



ARIZONA

COUNTER-TERRORISM INFORMATION CENTER FACIAL RECOGNITION



The Maricopa County Sheriff's Office and the Arizona Counter Terrorism Information Center would like to take this opportunity to introduce you to the Center's latest investigative technology: Facial Recognition.

The Facial Recognition Unit of the Maricopa County Sheriffs Office (MCSO) is assigned to the Arizona Counter Terrorism Information Center (ACTIC) and follows the ACTIC policy on the submission and dissemination of law enforcement investigative information. The primary function of the Facial Recognition Unit is to provide a potential lead for the identification of suspects in any suspected criminal activity. Use of Facial Recognition as an investigative tool will fall under the same guidelines (A.R.S. § 41-1750 et al. and CFR 28 part 23) as all of its intelligence databases, and is designed to be used in conjunction with, and as a supplement to traditional investigative procedures. In order to utilize Facial Recognition, law enforcement officers / agencies must provide information demonstrating an active law enforcement investigation is ongoing. Facial Recognition research requests can only be submitted in conjunction with an official law enforcement investigation. A case / department / intelligence report number, criminal code number and crime designation (e.g. - Homicide, ID Theft, Armed Robbery, etc.) ***are required*** with every request for facial recognition submission.

The MCSO - ACTIC Facial Recognition Unit can process a facial image into the FR database and have the image compared to millions of driver's license and mugshot images and have results in ***seconds***.

The requirement to complete a submission is a request form and a still frontal face image (the image can be from a variety of sources including police artist renderings). The image is then compared against the facial recognition database. We are taking the labor intensive work out of identifying suspects, missing persons, identity theft, unidentified deceased persons and persons of interest. By using this technology, we can help you solve more crimes, expedite and make more arrest(s) on your cases and protect citizens and our communities. Please feel free to contact us.

Submit Facial Recognition requests to: ACTICFR@azdps.gov

Pat Bristow, Intelligence Analyst Supervisor, Facial Recognition Unit Supervisor
Office = 602.644.5916 Cell = 602.616.1714 Email = pbristow@azdps.gov

Off. Sally Estrada, Facial Recognition Unit
Office = 602.644.5914 Pager = 602.202.3280 Email = sestrada@azdps.gov

Off. Bryan Inawat, Facial Recognition Unit
Office = 602.644.5913 Pager = 602.302.0721 Email = binawat@azdps.gov

***Homeland Security
&
The National Facial Recognition Network
Briefing Paper
October 06, 2008***

***Maricopa County Sheriff's Office
Joe Arpaio - Sheriff***



"VICTORY THROUGH COOPERATION"

Norm Beasley & Ray Churay

Maricopa County Sheriff's Office

Executive Summary

The Maricopa County Sheriff's Office under the direction of Sheriff Joe Arpaio implemented a facial recognition unit within the agency and has assigned it to the Arizona Counter Terrorist Information Center to assist in counter terrorist and criminal investigations.

This proposal recommends the establishment of the **National Facial Recognition Network**. This program has the potential to be a key component in the Nations Homeland Security effort. The NFRN would link existing and proposed local fusion centers, USDHS, FBI and other Federal support centers thereby providing direct support to ongoing criminal and national security investigations at the federal, state and local level.

Overview

The MCSO Facial Recognition Unit is an active component of the Arizona Counter Terrorist Information Center providing direct investigative support to ACTIC participating agencies, Arizona and out of state local, state and Federal law enforcement agencies

