment, Homeland Security Presidential Directive-12, and security clearance determinations. At the successful conclusion of the initial ten-month pilot, the DoD expects to request the continuation of this initiative on an ongoing operational basis. Such a request will result in a revised MOU.

As part of this pilot, the BTF will submit fingerprint and biographic data to the CJIS Division. The CJIS Division will conduct searches against the Integrated Automated Fingerprint Identification System (IAFIS) and provide the results of those searches to the BTF for dissemination to subordinate authorized DoD entities.

V. SPECIFIC RESPONSIBILITIES

A. The CJIS Division will:

1. Establish an electronic interface between the CJIS Division and the BTF to support the processing of biometric submissions relating to the IDProTECT Project.
2. Provide the BTF with a unique Originating Agency Identifier to be used exclusively for fingerprint submissions relating to the IDProTECT Project.
3. Search the IAFIS based on the fingerprint and biographic data submitted by the BTF as specified in this MOU.
4. Provide to the BTF the results of those searches in an electronic format mutually agreed upon by the CJIS Division and the BTF.
5. Bill the BTF monthly for fingerprint submissions related to the IDProTECT Project as specified in the Interagency Agreement (IA).
6. Provide a point of contact (POC) for administrative issues relating to this MOU. Unless otherwise notified, the CJIS Division POC is:

[REDACTED]
Federal Bureau of Investigation
Criminal Justice Information Services Division
[REDACTED]
1000 Custer Hollow Road
Clarksburg, WV 26306
[REDACTED]

b6 per FBI

B. The BTF will:

1. Submit electronic fingerprint-based criminal history record check search requests to the FBI in compliance with the American National Standard for Information Systems - *Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information* (ANSI/NIST ITL 1-2007).
2. Coordinate and execute an IA with the CJIS Division.
3. Coordinate with the CJIS Division to ensure appropriate testing has been performed and approval has been granted for the type (flat or rolled) of fingerprint submissions.
4. Make a reasonable effort to ensure that all fingerprint submissions are properly and adequately completed by the applicant or the submitting agency. The reason fingerprinted must appear in the appropriate areas of each fingerprint submission.
5. Remit payments for fingerprint processing services as specified in the IA. The BTF will ensure sufficient funds are available to reimburse the FBI for services rendered.
6. Submit Federal Applicant User Fee Type of Transaction (TOT) fingerprint submissions. Any change in TOT must be documented in an addendum to this MOU prior to the submission of such fingerprints.
7. Provide a POC for administrative issues relating to this MOU. Unless otherwise notified, the BTF POC is:

Ms. Cheley Gabriel
Chief
DoD Biometrics Task Force
Enterprise Support Division

b6 per ARMY

VI. EFFECT OF THIS AGREEMENT

- A.** This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise against any of the parties, their parent agencies, the

United States, or the officers, employees, agents, or other associated personnel thereof. The parties will seek to resolve any disputes regarding this MOU by mutual consultation.

- B. This MOU is not an obligation or commitment of funds (except as noted in the SPECIFIC RESPONSIBILITIES paragraph above), nor a basis for transfer of funds, but rather is a basic statement of the understanding between the parties of the matters described herein. Unless otherwise agreed in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the language in this MOU in no way implies that funds will be made available for such expenditures.
- C. This MOU does not constitute an agreement for any party to assume or waive any liability or claim under any applicable law.
- D. The information involved in this MOU may identify U.S. persons, whose information is protected by the Privacy Act of 1974 and/or Executive Order 12333 (or any successor executive order). All such information will be handled lawfully pursuant to the provisions thereof.
- E. Each party that discloses personally identifiable information (PII) is responsible for making reasonable efforts to ensure that the information disclosed is accurate, complete, timely, and relevant.
- F. Before using PII shared pursuant to this MOU, the recipient agency will make reasonable efforts to ensure that the information is accurate, timely, relevant and complete.
- G. In the event that either party to this MOU becomes aware of any inaccuracies in information received from the other party pursuant to this MOU, the information recipient will promptly notify the information provider so that corrective action can be taken.
- H. Section (c) of the Privacy Act, 5 U.S.C. 552a(c), requires that an agency maintain the ability to provide an accounting for covered disclosures made outside the disclosing agency. The accounting must include the date, nature, and purpose of each disclosure and the name and address of the person or agency to which the disclosure is made. The accounting must be maintained for five (5) years after the disclosure for which the accounting is required or for the life of the record, whichever is longer. To the extent that this provision of the Privacy Act is applicable to disclosures of PII made under the MOU, each party will be responsible for compliance.

- I. Each party will immediately report to the other party each instance in which information received from the other party is used, disclosed, or accessed in an unauthorized manner (including any information losses or breaches).
- J. Each party will provide appropriate training regarding the responsibilities under this MOU to individuals whose information sharing activities are covered by the provisions of this MOU.
- K. Subject to federal law or regulation, the FBI may audit the handling and maintenance of information relevant to this MOU in electronic and paper recordkeeping systems to ensure that appropriate security and privacy protections are in place.

VII. EFFECTIVE DATE, MODIFICATION AND TERMINATION

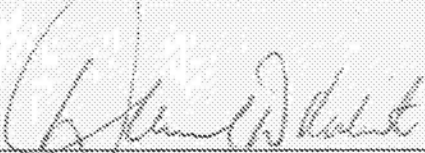
This agreement shall be effective when executed by both parties and will continue in effect until terminated. This agreement may be modified at any time by written consent of the parties.

This MOU may be terminated, with respect to any party, at any time upon written notice to the other party. Any party desiring to withdraw from this MOU will endeavor to provide such written notification to the other party at least thirty (30) days prior to withdrawal. The parties intend to review this MOU annually to ensure all provisions are meaningful and current.

MOU between the FBI CJIS Division and the DoD BTF concerning the Channeling of Civil Fingerprint Submissions

The foregoing represents the understanding reached by the FBI CJIS Division and the DoD BTF.

FOR THE FEDERAL BUREAU OF INVESTIGATION:

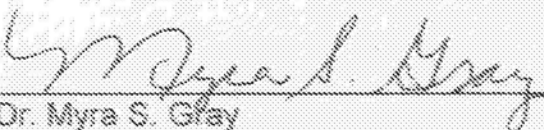


Daniel D. Roberts
Assistant Director
FBI CJIS Division

12/31/09

Date

FOR THE DEPARTMENT OF DEFENSE:



Dr. Myra S. Gray
Executive Manager, DoD Biometrics
Director, Biometrics Task Force

01/07/2010

Date

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DEPARTMENT OF STATE
BUREAU OF DIPLOMATIC SECURITY
AND
THE DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
AND
THE DEPARTMENT OF DEFENSE
DEFENSE FORENSICS AND BIOMETRICS AGENCY
FOR
SHARING OF BIOMETRIC AND OTHER IDENTITY MANAGEMENT DATA

I. PARTIES

The parties to this Memorandum of Understanding (MOU) are the Department of State (DOS) Bureau of Diplomatic Security (DS), the Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division, and the Department of Defense (DOD) Defense Forensics and Biometrics Agency (DFBA), hereinafter referred to as "party" or "the parties."

