MEMORANDUM OF UNDERSTANDING (MOU) BETWEEN THE FEDERAL BUREAU OF INVESTIGATION (FBI) AND THE TEXAS DEPARTMENT OF PUBLIC SAFETY (TX DPS) FOR PARTICIPATION IN THE NEXT GENERATION IDENTIFICATION (NGI) IRIS PILOT (IP)

1. PURPOSE

a. The purpose of this Memorandum of Understanding (MOU) is to document the agreed responsibilities and functions of the parties for the limited purpose of testing and evaluating the Federal Bureau of Investigation's (FBI) Iris Pilot (IP).

b. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise among or against any of the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

2. PARTIES

a. This MOU is entered into by the FBI and the Texas Department of Public Safety (TX DPS) (hereinafter, "the parties").

b. The Assistant Director, Criminal Justice Information Services (CJIS) Division, FBI, is responsible for administering this MOU for the FBI, and has designated the Section Chief of the NGI Program Office (NGIPO) as the FBI's point of contact (POC) for this purpose. The Assistant Director, Law Enforcement Support Division, Texas Department of Public Safety is responsible for administering this MOU for the TX DPS, and has designated the Deputy Assistant Director for the Crime Records Service, Law Enforcement Support Division as the TX DPS's POC for this purpose.

3. AUTHORITIES

The FBI enters into this MOU pursuant to 28 U.S.C. § 534, 42 U.S.C. § 3771 (a)(2), and 28 C.F.R. § 20.31. The TX DPS enters into this MOU pursuant to Texas Government Code, Chapter 411, including but not limited to Section 411.042.

4. BACKGROUND INFORMATION

The FBI operates a family of automated systems that support the capability to provide identification, verification, information, investigation, notification, and data management services to its users. One of those systems, the Integrated Automated Fingerprint Identification System (IAFIS) was implemented in July 1999 and houses the world's largest collection of digital fingerprint images, features from digital fingerprint images, and criminal history information. Collectively, this data comprises the

biometrics, content, format, and units of measurement for the electronic exchange of information that may be used in the fingerprint identification of a subject.

The current IAFIS allows the exchange of fingerprint identification data across jurisdictional lines and between dissimilar systems. However, with technological advances in automated fingerprint identification equipment (e.g. hardware, software, and digital imaging) and in order to remain responsive to law enforcement and other customer needs, it became essential to enhance the IAFIS. NGI will provide these enhancements to IAFIS as IAFIS becomes NGI.

One of the objectives of NGI is to enhance IAFIS capabilities to reduce terrorist and criminal activity by improving and expanding biometric services to its users. The IP is an NGI initiative that facilitates the improvement and expansion of biometric services.

In 2009, the FBI's IAFIS was enhanced to accept iris images for storage purposes when submitted with criminal ten-print submissions. Today, the FBI CJIS Division possesses over 30,000 iris images that are not available for searching.

To address and enhance iris processing capabilities, the FBI is initiating the IP as a collaborative effort to identify user needs, demonstrate proof of concept, establish thresholds for lights out (no human intervention) searches at the national level, and refine a useful investigative and identification tool for the law enforcement community. The IP will allow for the evaluation of iris capture and recognition technology in an operational setting while addressing some of the key challenges associated with the technology's use for a large-scale law enforcement application.

The IP will: 1) provide an iris image search capability; 2) permit the bulk submission of iris images maintained in local, state, and federal repositories, resulting in a more robust iris repository; 3) define transactions in the FBI's Electronic Biometric Transmission Specification (EBTS) to support iris searches and submissions; and 4) establish minimum device specifications and best practices.

During the IP, relevant transactions will be analyzed by the parties to assess system performance. In addition, lessons learned and user input will be considered.

TX DPS will utilize the system for investigation and identification purposes. In support of this initiative, the participating agency will submit iris images for a search to the TX DPS. The TX DPS will forward iris submissions to the CJIS Division, via the CJIS Wide Area Network (WAN) or other FBI approved secure connection, for comparison against the FBI's IP repository. This pilot is designed to provide participating law enforcement agencies with an automated iris recognition search of the iris pilot repository, which will be expanded and updated periodically throughout the pilot.