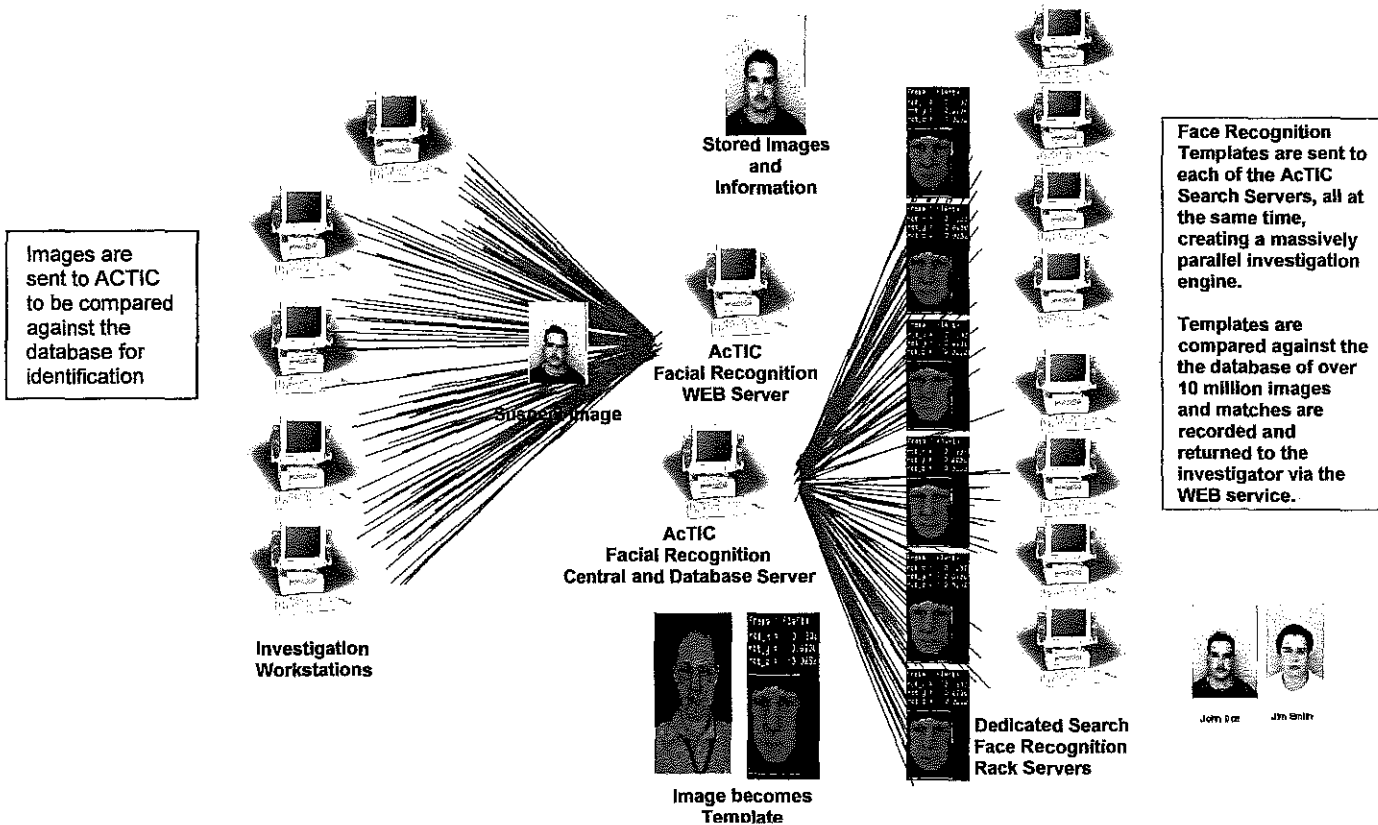
The Arizona Counter Terrorist Information is the state's single fusion center. It operates under an all crimes concept. Two hundred and forty state, local and federal investigators, analysts and support personnel from forty-three different agencies are assigned to the center. This includes the Federal Bureau of Investigation Joint Terrorist Task Force and the Field Intelligence Group. Investigators conduct both criminal and intelligence investigations.

The Program has significant potential in supporting on going criminal and national security related investigations, prevention and pre-event preparedness operations. It can be used effectively in suspect identifications using photographs, surveillance still and video, suspect sketches and even forensic busts by comparing unknown persons involved or suspected to be involved in criminal or terrorist activity with known program data bases. It can be field deployable for special events and on-site identifications. Further uses include identity fraud, sexual predators and missing and abducted children to name only a few.