II. PURPOSE

The purpose of this MOU is to share biometric and contextual data among the parties by leveraging existing data sharing practices through developing a direct conduit for the parties to access databases storing biometric information. It is in the Nation's interest for DS, CJIS and DFBA to share this information to ensure the prompt and accurate updating of biometric records worldwide, guaranteeing the overall accuracy and thoroughness of regular name checks and background investigations for suitability and security determinations. Facilitating and improving the capabilities of each party to share biometric information with each other will directly affect the safety and security of U.S. Government officials and facilities domestically and internationally. Under an existing information sharing MOU between DOD and FBI, the DOD Automated Biometric Identification System (ABIS) shares biometric information with CJIS through the Integrated Automated Fingerprint Identification System (IAFIS). Likewise, DS and CJIS share biometric data directly under an interagency agreement for non-criminal justice applicant fingerprint checks.

III. AUTHORITY

DFBA enters into this MOU under the authority of National Security Presidential Directive-59 (NSPD-59)/Homeland Security Presidential Directive-24 (HSPD-24) for the use, analysis, and sharing of biometric and associated biographic and contextual information of individuals necessary to protect national security; Public Law 106-246, section 112; and DOD Directive 8521.01E, Department of Defense Biometrics.

CJIS enters into this MOU under the authority of 5 U.S.C. § 9101, 28; U.S.C. § 533, 534; 28 C.F.R. § 0.85; and the Attorney General's April 11, 2002, order to coordinate and share information related to terrorism.

DS enters into this MOU under the authority of Executive Order 12968, Access to Classified Information; 5 C.F.R. § 731, Suitability and Actions; NSPD-59/HSPD-24 for the use, analysis, and sharing of biometric and associated biographic and contextual information of individuals necessary to protect national security; HSPD-12 for use of the government-wide standard identification system; HSPD-11 regarding immigration; HSPD-6 for diplomatic, law enforcement, immigration, visa and protective processes; 22 U.S.C. § 4806, Protection of Foreign Consulates; 22 U.S.C. § 4807, Establishment of Visa and Passport Security Program in the Department of State; 18 U.S.C. § 911, False representation of citizens of the United States; 18 U.S.C. § 1028, Fraud and related activity in connection with identification documents, authentication features, and information; 18 U.S.C. § 1546, Fraud and misuse of visas, permits, and other documents; and 18 U.S.C. § 7, Special maritime and territorial jurisdiction of the United States.

IV. DEFINITIONS

- A. **BIOMETRIC:** A measure of an identifying physical aspect of an individual—e.g., a fingerprint, iris scan, or DNA—that can be turned into a digital template capable of being electronically stored and compared for verification or matching purposes.
- B. **BIOMETRIC DATA:** Computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores. Biometric data is used to describe the information collected during an enrollment, verification, or identification process, but does not apply to end user information such as user name, demographic information and authorizations.
- C. **BIOMETRICS:** A general term used alternatively to describe a characteristic or a process. As a characteristic, it is the measure of a biological (anatomical and physiological) and/or behavioral biometric characteristic that can be used for automated recognition. As a process, it is automated methods of recognizing an individual based on the measure of biological (anatomical and physiological) and/or behavioral biometric characteristics.
- D. **CONTEXTUAL DATA:** Elements of biographical and situational information associated with an enrollment and permanently recorded as an integral component of the biometric file.
- E. **DEROGATORY INFORMATION:** For the purposes of this MOU and associated annexes, derogatory information is defined as any information related to known or suspected involvement in terrorism or terrorist activities; known criminal history; known or suspected participation in espionage or counter-intelligence activities; known or suspected falsification of records in seeking employment with any U.S.

government entity or access to any U.S. Government facility; known or suspected falsification of travel documents.

- F. **ENROLLMENT:** The process of collecting a biometric sample from a biometric subject, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.
- G. **INFORMATION INCIDENT:** The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, or for any other than authorized purpose, have access or potential access to shared unclassified information in usable form, whether physical or electronic.
- H. **PERSONALLY IDENTIFIABLE INFORMATION (PII):** Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
- I. **PERSONS OF INTEREST:** Any non-U.S. person on whom DS holds derogatory information as defined above.
- J. **U.S. PERSON:** A living person who is a citizen of the United States, an alien lawfully admitted for permanent residence in the United States, or a member of the U.S. Armed Forces.

V. **BACKGROUND**

DS is responsible for providing a safe and secure environment for the conduct of U.S. foreign policy worldwide, establishing a security infrastructure to protect personnel, information and computer security. The Assistant Director for Domestic Operations (DS/DO) leads a global investigative office that conducts both criminal investigations involving the issuance of U.S. passports and visas and complex visa fraud investigations involving human smuggling, organized crime, or terrorism. The Office of Personnel Security and Suitability (DS/SI/PSS) reviews and analyzes background investigations of candidates for employment, and for employees and contractors seeking physical and logical access to DS to assure that granting an individual access to classified information is consistent with the interests of national security. DS/SI/PSS conducts approximately 35,000 personnel security background investigations for suitability determinations and clearances each year. These background investigations include an increasing number of requests and applications from foreign nationals for access to U.S. facilities abroad. The Deputy Assistant Secretary and Assistant Director for International Programs (DS/IP) and the Deputy Assistant Secretary for High Threat Programs (DS/HTP) provide leadership, support, and oversight of overseas security and law enforcement programs and related policy for the benefit of U.S. Government interests and the international community.

The CJIS Division serves as the Nation's central repository for identification and criminal history record information. The CJIS Division maintains millions of digital representations of fingerprint images, features from digital fingerprint images, and associated criminal history record information in the Fingerprint Identification

Record System (FIRS). The FIRS incorporates an automatic fingerprint search capability via its IAFIS.

DFBA leads and coordinates the development, adoption and institutionalization of biometric techniques for acquiring and retaining biometric and other descriptive data recorded by military units. DFBA's Biometrics Identity Management Activity (BIMA) operates and maintains the DOD's ABIS, which stores, matches, and shares biometrics and other identity management data (including biographical and contextual data).

The parties acknowledge that the information involved in this MOU may identify U.S. persons whose information is protected by the Privacy Act of 1974 and/or Executive Order 12333 (or any successor executive order). All such information will be handled lawfully pursuant to the provisions thereof.

VI. RESPONSIBILITIES

All parties will:

1. Adhere to applicable technical standards, appropriate business processes, and privacy protection mechanisms required under the Privacy Act of 1974 related to the sharing of U.S. Government data and conform to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII). Subsequent to the signing of this MOU, the parties will develop and agree to technical procedures identifying the specific processes by which privacy protections will be observed. No data will be shared pursuant to this MOU until such procedures are implemented.

2.

3.

4.

5.

b7E per DOS

[Redacted]

b7E per DOS

6. Report to the other parties immediately upon discovering that an information incident has occurred.

7. [Redacted]

8. [Redacted]

b7E per DOS

VII. FUNDING

This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

VIII. EFFECT OF THIS AGREEMENT

This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise against any of the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof. The parties will seek to resolve any disputes regarding this MOU by mutual consultation.

This MOU does not rescind or modify, in whole or in part, any existing agreements between or among the parties. In the event of an inconsistency or conflict between this and other agreements, the party identifying the issue will discuss and resolve the conflict with all other parties before any action is taken. Additionally, should any conflict arise concerning the substance or interpretation of the terms of this agreement, the issues in question will be discussed and resolved by all parties before any action is taken.

IX. DISPUTE RESOLUTION

In the event that disputes among DS, CJIS, and DFBA cannot be resolved at the program level despite good faith efforts, the matter should be elevated to the approving officials listed in section XI for resolution.

