UNEXECUTED

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

THE MARYLAND DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL SERVICES INFORMATION TECHNOLOGY AND COMMUNICATIONS DIVISION

FOR THE

BULK SUBMISSION OF PHOTOS TO THE FEDERAL BUREAU OF INVESTIGATION FOR INCLUSION IN THE INTERSTATE PHOTO SYSTEM FACIAL RECOGINITION PILOT REPOSITORY

GENERAL PROVISIONS

1. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, and the Maryland (MD) Department of Public Safety and Correctional Services Information Technology and Communication Division (DPSCS-ITD), hereinafter referred to as the "Parties," is for the limited purpose of enabling the bulk submission of photos to the Next Generation Identification (NGI) Interstate Photo System Facial Recognition Pilot (IPSFRP) Repository. This MOU memorializes the Parties' understanding regarding submission requirements for photos to be submitted to the CJIS Division's NGI IPSFRP Repository by way of bulk photo submission.

2. BACKGROUND: The FBI has a family of automated systems that support its 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), implemented in July 1999, houses the largest collection of digital representations of fingerprint images, features from the digital fingerprint images, and criminal history information in the world. 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 for the exchange of fingerprint identification data effectively across jurisdictional lines and between dissimilar systems. However, given technological advances in automated fingerprint identification equipment, including hardware, software, and digital imaging, and to remain responsive to law enforcement and other customer needs, it is essential that enhancements be made to the IAFIS. One of the objectives of the NGI Program will be to incrementally replace the current IAFIS capabilities to reduce terrorist and criminal activity by improving and expanding biometric services to its users. IPS enhancements are one of the NGI initiatives which facilitate the improvement and expansion of biometric services.

The goal of the NGI IPS enhancement initiative is to expand the national photo repository, provide easier access to the photos by CJIS Division customers, and enhance the IAFIS photo capabilities. Core changes to be implemented in support of this goal include: 1) Permitting submission of photos independent of an arrest submission with fewer than ten fingerprints and a FBI Number (FNU) or Universal Control Number (UCN) while continuing to allow legacy capabilities of photo submissions with arrests; 2) ***Permitting Bulk Submission of Photos***; 3) Permitting submission of non-facial photos that are compliant with Electronic Biometric Transmission Specification (EBTS) such as Scars, Marks, and Tattoos (SMTs); 4) Permitting search of SMT photos by SMT descriptors; 5) Permitting investigative search of photos using biographical criteria; 6) Permitting IPS photo retrieval via the National Crime Information Center (NCIC); 7) Permitting submission of photos with Civil Type of Transactions (TOT); 8) Eliminating restriction of ten photo sets per FBI record; and 9) Providing an automated facial recognition search capability for investigative purposes. These enhanced photo services will increase the number of photos in the national repository, increase NGI photo capabilities, and allow easier access to photos by CJIS Division customers.

With respect to the bulk submission of photos, several state agencies have contacted the CJIS Division requesting the immediate ability to submit photos maintained in their state repositories to NGI. Currently, IAFIS only allows authorized agencies to submit photos with a corresponding tenprint fingerprint card submission. This limitation prevents the IAFIS from accepting bulk submissions of photos. Upon implementation, the NGI IPS Bulk Photo Submission enhancement will allow local, state, tribal and federal database owners to submit photos to the national repository in a more efficient manner. In the interim, enabling the bulk submission of photos into the IPSFRP Repository will ultimately increase the number of photos in the NGI IPS and create the ability to search a significantly expanded national photo database.

3. AUTHORITY: The FBI enters into this MOU pursuant to Title 28, United States Code (U.S.C.), Section 534 and 28, Code of Federal Regulation, § 20.31. The MD DPSCS-ITCD enters into this MOU pursuant to Criminal Procedure Article, §§213-220, Annotated Code of Maryland and Code of Maryland Regulations (COMAR) 12.15.01.

4. SCOPE: This MOU applies to the MD DPSCS-ITCD bulk submission of photos meeting submission criteria to the FBI's IPSFRP Repository.

A. The FBI will:

1. Accept encrypted (FIPS 140-2 Compliant) criminal mug shot photo enrollment requests in bulk via multiple mechanisms (CD, DVD, HDD, Secure File Transfer) mutually agreed to by the Parties;

2. Support encrypted removable media for the bulk import of encrypted criminal mug shot photos;

3. Enable an Authorized FBI System Administrator to load machine readable data media for the input of encrypted criminal mug shot photo enrollment requests into the NGI IPSFRP Repository;

4. Provide a collective response as to enrollment or rejection for encrypted criminal mug shot photo enrollment requests when submitted in bulk;

5. Transfer the bulk encrypted criminal mug shot photos submitted to the IPSFRP Repository in accordance with this MOU to the Interstate Photo System National Repository; and

6. Designate a point of contact (POC) for issues and concerns related to the bulk submission of criminal mug shot photos to the NGI IPSFRP Repository.

B. The MD DPSCS-ITCD will:

1. Verify that all encrypted criminal mug shot photos match the FNU and arrest cycle prior to submission to the CJIS Division via this initiative;

2. Verify that each encrypted criminal mug shot photo submitted is accompanied with the correct FNU and date of arrest;

3. Verify that all mandatory Type 2 and Type 10 field information is provided to the CJIS Division with each encrypted criminal mug shot photo submitted;

4. Submit encrypted (FIPS 140-2 Compliant) criminal mug shot photos for enrollment into the NGI IPS via a mutually agreed upon accepted mechanism (CD, DVD, HDD, Secure File Transfer); and

5. Designate a POC for issues and concerns related to the bulk submission of criminal mug shot photos to the NGI IPSFRP Repository.

5. FUNDING: There are no reimbursable expenses associated with this MOU. Each Party will fund its own activities unless otherwise agreed to in writing. Expenditures will be subject to budgetary processes and availability of funds and resources 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.

6. DISCLOSURE AND USE OF INFORMATION: The opportunity to submit criminal mug shot photos in bulk to the IPSFRP Repository will be offered to authorized agencies. The IPSFRP and the associated Repository are considered to be a part of the Fingerprint Identification Records System (FIRS); therefore all CJIS rules regarding access to, and dissemination/use of, FBI provided information will apply. The Parties acknowledge that information involved in this initiative may identify United States persons whose information is protected by the Privacy Act of 1974, Executive Order 12333, any successor executive order, or other federal authority. Accordingly, all such information will be treated as "law enforcement sensitive" and protected from unauthorized disclosure. Each Party will immediately report to the other Party any instance in which data received from the other Party is used, disclosed, or accessed in an unauthorized manner (including any data losses or breaches).

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 and TERMINATION:

A. All activities under this MOU will be carried out in accordance to the aforementioned provisions, conform to privacy protections provided at 5 U.S.C. § 552a, and incorporate security protections listed in the most current version of the CJIS Security Policy.

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

C. Either Party may terminate this MOU upon thirty (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. ENTRY INTO FORCE, AND DURATION: This MOU, which consists of ten (10) 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. 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 preceding ten (10) sections represent the understandings reached between the FBI and the MD DPSCS-ITCD.

FOR THE FEDERAL BUREAU OF INVESTIGATION

David Cuthbertson
Assistant Director
Criminal Justice Information Services Division

7/5/12
Date

FOR THE MARYLAND DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL SERVICES INFORMATION TECHNOLOGY AND COMMUNICATIONS DIVISION

Ronald C. Brothers
Chief Information Officer
Maryland Department of Public Safety and
Correctional Services

Date

Approved for form and legal sufficiency:

Stuart Nathan
Principal Counsel
Maryland Department of Public Safety and
Correctional Services

Date