The programs current database consists of approximately 14.5 million Arizona Driver License Photos; 3.2 million Arizona County and City Jail Booking photographs; 12,000 convicted sex offender images; and 1,700 violent felony warrant photographs. MCSO has partnered with USDOJ to gain access to the Federal Joint Automated Booking System (JABS) which contains another 1.5 million photographs of persons booked by federal agencies nationwide. The ACTIC facial recognition unit is capable of comparing a single image to the entire 19.2 million photo database in 15 seconds or less. Participation by the Nations State and Local Fusion Centers would significantly expand the capabilities of the program.

AcTIC Image Investigation System (IIS)



National Facial Recognition Network Vision

The National Facial Recognition Network would be a partnership with law enforcement and other criminal justice agencies nationwide, linking state and local fusion centers, USDHS, FBI & the National Terrorist Screening Center. It would provide a vehicle for a national search capability for wanted suspects and known or suspected terrorists with the State and Local Fusion Centers acting as the central point of contact within their jurisdictions.

These State and Local Fusion Centers would provide their states criminal arrest images for inclusion to the program. The Maricopa County Sheriff's Office Facial Recognition Unit would then provide facial recognition investigative support services to these centers on active criminal or intelligence cases.

As noted above, the ACTIC has included the Arizona Driver Licenses in the ACTIC data base, but is only asking for other state's booking photographs. It is believed that most state laws or administrative practices with regard to driver license photographs would prohibit transmission of that data base to another state.

Therefore, depending upon local administrative practices or laws, and the resources available at other fusion centers, a consideration should be given to the creation of a facial recognition unit that has the ability to access, copy, and store, and search that state's driver licenses for inclusion into the NFRN.

The NFRN Initiative will be a vital tool to the federal, state, and local law enforcement agencies that are responsible for keeping our communities and nation safe. It would allow law enforcement agencies to rapidly and easily share information thereby enabling officers to make swift threat assessments and expedite apprehension of known/suspected terrorists and other wanted criminals

The NFRN supports existing National initiatives including; National Criminal Intelligence Sharing Plan; Global Justice Information Sharing Initiative; and Global Fusion Center Guidelines. It is designed to conform to 28CFR Part 23 and all privacy, civil rights and civil liberties protection requirements using the recently released USDOJ Privacy, Civil Rights and Civil Liberties Policy Templates for Justice Information Systems.

National Facial Recognition Network Connectivity

The Regional Information Sharing Systems (RISS) has approved the use of their system to connect agencies. The Regional Information Sharing System (RISS) consists of six regional centers that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are drug trafficking, terrorism, violent crime, cyber-crime, gang activity, and organized criminal activities. Each of the centers selects its own target crimes and the range of services provided to member agencies.

The Arizona based RISS project, Rocky Mountain Information Network will take lead in coordination. The RMIN geographical region includes Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming and has member agencies in Canada. All RMIN member agencies have agreed to participate in FRN. A total of 270 law enforcement and criminal justice agencies nationwide have agreed to participate in the National Facial Recognition Network when established.

For further information contact:

Ray Churay
Deputy Chief, Intelligence Division
602-876-3268
r_churay@MCSO.maricopa.gov

Norm Beasley

Counter Terrorism Coordinator, Intelligence Division
602-390-8314
n_beasley@MCSO.maricopa.gov

KEENER



The facial recognition MANUAL

This manual is not to leave the ACTIC facility.