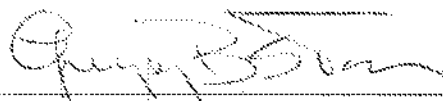
X. EFFECTIVE DATE, DURATION, AMENDMENT, TERMINATION

The terms of this agreement and any subsequent addenda shall be effective upon the signature of all parties and shall continue in effect unless notice is given by one party to the others that the notifying party wishes to renegotiate, terminate, or withdraw from the agreement. Such written notice shall be provided at least 60 days prior to the proposed amendment, termination, or withdrawal. Modifications shall have a written agreement of consent by all parties.

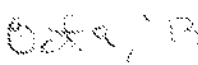
The authorized agency officials whose signatures appear below have committed their respective agencies to the terms of this agreement, subject to annual review to determine whether amendments are needed.

XI. APPROVAL

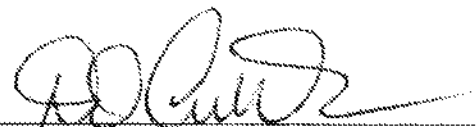
The foregoing represents the understanding reached between DS, CJIS, and DFBA.



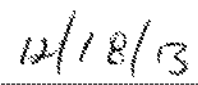
Gregory B. Starr
Principal Deputy Assistant Secretary
Bureau of Diplomatic Security
Department of State



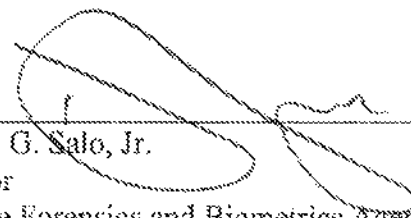
Date



David Cuthbertson
Assistant Director
Criminal Justice Information Services Division
Federal Bureau of Investigation



Date

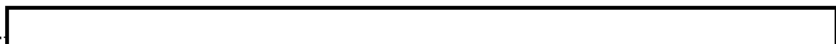





Donald G. Salo, Jr.
Director
Defense Forensics and Biometrics Agency
Department of Defense



Date

Attached:

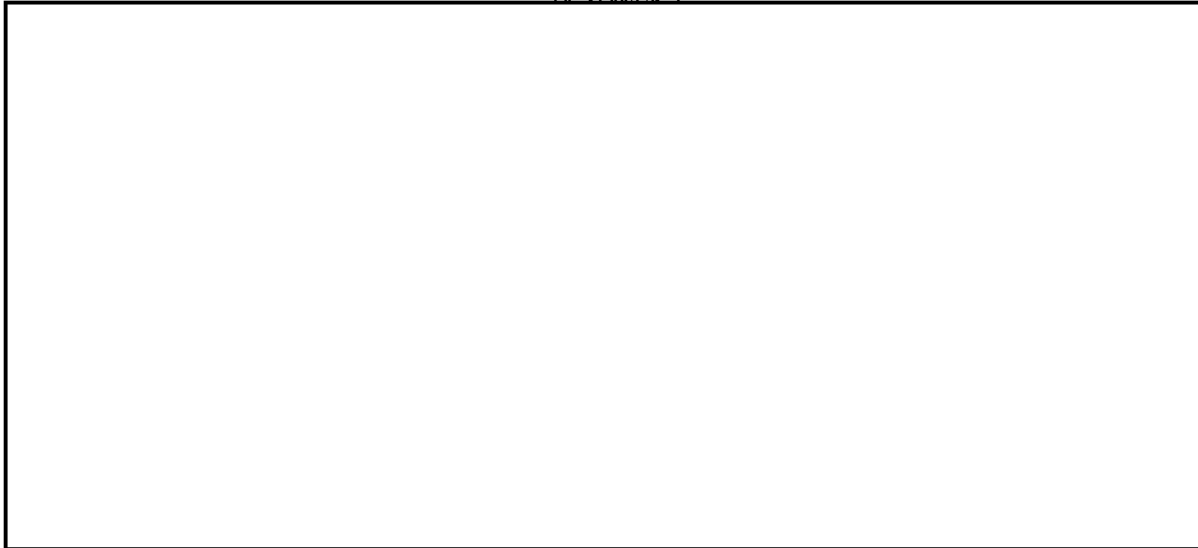
- A. Annex 1 - 

- B. Annex 2 - 


b7E per DOS

C. Annex 3

b7E per DOS

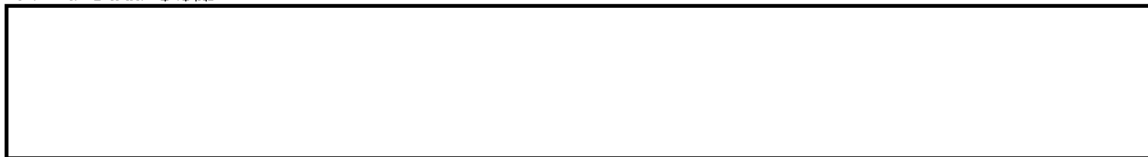
ANNEX 1



b7E per DOS

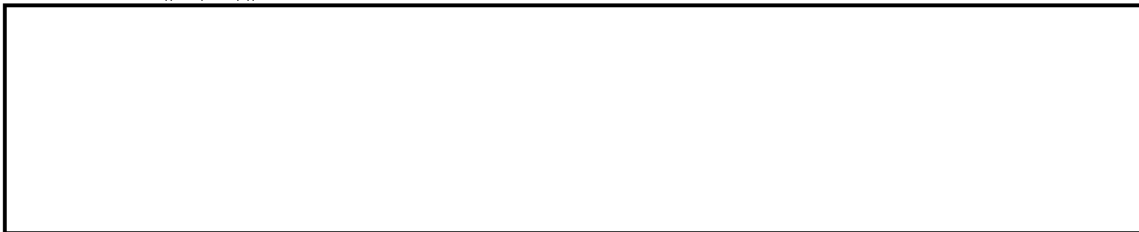
This Annex is governed by the general provisions of the Memorandum of Understanding (MOU) between the Department of State (DOS) Bureau of Diplomatic Security (DS), the Federal Bureau of Investigations (FBI) Criminal Justice Information Services Division (CJIS) and the Department of Defense (DOD) Defense Forensics and Biometrics Agency (DFBA) for sharing of biometric and other identity management data.

I. PURPOSE



b7E per DOS

II. OBJECTIVE



b7E per DOS

III. SCOPE

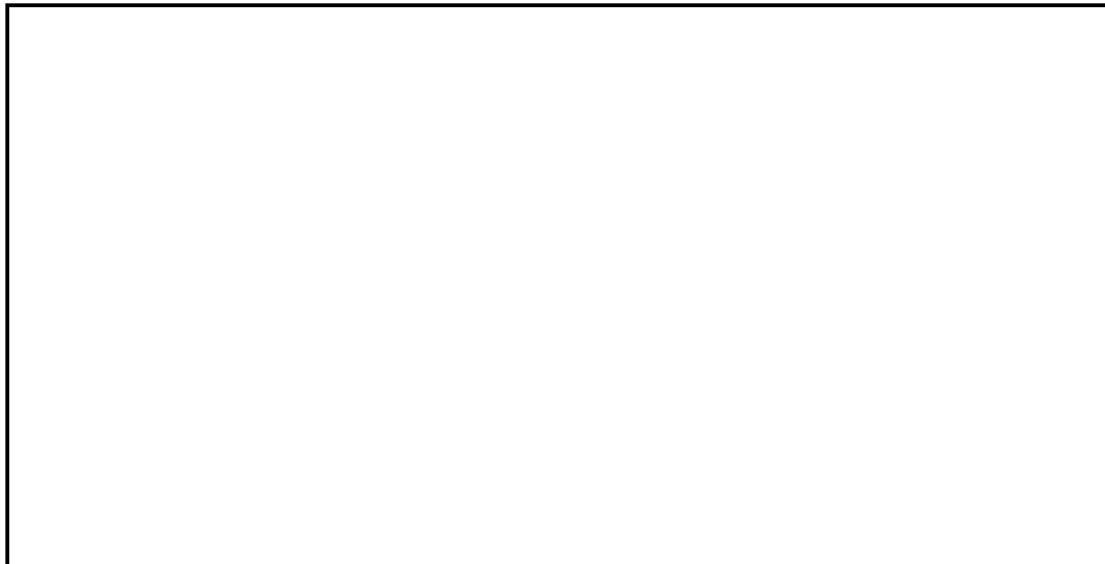


b7E per DOS

IV. PROCEDURES



b7E per DOS



b7E per DOS

V. FUNDING

This Annex is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this Annex and its source MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