CJIS Division responses to iris image matches under this initiative will include, but not be limited to, the master name and a numeric identifier.

System availability will be limited during this initiative. Accordingly, the CJIS Division will provide advanced notice of sporadic system availability, backup recovery limitations, and shortfalls during the pilot. In addition, the CJIS Division may limit the number of transactions that will be accepted during the pilot.

The IP is scheduled to be operational from September 2013 to September 2014. At its conclusion, the IP will be reevaluated.

5. **SPECIFIC RESPONSIBILITIES**

This MOU applies to iris images provided by the TX DPS and the FBI's responses thereto. Iris search responses will be provided to limited authorized agencies. All DOJ regulations and policies, including, but not limited to the CJIS Security Policy, apply to the access to, dissemination of, and use of FBI-provided information.

It is the intent of the parties that the exchange of information set forth in this MOU will be conducted at the unclassified level. Classified information will neither be provided nor generated under this MOU.

Specifically, the FBI will:

a. Accept up to two iris images per IP search request;

b. Search iris image(s) against the IP repository;

c. Provide a rapid response to include, but not be limited to, the master name and a numeric identifier;

d. Maintain a log of all transactions and disseminations;

e. Designate a POC for issues and concerns related to this initiative; and

f. Conduct post-analysis on submitted transactions relative to system performance and provide the results of such analysis to the submitting agency.

The TX DPS will:

a. Submit no more than two iris images (EBTS - ANSI compliant) per IP search request via the CJIS WAN or other FBI approved secure connection;

b. Accept iris image search responses;

c. Disseminate FBI responses to limited authorized criminal justice agencies; and

d. Designate a POC for issues and concerns related to this initiative.

Both parties agree:

a. The information involved in this MOU may identify United States persons, whose information is protected by the Privacy Act of 1974 and/or Executive Order 12,333 (or any successor executive order). The FBI will ensure that all such information is handled lawfully pursuant to the provisions thereof. In addition, the TX DPS will comply with its state privacy laws.

b. The information derived from the FBI IP search requests and responses shall only be used as investigative leads and shall not be considered as positive identifications. The parties are prohibited from relying solely on IP search responses as the sole impetus for law enforcement action. Other indicators and factors must be considered by the submitting agency prior to taking action.

c. The parties will review and make appropriate changes, if any, to their privacy compliance documents, to reflect the implementation of this MOU so as to ensure privacy risks are appropriately mitigated.

d. Each party that discloses and/or uses PII, pursuant to this MOU, will make reasonable efforts to ensure that the information disclosed and/or used is accurate, relevant, timely, and complete.

e. In the event that either party 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.

f. 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).

g. 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.

6. **EFFECT OF THIS MOU**

a. This MOU is not an obligation or commitment of funds, nor a basis for the transfer of funds, but rather is a basic statement of the understanding between the parties of the matters described herein. 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.
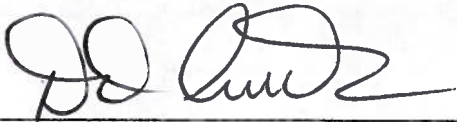
b.   This MOU does not constitute an agreement for either party to assume or waive any liability or claim under any applicable law.

c.   This MOU is not intended to be enforceable in any court or administrative forum. The parties will seek to resolve any disputes regarding this MOU by mutual consultation.

7.   **EFFECTIVE DATE, ADMINISTRATION, AND TERMINATION**

a.   This MOU, consisting of seven (7) sections, shall become effective when executed by both parties and will continue in effect until terminated. This MOU may be modified at any time by written consent of both parties.

b.   This MOU may be terminated, with respect to either party, at any time, upon written notice of termination to the other party. The party desiring to terminate this MOU will provide such written notification to the other party at least thirty (30) days prior to termination. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action.

c.   The parties intend to review this MOU annually to ensure all provisions are meaningful and current.

The preceding seven (7) sections represent the understandings reached between the FBI and the TX DPS.

FOR THE FEDERAL BUREAU OF INVESTIGATION

David Cuthbertson   10/24/13
Assistant Director   Date
Criminal Justice Information Services Division

FOR THE TEXAS DEPARTMENT OF PUBLIC SAFETY

Skylor Hearn   10-3-13
Assistant Director   Date
Law Enforcement Support Division