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

1. Retrieve request form and image(s) from ACTICFR inbox and place them into their case folder.
 - a. Fill in the area labeled "Facial Recognition Unit Use Only" with the following information: number of images, quality of images, date and time received and FR staff assigned.
 - i. Print the request form and the images into a contact sheet (directions are given in Appendix 1).
 - b. Folders will be assigned for each year, month, agency and case
 - c. Case folders are to be labeled as the follows: Case Number_Date Received
 - i. Example: 2008-123456_120308
 - ii. The case number will be found on the request form. This is a mandatory requirement. Do not begin to work on a case without a case number and criminal code.
 - d. Submitted images are to be place in a folder labeled "Submitted."
2. Each case must be entered into the Facial Recognition Case Log in order to obtain its assigned Case Tracking number (CT #).
 - a. Location of log: S:\Facial Recognition\FR Image Case & File Archives\FR Case Log
 - b. Enter data into the following fields:
 - i. CT # – CT # is sequential and needs to be labeled accordingly
 1. Write the number in the gray box on the top right corner of the FR Request Form
 - ii. Date Rec'd – date case was received; not the day you worked on the case
 - iii. Agency – agency that submitted the request
 1. If the individual is assigned to the ACTIC, obtain their assigned squad instead of their home agency
 - iv. Case # – case number
 - v. Request P/R – there are two types of requests
 1. Proactive (P) – request was initiated by the Facial Recognition Unit
 2. Request (R) – request was initiated by another agency or unit
 - vi. Assigned to – operator assigned to the case
 - vii. Case Status – there are three statuses

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

1. In Progress – the operator is currently working the case
 2. Pending – the operator is awaiting additionally information for the submitting party
-
3. Completed – the case is completed with the date noted
3. After entering the request into the log, the request must be entered into FR Case Tracking.
 - a. Sign into FR Case Tracking and select “Create New Case”
 - i. Enter data into the following fields (example in Appendix 2):
 1. 28CFR Case Dates
 - a. Open Date – date case was received; not the day you worked on the case
 - b. Purge Date – this is the date five years from the date submitted
 2. Case Info
 - a. Agency Case # – agency case number
 - b. Actic Case # – CT #
 - c. Agency – agency that submitted the request
 - i. Do not use spaces. Examples:
 1. MaricopaCSO
 2. PeoriaPD
 3. USMarshals
 4. USPIS
 - d. ORI# – list the agencies ORI number
 - e. # of Photos – indicate the number of usable photos submitted
 - i. Formatting is as follows: 00001 and 00012. Notice the ✖ number is to be five digits long.
 - f. Charge Code – enter the Arizona Revised Statue (ARS) or the United States Criminal Code (USC)
 - i. Formatting is as follows:
 1. ARS – 13-1105
 2. USC – 18USC1073
 - g. Crime Designation – enter just the description of the charge code

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

i. Example

1. ARS – 13-1105 – Homicide
 2. USC – 18USC1073 – Homicide
-

h. Charge Description – leave blank

i. Add a comment – there are a variety of comments that can be added here

i. If you are doing a proactive case indicate it there by simply stating: Proactive.

ii. If the submitting agency is requesting research for another agency note that in the comment box

3. Requester Info

a. Name – just use the last name of the individual

b. Serial – enter the serial number of the individual

c. Agency – agency that submitted the request. Formatting is same as in Case Info.

d. Phone # – enter the contact information for the individual

i. Formatting is as follows:

1. Do not use spaces - (602)644-5914

e. Email – enter the email address for the individual

f. Supervisor Name – just use the last name of the individual

g. Supervisor Phone # – enter the contact information for the individual. Formatting is same as before.