VI. EFFECTIVE DATE, DURATION, AMENDMENT, TERMINATION

This Annex shall be effective upon the signature of all parties and shall continue in effect unless notice is given by one party to the other that the notifying party wishes to renegotiate, terminate, or withdraw from the agreement. Such written notice shall be provided at least 60 days prior to the proposed amendment, termination, or withdrawal. Modifications shall have a written agreement of consent by both parties.

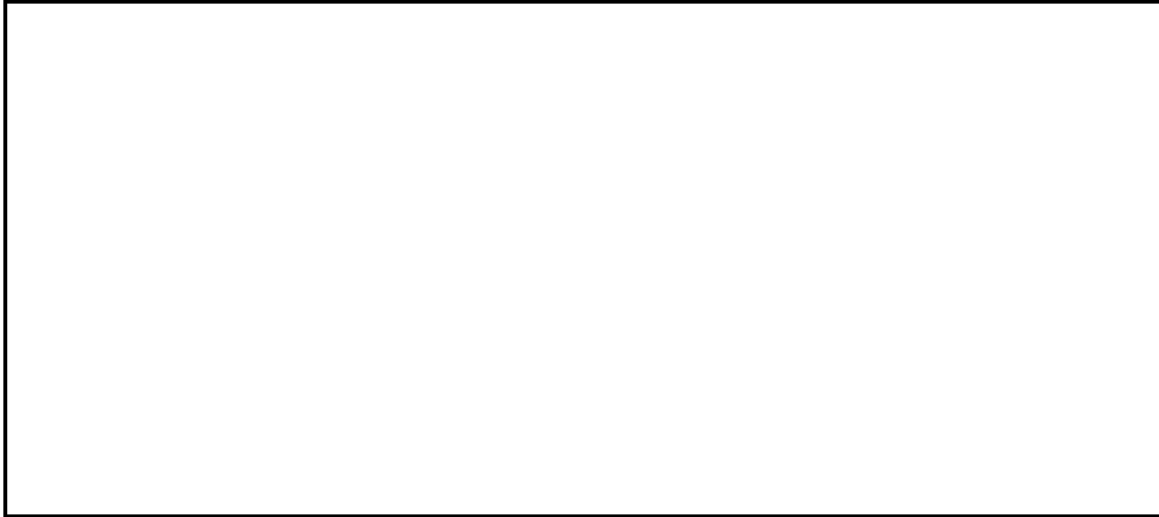
The authorized agency officials whose signatures appear in the MOU have committed their respective agencies to the terms of this agreement, subject to annual review to determine whether amendments are needed.

VII. APPROVAL



b7E per DOS

ANNEX 2



b7E per DOS

This Annex is governed by the general provisions of the Memorandum of Understanding (MOU) between the Department of State (DOS) Bureau of Diplomatic Security (DS), the Federal Bureau of Investigations (FBI) Criminal Justice Information Services Division (CJIS) and the Department of Defense (DOD) Defense Forensics and Biometrics Agency (DFBA) for sharing of biometric and other identity management data.

I. PURPOSE



b7E per DOS

II. OBJECTIVE



b7E per DOS

III. SCOPE

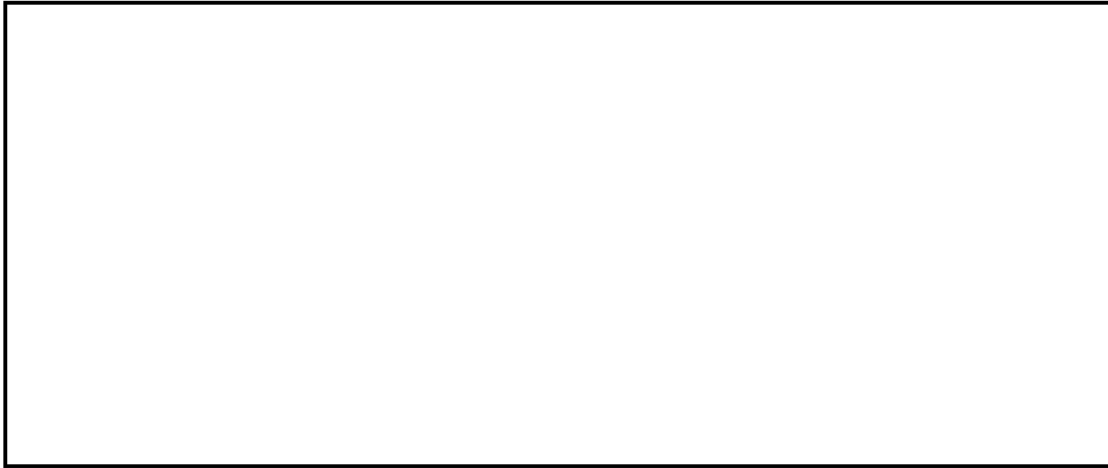


b7E per DOS

IV. PROCEDURES



b7E per DOS



b7E per DOS

V. FUNDING

This Annex is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this Annex and its source MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

VI. EFFECTIVE DATE, DURATION, AMENDMENT, TERMINATION

This Annex shall be effective upon the signature of both parties and shall continue in effect unless notice is given by one party to the other that the notifying party wishes to renegotiate, terminate, or withdraw from the agreement. Such written notice shall be provided at least 60 days prior to the proposed amendment, termination, or withdrawal. Modifications shall have a written agreement of consent by both parties.