h. Type of Images – there are a few main types of images

i. JPG – Jpeg which is what most pictures are formatted as

ii. BMP

iii. Composite – this a sketch by either an artist or a computer software

iv. All other image types will be converted to JPG

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

- i. Date of Image – if the date of image is provided on the request form enter it here; if not enter the date the request was submitted
 - j. Subject Info – enter subject information as shown on the request form
-
4. Send to Supervisor – select the acting supervisor
 5. Press Save
4. Place the contact sheet along with the request form in the supervisor's inbox on the outside of their door. The supervisor will then look over the case and documentation and either approve or disapprove the case. The supervisor will notify you of the decision.
 - a. If supervisor is not on shift, begin working on the case from here.
 5. Once an approval is received, the operator can then begin working on the case. (APPROVAL)
 6. Open Image Investigation 3.X.
 - a. Make sure all databases are checked
 - b. The starting similarity is .9
 - c. Click "Insert Image" and locate the image you are researching. Then select "Open." The image will then populate into the "Face Image" placeholder.
 - d. Click "Search." The software will then begin to search through each of the servers and generate results. The number of images produced is generated as "Received: 2 / 10." The "2" indicates the number of images displayed and the "10" indicates the total number of results. Once the search is completed both numbers will be the same; the display will read "Displayed X/X." If not notify the supervisor.
 - i. If the total number of results reaches over 500, stop the search immediately by clicking "Stop." The "Search" box will remain grayed out until the software has completely stopped the search. To continue the search, raise the similarity level and click search. Do not close the program as this may cause system issues.
 - ii. If the message "No Face Found" appears, lower the similarity level and click search again. Do this until results are generated. If the message appears at the similarity's lowest level, then the image results are documented as no face found (NFF).

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

- e. Review the results and identify possible leads
 - i. Information regarding the image can be located when the image is selected. It will populate the "Database Image" placeholder and the corresponding information with populate in the "Database Image Information" placeholder.
 1. ACTIC # – a unique number given to all images in the database
 2. Unique ID – currently there are three types of ID
 - a. Driver's License – DL number then the date of image
 - i. Example: A12345678_20080912
 - b. Booking Image – PCN number then the date of image
 - i. Example: 2802077927_20080923
 1. The first two digits of the PCN indicate what agency booked the subject in
 - c. JABS Image – FBI number then the date of image
 - i. Example: FBI-652331WB9_20050920
 3. Date of Birth
 4. Date of Image – date the image was taken
 5. Database From – what server the image is located on
 6. Image – name of the image on the server
 - ii. Results are to be saved in a new folder labeled "Results" and then in a folder labeled after the image searched.
 1. For example, the submitted image is labeled as P123456. Within the Results folder, folder is created and labeled as P123456. All leads identified using P123456 are to be placed in this folder.
 2. To save an image, select the image in the results area, right click and select "Save As." Save the image using the default image name along with the date of birth associated with that image.
 - a. Example: A12345678_20080912_1983-03-21
 - iii. The operator may also choose to use an image result to initiate a search. By selecting the image in the results area, right click and select "Search." The database image will then populate the "Face Image" placeholder and the software will initiate the search automatically.

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

- iv. Print all results on an image contact sheet.
7. Once all searches and research has been completed, the operator is then to write a narrative regarding the search. There are two types of narratives, proactive and request. Both formats can be found in Appendix 3. Print the narrative when complete.
8. Fill in the remaining area of the "Facial Recognition Unit Use Only" grayed box with the following information: results supplied to the requestor – MVD, MUG, JABS, NR, and/or NFF.
9. Package the request form, submitted contact sheet and results contact sheet along with the narrative. Place the package in the supervisor's inbox on the outside of their door. The supervisor will then look over the case and documentation and either approve or disapprove the case for dissemination. The supervisor will notify you of the decision.
 - a. If supervisor is not on shift, continue with dissemination process.
10. Dissemination process:
 - a. No results/no face found/no additional information -- these results can be given over ACTIC email. Do not include any identifying information other than the case number.
 - b. Results – there are three ways to do disseminate results
 - i. Via phone – contact the requestor and provide them with the results.
 - ii. Via email – due to 28CFR and policy, results can only be sent via encrypted email. FR uses only FBI-LEO and RMIN/RISS. The requestor must have one of these accounts in order to obtain their results this way.
 - iii. In person – the requestor may pick up the results from the operator.
 - c. The method of dissemination is then recorded on the request form.
 - i. If the requestor picks up the results or sends some one to do so they must sign the request form.
11. After the case is complete, scan the package into PDF format and save it in the case folder.
12. Copy the case folder into FR Case Tracking File Store under its assigned case tracking number.
13. Sign into FR Case Tracking and select the case you are working on.
 - a. Click "Upload" – there is no need to actually upload a document
 - b. Under the "Publish To" drop down, select the assigned supervisor.