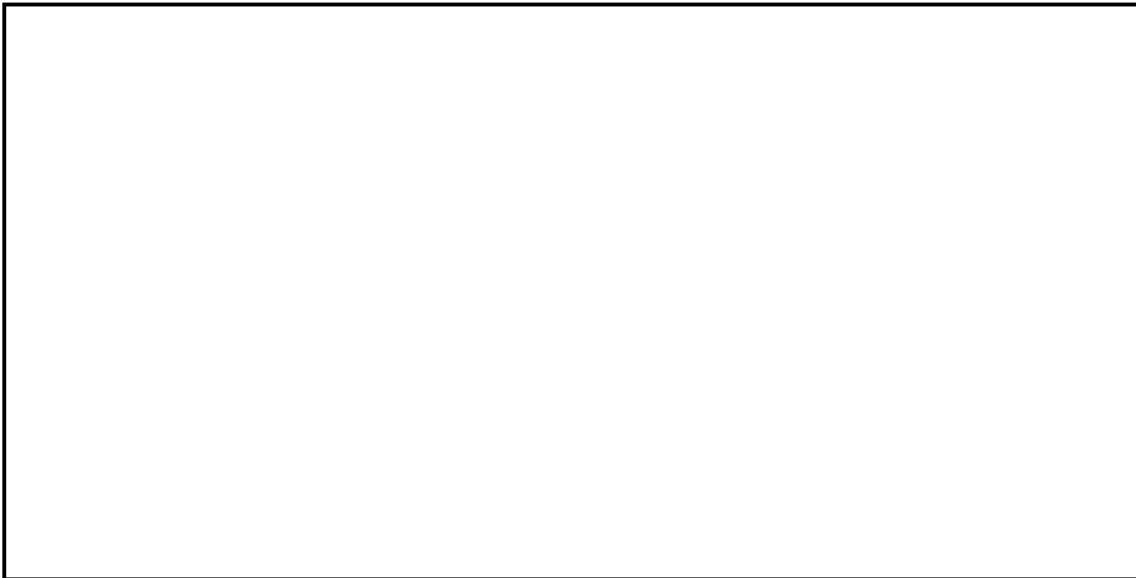
The authorized agency officials whose signatures appear in the MOU have committed their respective agencies to the terms of this agreement, subject to annual review to determine whether amendments are needed.

VII. APPROVAL



b7E per DOS

ANNEX 3



b7E per DOS

This Annex is governed by the general provisions of the Memorandum of Understanding (MOU) between the Department of State (DOS) Bureau of Diplomatic Security (DS), the Federal Bureau of Investigations (FBI) Criminal Justice Information Services Division (CJIS) and the Department of Defense (DOD) Defense Forensics and Biometrics Agency (DFBA) for sharing of biometric and other identity management data.

I. PURPOSE



b7E per DOS

II. OBJECTIVE



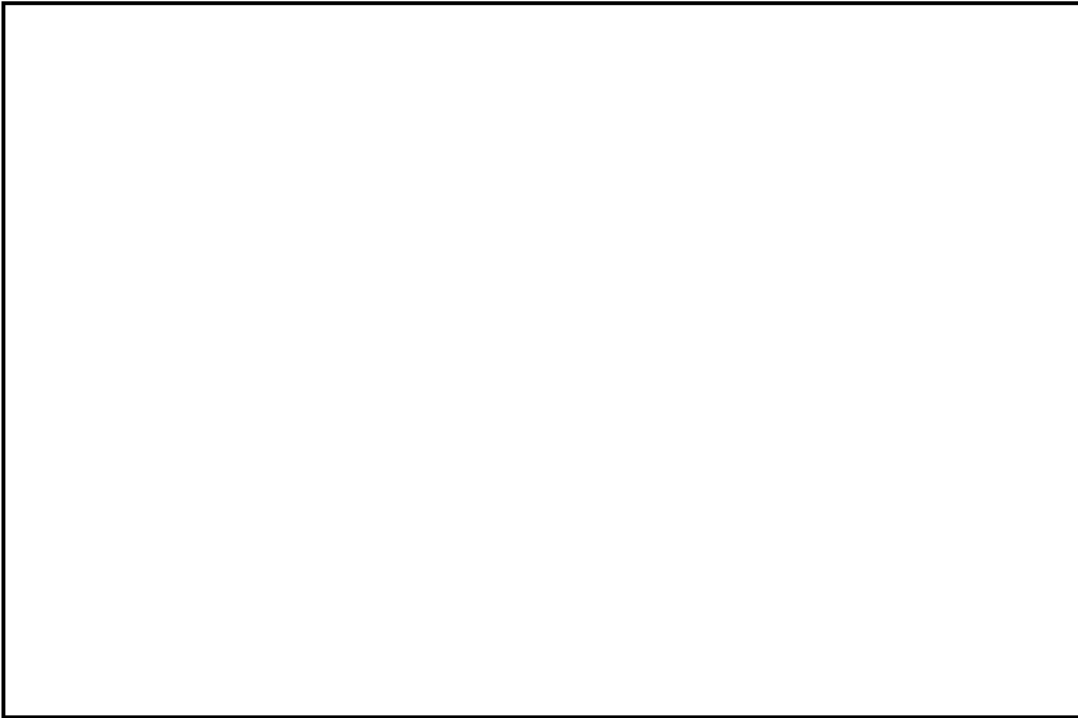
b7E per DOS

III. SCOPE



b7E per DOS

IV. PROCEDURES



b7E per DOS

V. FUNDING

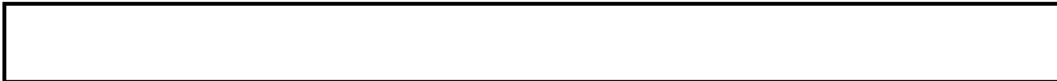
This Annex is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this Annex and its source MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

VI. EFFECTIVE DATE, DURATION, AMENDMENT, AND TERMINATION

This Annex shall be effective upon the signature of both parties and shall continue in effect unless notice is given by one party to the other that the notifying party wishes to renegotiate, terminate, or withdraw from the agreement. Such written notice shall be provided at least 60 days prior to the proposed amendment, termination, or withdrawal. Modifications shall have a written agreement of consent by both parties.

The authorized agency officials whose signatures appear in the MOU have committed their respective agencies to the terms of this agreement, subject to annual review to determine whether amendments are needed.

VII. APPROVAL



b7E per DOS

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**MEMORANDUM OF UNDERSTANDING
BETWEEN THE FEDERAL BUREAU OF INVESTIGATION
AND THE DEPARTMENT OF DEFENSE
GOVERNING INFORMATION SHARING,
OPERATIONAL COORDINATION, AND INVESTIGATIVE RESPONSIBILITIES**

1. PURPOSE. This Memorandum of Understanding (MOU) between the Department of Defense (DoD) and the Federal Bureau of Investigation (FBI) [hereinafter the Parties] is designed to promote systemic, standardized, and controlled information sharing, and to clarify operational coordination procedures and investigative responsibilities between DoD and FBI.

2. SCOPE.

a. This MOU covers the FBI/DoD sharing of counterintelligence, counterterrorism, foreign intelligence, law enforcement, operational, and other information; and operational coordination, and investigative responsibilities.

b. This MOU applies to all components of FBI and DoD.

c. All future agreements between FBI and DoD regarding information sharing, operational coordination, and investigative responsibilities shall be consistent with this MOU and shall be incorporated as annexes once adopted.

d. This MOU, along with Annexes A (Counterterrorism Information Sharing), B (Counterintelligence Information Sharing), and future annexes covering Counterintelligence and Counterterrorism Jurisdiction and Operational Activities, when approved, supersede the "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation" (1979) and the 1996 supplement thereto, "MOU Regarding Coordination of Counterintelligence Matters." All other existing agreements and understandings between DoD Components and FBI governing information sharing, operational coordination, or investigative responsibilities will remain in effect except for those provisions that are inconsistent with this MOU and its Annexes. Whenever there is an inconsistency, this MOU and its Annexes will govern. All existing agreements and understandings between DoD Components and FBI will be expeditiously reviewed, updated, or rescinded, and copies forwarded to the FBI Executive Assistant Director, National Security Branch, the FBI Office of General Counsel, and the DoD Under Secretary of Defense for Policy (Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs)) as repositories for FBI and DoD, respectively. Those MOUs that have as their primary objective information sharing, operational coordination, or investigative responsibilities for intelligence, counterintelligence, force protection, law enforcement, security, or counterterrorism purposes shall be appended as annexes to this MOU, subject to mutual agreement by the Executive Assistant Director, National Security Branch, and the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs), or their designated representatives.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

3. REFERENCES.

- a. The USA PATRIOT Act (Public Law 107-56), as amended.
- b. The Homeland Security Act, as amended (Public Law 107-296).
- c. The Intelligence Reform and Terrorism Prevention Act (Public Law 108-458), as amended.
- d. The National Security Act of 1947, as amended.
- e. Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans.
- f. Executive Order 12333, United States Intelligence Activities, as amended.
- g. Executive Order 13526, Classified National Security Information.
- h. Homeland Security Presidential Directive 6, Integration and Use of Screening Information.
- i. Homeland Security Presidential Directive 11, Comprehensive Terrorist Related Screening Procedures.
- j. Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors.
- k. Homeland Security Presidential Directive 15/National Security Presidential Directive 46, U.S. Policy and Strategy in the War on Terror (and Annexes).
- l. Homeland Security Presidential Directive 24/National Security Presidential Directive 59, Biometrics for Identification and Screening to Enhance National Security.
- m. Intelligence Community Directive 710, Classification and Control Markings System.
- n. The Privacy Act of 1974, as amended.