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

c. In the comment field, insert "OK" and click "Send To"

14. Open Facial Recognition Case Log and update the progress of your case to complete.

15. Stats:

a. At the end of the shift each operator is to record the number of cases as follows:

i. Cases Submitted

ii. Number of Images Submitted – only record those images that are usable

iii. Cases Completed

iv. Results

1. No Face Found

2. MUG

3. MVD

4. JABS

5. No results – search produced no additional images

v. Pending

vi. Comments

b. Stat sheets are then forwarded weekly to FR supervisor

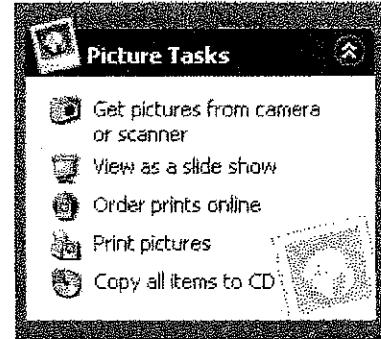
MCSO/ACTIC Facial Recognition Procedures

Image Records Request

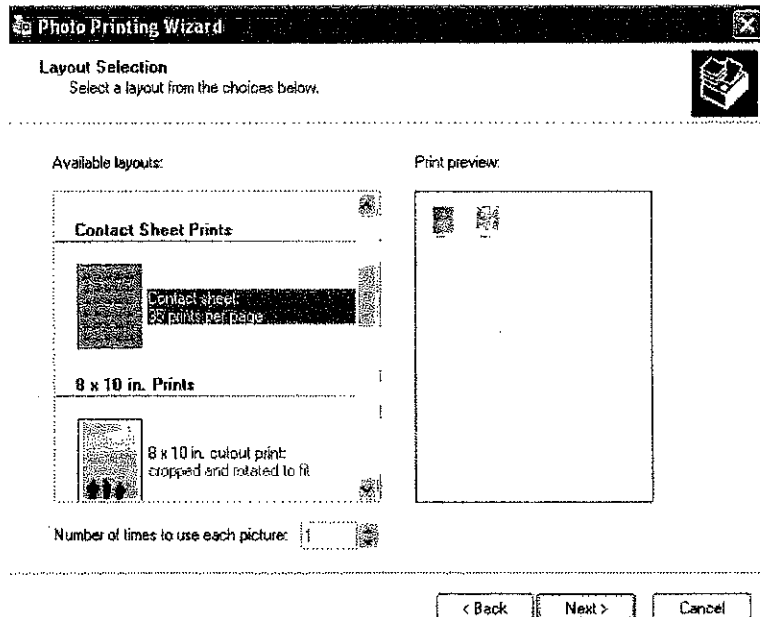
Appendix 1

How to Print a Contact Sheet

1. Open the folder the images are contained in.
2. Click on "Print Pictures." *ACUTE PDF*
 - a. If this task panel does not appear, select the first image, right click, scroll down to "Open With" and select the "Windows Picture and Fax Viewer." This will open a viewer; at the bottom there will be a print icon, click on it.



3. A welcome screen will appear. Click "Next."
4. The "Picture Selection" screen appears and displays all images in the folder. You can select the images you want to print or select all. Click "Next."
5. On the Printing Options screen select the correct printer. Click "Next."
6. On the Layout Selection screen, choose the third option which is the Contact Sheet. Click "Next."
7. This will automatically start the printing process.
8. Select "Finished" and you're done.