4. DEFINITIONS. (Note: All definitions are for the purposes of this MOU and Annexes.)

- a. Counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
- b. Counterterrorism. Information gathered and operations conducted, including offensive measures, taken to prevent, deter, preempt, or respond to domestic or international terrorism.

c. DoD-Affiliated Personnel. DoD active duty and retired military personnel, civilian employees, contractors and their employees, active and inactive reservists, National Guard members, family members of active duty and civilian personnel, persons residing on or having access to a DoD facility, persons under consideration for DoD employment, and former DoD employees or contractors.

d. DoD Components. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense.

e. Force Protection. Protective measures taken to mitigate hostile actions against DoD personnel (including family members), resources, facilities, and critical information.

f. Foreign Intelligence. Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

g. Information Sharing. A timely two-way flow of information that has an impact on the missions, capabilities, operations, resources, or infrastructure of one or both of the Parties. Information sharing is intended to support the national security of the United States and the missions and capabilities of both Parties, including, but not limited to law enforcement, war fighter operations, intelligence activities, detainee affairs, force protection efforts, anti-terrorism, special operations, stability operations, homeland defense, counterintelligence, critical infrastructure protection, and other national interests.

h. Investigative Responsibilities. The act of fact gathering: 1. pertaining to a criminal act leading to, and including, the submission of evidence to a prosecutive authority; or 2. pertaining to the collection of intelligence.

i. Operational Coordination. The solicitation of inputs prior to undertaking a proposed action, with the understanding that no such action will be taken until any identified objections have been resolved.

5. GENERAL AGREEMENTS AND PROCEDURES.

a. Agreement. The Parties agree to share (consistent with any applicable legal restrictions) all counterintelligence, counterterrorism, foreign intelligence, law enforcement, operational, and other information that reasonably appears relevant to the mission, function, and capability of the other organization. The Parties also agree to coordinate and conduct operations as specified in Annexes to this MOU.

b. Procedures. The Parties will jointly develop understandings and procedures governing the sharing and protection of counterintelligence information, counterterrorism information, foreign

intelligence, law enforcement, operational, and other information. In addition, the parties will jointly develop understandings and procedures governing operational coordination and investigative responsibilities. These understandings and procedures shall be incorporated into individual annexes to this MOU.

6. GENERAL PROVISIONS.

a. Conflict with Current Law, Regulations, or Directives. This MOU is not intended to conflict with current law, executive orders, or regulations (including the directives of the FBI, DOJ, DoD, and the Office of the Director of National Intelligence), or court orders (including court-ordered procedures). If any term or provision of this MOU is inconsistent with such authority, then the term or provision will be invalid, but the remaining terms and conditions of this MOU will remain effective.

b. Non-Fund Obligor Document. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds. Instead, it establishes a process to ensure mission-essential sharing of information already available, and encourages more efficient and effective sharing of mission-essential information collected in the future. There are no reimbursable expenses associated with the routine sharing of the information covered by this MOU, and each Party shall bear its own costs in relation to the MOU. Expenditures will be subject to Federal and departmental budgetary processes and the availability of funds pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that this MOU in no way implies that Congress will appropriate funds for such expenditures.

c. No Private Rights Created. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the Parties, their parent agencies, the U.S. Government, or the officers, employees, agents, or other associated personnel thereof.

d. Privacy Clauses.

(1) The Parties to this MOU will comply with the provisions of the U.S. Constitution and all applicable laws, executive orders, regulations, court orders (including court-ordered procedures) and policies.

(2) The Parties acknowledge that the information covered by this MOU may identify U.S. persons. The sharing of such information may be governed or limited by the Privacy Act of 1974, Executive Order 12333 (or any successor executive order), and/or regulation. All such information must be handled lawfully and in accordance with the provisions thereof, as well as the provisions of all other laws, regulations, and directives that govern the dissemination of U.S. person information.

(3) The Parties further acknowledge that this MOU is subject to guidelines that concern the protection of privacy, civil liberties, and other rights in the Information Sharing Environment

(ISE). The Parties agree to comply with these guidelines to the extent they are applicable.

(4) The Parties agree to review and make appropriate changes, if any, to their privacy compliance documents, including applicable Privacy Act system of records notices and notices required by the Privacy Act (5 U.S.C. 552a(e)(3)), to ensure that the scope and routine uses of such notices permit the collection, maintenance, and sharing of personal information.

(5) Each Party will be responsible for conducting any Privacy Impact Assessment(s) that implementation of this MOU may require under laws, regulations, or policies applicable to the respective Party.

(6) Each Party that discloses Personally Identifying Information (PII) to the other, or that uses PII disclosed by the other Party, will make reasonable efforts to ensure that the information disclosed is accurate, complete, timely, and relevant.

(7) Each Party to this MOU provides access to information from its records with the understanding that in the event the recipient becomes aware of any inaccuracies in the data, the recipient will promptly notify the other Party so that corrective action can be taken.

(8) Section (c) of the Privacy Act (5 U.S.C. 552a(c)) requires that an agency maintain the ability to provide an accounting for covered disclosures made outside the disclosing agency. The accounting must include the date, nature, and purpose of each disclosure and the name and address of the person or agency to which the disclosure is made. The accounting must be maintained for five years after the disclosure for which the accounting is required or for the life of the record, whichever is longer. To the extent that this provision of the Privacy Act is applicable to disclosures of PII made under this MOU, each Party will be responsible for compliance.

(9) Each Party is responsible for ensuring that information it discloses was not knowingly obtained or maintained in violation of any law, regulation, court order (including court-ordered procedures or certain other procedures submitted to courts), or policy applicable to the disclosing Party, and that information is only made available to the receiving Party as may be permitted by laws, regulations, court order (including court-ordered procedures or certain other procedures submitted to courts), policies, or procedures applicable to the disclosing Party.

(10) Each Party will immediately report to the other Party each instance in which data received from the other Party is used, disclosed, or accessed in an unauthorized manner (including any data losses or breaches). Further, the Party responsible for the breach will determine whether or not it is appropriate to notify the individuals involved, and do so if required.

(11) Each Party agrees that it will provide appropriate training regarding the responsibilities under this MOU to individuals whose information sharing activities are covered by the provisions of this MOU.

(12) Any violation of or dispute concerning these provisions shall be resolved through the adjudication process in Part 7.

7. ADJUDICATION PROCEDURES. When there are information sharing disagreements between the Parties related to this MOU, the following procedures will be used to resolve the disagreement rapidly:

a. The Parties will make every effort to resolve the disagreement at the lowest level possible, escalating as necessary through their respective organizations to achieve satisfactory resolution.

b. In the event resolution cannot be reached at lower levels, the Parties shall raise the disagreement to the FBI Executive Assistant Director, National Security Branch, and the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs). Within 48 hours of receiving notice of the impasse, these individuals shall communicate to resolve the disagreement.

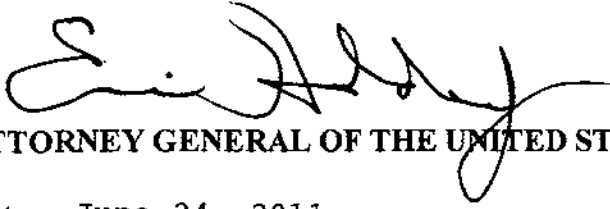
c. Should a resolution not be reached by the FBI Executive Assistant Director, National Security Branch, and the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs), the matter is to be referred within ten working days to the Under Secretary of Defense for Policy (in consultation with the Under Secretary of Defense for Intelligence) and the Director, FBI, for decision.

d. Disagreements arising from individual Annexes to this MOU will be governed by adjudication procedures delineated in the specific governing Annex.

8. NEW ANNEXES. DoD Components and FBI elements may enter into new information sharing, operational coordination, or investigative responsibility understandings consistent with their charters and authorities. Prior to signature, these understandings shall be forwarded to the Office of the Under Secretary of Defense for Policy and the FBI National Security Branch for coordination and review for consistency with this MOU, other applicable annexes, and departmental policy. Copies of final signed understandings are to be provided to the Under Secretary of Defense for Policy and the FBI National Security Branch and added as annexes to this MOU.

9. POINTS OF CONTACT. The Parties shall identify their respective points of contact in the Annexes.

10. EFFECTIVE DATE AND TERMINATION. The terms of this MOU become effective on the date on which it is signed by all Parties. Any Party may terminate this MOU upon 30 days written notice to the head of the other Party. All rights, obligations, responsibilities, limitations, and other understandings with respect to the disclosure and use of all information received during a Party's participation in this MOU shall survive any termination or release of a Party. In the event this MOU requires revision, renegotiation, or termination, all annexes will remain in effect unless otherwise agreed to by mutual consent of the Parties.



ATTORNEY GENERAL OF THE UNITED STATES

Date: June 24, 2011



SECRETARY OF DEFENSE

Date: AUG 2 2011

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE FEDERAL BUREAU OF INVESTIGATION
AND
THE DEPARTMENT OF DEFENSE
FOR TESTING AND PROTOTYPING THE
RAPID SEARCH OF THE REPOSITORY FOR INDIVIDUALS OF SPECIAL CONCERN

GENERAL PROVISIONS

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, and the Department of Defense (DoD), hereinafter referred to as the "parties", is for the limited purpose of testing and prototyping the FBI's Repository for Individuals of Special Concern (RISC) formerly referred to as the Enhanced Terrorist Identification Service (ETIS). This MOU memorializes the parties' understandings regarding the transmittal, receipt, storage, use, and dissemination of information relating to this initiative.

2. **BACKGROUND:** The FBI maintains millions of digital representations of fingerprint images, features from digital fingerprint images, and associated criminal history record information in the Fingerprint Identification Record System (FIRS), which incorporates the automatic search capability provided by the Integrated Automated Fingerprint Identification System (IAFIS). Collectively, these data comprise the biometric content, format, and units of measurement for the electronic exchange of information that may be used for positive fingerprint identifications. Given the advances in fingerprint identification technology, including hardware, software, and digital imaging, it is essential that IAFIS' search capabilities be enhanced to meet authorized customer needs. The CJIS Division's Next Generation Identification (NGI) Program will reduce terrorist and criminal activities by improving and expanding biometric services that are provided to the FBI's user community.

The RISC rapid search functionality will provide law enforcement the capability to search a limited population of FIRS-maintained fingerprints using a minimum of two and maximum of ten rolled or flat fingerprints. These searches will be checked against the RISC, which is anticipated to contain records of Wanted Persons, Known or Suspected Terrorists, and other persons of special interest. RISC data, for this initiative, will be extracted from FBI systems on a daily basis. Consequently, the RISC database will NOT always have the most current data available to the FBI.

CJIS Division responses to apparent fingerprint matches under this initiative will include, but not limited to, Red (Hit), Yellow (Possible Hit), and Green (No Hit) indicators. In addition, the responses will support dissemination rules based on a multi-tiered shared data structure.

The DoD has instituted and deployed a localized rapid identification program from mobile and/or fixed sites. Agency vendors have provided software and fingerprint capture devices that provide law enforcement officers the ability to scan fingerprint images and transmit these images to the DoD. The DoD will forward these images to the CJIS Division, via the CJIS Wide Area Network (WAN), for comparison against the RISC.

During the pilot test, relevant transactions will be analyzed by the parties and their authorized contractors to assess system performance. In addition, RISC system design will be refined using lessons learned and user input.

System availability will be limited during this initiative. Accordingly, the CJIS Division is providing advance notice of sporadic system availability, backup recovery limitations, and failover shortfalls during the prototype phase. In addition, the CJIS Division may limit the number of transactions that will be accepted during this phase.

3. AUTHORITY: The FBI enters into this MOU under the authority provided by Title 28, United States Code, § 534.

4. SCOPE: This MOU applies to fingerprint images provided by the DoD when requesting RISC searches and the FBI's resulting responses.

A. The FBI will:

1. Accept a minimum of two and maximum of ten flat or rolled type 4 fingerprint image submissions;
2. Accept and search the images against RISC fingerprint images;
3. Provide rapid responses, to include, but not limited to, Red (Hit), Yellow (Possible Hit), and Green (No Hit) indicators;
4. Disseminate rapid responses in accordance with multi-tiered dissemination rules;
5. Maintain a log of all transactions and disseminations;
6. Designate a point of contact (POC) for issues and concerns related to this initiative; and,

7. At the conclusion of the prototyping phase, delete or destroy all fingerprint images received from DoD as part of this initiative from all databases and logs unless authorized by the DoD to retain them.

B. The DoD will:

1. Capture/receive fingerprint images from DoD approved mobile and/or fixed capture devices;
2. Submit these fingerprint images for a rapid fingerprint search request to the CJIS Division via the CJIS WAN;
3. Accept Red (Hit), Yellow (Possible Hit), Green (No Hit), and other appropriate responses;
4. Disseminate the responses to authorized recipients; and,
5. Designate a POC for issues and concerns related to this initiative.

5. **FUNDING:** There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed in writing. Expenditures will be subject to budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

6. **DISCLOSURE AND USE OF INFORMATION:** The RISC rapid search will be limited to authorized criminal justice agencies for criminal justice purposes. The RISC, and the rapid search thereof, are considered to be a part of the FIRS; therefore, all CJIS rules regarding access to FIRS and use of information apply. During the prototyping phase, the parties are prohibited from relying solely on RISC Rapid Search responses as the impetus for any law enforcement action. Instead, search responses serve as potential links between submitted images and true identities that must be independently verified.

7. **SETTLEMENT OF DISPUTES:** Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

8. **SECURITY:** It is the intent of the parties that the transfer of information described under this MOU will be conducted at the unclassified level. Classified information will neither be provided nor generated under this MOU.

9. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

A. All activities under this MOU will be carried out in accordance to the above-described provisions.

B. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

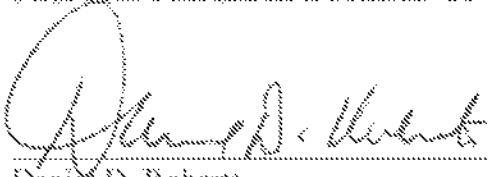
C. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

1. The parties will continue participation, financial or otherwise, up to the effective date of termination.
2. Each party will pay the costs it incurs as a result of termination.
3. All information, copies thereof, and rights therein received under the provisions of this MOU prior to the termination will be maintained in accordance with the receiving party's practices.

10. This MOU, which consists of ten sections, will enter into effect upon the signature of both parties, will be reviewed annually to determine whether amendments are needed, and will remain in effect until terminated or completion of the testing and prototyping phase. By addendum to this MOU, additional law enforcement agencies and organizations may be approved to participate and provide Point of Contact information. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the FBI and the DoD.

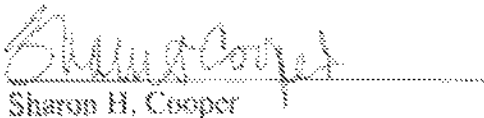
FOR THE FEDERAL BUREAU OF INVESTIGATION



Daniel D. Roberts
Assistant Director
Criminal Justice Information
Services Division

7/2/2010
Date

FOR THE DEPARTMENT OF DEFENSE



Sharon H. Cooper
Director
Defense Human Resource Activity
Office of Under Secretary of Defense
(Personnel Readiness)

Aug 12 2010
Date

**MEMORANDUM OF UNDERSTANDING
BETWEEN
THE FEDERAL BUREAU OF INVESTIGATION
AND
THE DEPARTMENT OF DEFENSE
FOR
SHARING OF BIOMETRIC AND OTHER IDENTITY MANAGEMENT
INFORMATION**

I. PURPOSE

National Security Presidential Directive-59 (NSPD-59) / Homeland Security Presidential Directive-24 (HSPD-24) requires U.S. Government agencies to use "in a more coordinated and efficient manner" biometric information in protecting the nation from "known and suspected terrorists" (KSTs) "and persons who may pose a threat to national security" (national security threats (NSTs)), consistent with applicable law. This Memorandum of Understanding (MOU) is entered into between the Federal Bureau of Investigation (FBI) and the Department of Defense (DoD) to provide for the sharing of unclassified biometric and other identity management information toward this important national security goal. Sharing of classified biometric and other identity management information will be coordinated separately.

II. BACKGROUND

The DoD Biometrics Program leads and coordinates the development, adoption, and institutionalization of biometric techniques for acquiring and retaining biometric and descriptive data recorded by military units. The DoD Biometrics Program maintains biometrics and other identity management data (including biographical data) regarding individuals who are or were in the custody of DoD as a result of military operations overseas, including foreign nationals detained under the law of war, and other biometric data obtained during military operations overseas. This data may also include individuals who may be involved in terrorist activities, serious crime or transnational activities threatening to homeland or national security. It is in the national interest for DoD and the FBI to share this information, so as to ensure prompt and accurate updating of records. Both DoD and the FBI have an affirmative duty to coordinate this information through the sharing of biometric and other identity management data stored in their respective repositories. Although sharing will begin with ten-print fingerprint biometrics and facial photographs, its scope is intended to be broad enough to include other biometric modalities (including palm prints and iris scans) as the technology and interoperability of the databases are enhanced.

The FBI's Criminal Justice Information Services (CJIS) Division serves as the nation's central repository for identification and criminal history record information. The CJIS Division maintains millions of digital representations of fingerprint images, features from digital fingerprint images, and associated criminal history record information in the Fingerprint Identification Record System (FIRS). The FIRS incorporates an automatic fingerprint search capability via its Integrated Automated Fingerprint Identification

System (IAFIS). Given the advances in fingerprint identification technology, including hardware, software and digital imaging, IAFIS capabilities are regularly enhanced to meet the growing needs of law enforcement, national security, and other customers.

III. AUTHORITY

DoD enters into this MOU under the authority of NSPD-59/HSPD-24 and DoD Directive 8521.01F, Department of Defense Biometrics. The FBI enters into this MOU under the authority of Title 28, United States Code (U.S.C.) 533 and 534; 28 Code of Federal Regulations 0.85; and the Attorney General's April 11, 2002, order to coordinate and share information related to terrorism.

IV. SPECIFIC RESPONSIBILITIES

A. The parties jointly agree:

1. To administer their collection and storage strategies to protect the privacy rights of all individuals represented by the data, ensuring the lawful use and proper dissemination of that data.
2. To maintain their respective data bases to ensure the integrity of the data, including maintaining timely, accurate and complete data, consistent with mission needs and operational constraints.
3. To establish procedures to resolve and adjudicate positive matches against such data.
4. To share the other party's data with another agency or foreign government only with the express consent of the party providing the data.
5. To update this MOU, as appropriate, through written addenda signed by authorized representatives.

B. DoD agrees:

1. To share with the FBI DoD-maintained data on individuals gathered during military operations overseas, including data on individuals who are or were in the custody of DoD, in a timely manner when the FBI's mission requires access to such data.
2. DoD's point of contact (POC) is the Director, Defense Research and Engineering (DDRE), who may be reached at

b6 per DOD

C. FBI agrees:

1. To share FBI-maintained data with DoD in a timely manner when DoD's mission requires access to such data.
2. FBI's POC is the CJIS Division, Intelligence, N-DEx and Global Operations Section, CJIS Division Intelligence Group Unit Chief, who may be reached at

b6 per FBI

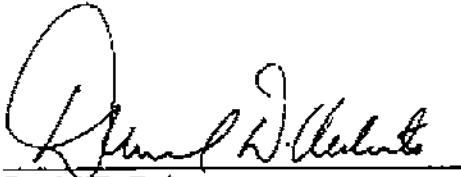
V. FUNDING

There are no reimbursable expenses associated with the sharing of biometric and other identity management data addressed in this MOU. This MOU is not an obligation or commitment of funds or a basis for transfer of funds, but rather it records an agreed to process that will ensure effective sharing of available information and encourage more efficient and effective sharing. Each party shall bear its own costs in relation to the MOU. The parties expressly acknowledge that the existence of the MOU in no way implies that Congress will appropriate funds for such expenditures.

VI. EFFECTIVE DATE, MODIFICATION, AND TERMINATION

This MOU and any subsequent addenda will enter into effect upon the signature of both parties and will be reviewed annually to determine whether amendments are needed. This MOU may be terminated at any time upon written notice to the other party. The party desiring to withdraw from this MOU will endeavor to provide such written notification to the other party at least thirty days prior to withdrawal. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

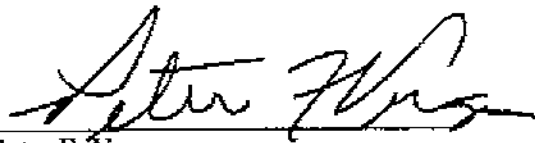
FOR THE FEDERAL BUREAU OF INVESTIGATION



Daniel D. Roberts
Assistant Director
Criminal Justice Information
Services Division

8/27/09
Date

FOR THE DEPARTMENT OF DEFENSE



Peter F. Verga
Deputy Under Secretary of Defense
Policy Integration & Chief of Staff

7/16/09
Date