Create New Case

28CFR Case Open Date

12/3/08

28CFR Case Purge Date

12/3/13

Case Info

Agency Case#: 2008-123456

Actic Case #: 2008-868

Agency: MaricopaCSO

ORI#: AZ0070000

of Photos: 00001

Charge Code: 13-1802

Crime Designation: Theft

Charge Description:

Add a comment:

Requester Info

Name: Estrada

Serial: A9823

Agency: MaricopaCSO

Phone #: (602)644-5914

Email: sestrada@azdps.gov

Supervisor Name: Bristow

Supervisor Phone #: (602)644-5916

Type Of Images: JPG

Date Of Image: 12/03/13

Subject Info: Jerry Allen White DOB 12/5/08

Send To Supervisor: PLB

Save

Creating a New Case

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

Appendix 2

Page 9 of 11

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

Appendix 3

Proactive

Maricopa County Sheriff's Office/ACTIC

Facial Recognition Unit

Narrative

REPORTING OFFICER / SPECIAL # Estrada A9823	LOG# 11.19.08	CASE #/NO. ACTICFR 08-0018065
---	-------------------------	---

On 11.19.08, Patrick Bristow, FRU Supervisor, provided me with a EVGCI Fusion Center Biweekly #30 that highlighted various fugitives. I performed a Criminal Search Inquiry through JWI on Marie Jackson (12/11/87) and Thomas Jackson (10/11/63). From the bulletin, I obtained two images, Marie Jackson and Thomas Jackson.

I submitted image Marie Jackson into FR and produced seven results.

From the results of Marie Jackson, I submitted image D03176327_20080702_1987-12-11 into FR and produced five results.

I submitted image Thomas Jackson into FR and produced two results.

From the results of Thomas Jackson, I submitted image B10806837_20080801_1963-10-11 into FR and produced two results.

No further information on the subject. No further action.

Submitted Image	Image Results		
	MUGS	JABS	MVD
Marie Jackson	2112075888_20080806_1987-12-11 2801088328_20070514_1987-12-11 2801100545_20080806_1987-12-11 2802063986_20061230_1987-12-11 2802065381_20070323_1987-12-11 2802073361_20080319_1987-12-11		D03176327_20080702_1987-12-11
Thomas Jackson	2803041506_20071113_1963-10-11		B10806837_20080801_1963-10-11
D03176327_20080702_1987-12-11	2112075888_20080806_1987-12-11 2801100545_20080806_1987-12-11 2802073361_20080319_1987-12-11		D03176327_20070306_1987-12-11 D03176327_20080702_1987-12-11
B10806837_20080801_1963-10-11	2803041506_20071113_1963-10-11		B10806837_20080801_1963-10-11

MCSO/ACTIC Facial Recognition Procedures

Image Records Request

Request

Maricopa County Sheriff's Office/ACTIC
Facial Recognition Unit
Narrative

<small>REPORTING OFFICER / SERIAL #</small> Estrada A9823	<small>DATE</small> 11.03.08	<small>CRIME #/CD</small> ACTIC Squad 2 2008-1315
---	--	---

On 11.03.08, Det. P. Walton #9908, ACTIC Squad 2, submitted an FR request with five images labeled as 526917907_NoDate, D01748305_20010919, D01748305_20080908, D01748305_20011106 and D01748305_20030218.

I submitted image 526917907_NoDate into FR and produced two results.

I submitted image D01748305_20010919 into FR and produced three results.

I submitted image D01748305_20080908 into FR and produced four results.

I notified Det. P. Walton in person of the FR disposition.

No further action.

Submitted Image	Image Results		
	MUGS	JABS	MVD
526917907_NoDate			526917907_19980101_1970-11-20 D01748305_20010919_1970-10-17
D01748305_20010919			D01748305_20010919_1970-10-17 D01748305_20011106_1970-10-17 D01748305_20031020_1970-10-17
D01748305_20080908			D01748305_20010919_1970-10-17 D01748305_20011106_1970-10-17 D01748305_20031020_1970-10-17 D01748305_20080908_1970-10-17

**MEMORANDUM OF UNDERSTANDING
BETWEEN THE JOINT AUTOMATED BOOKING SYSTEM PROGRAM MANAGEMENT OFFICE,
MARICOPA COUNTY SHERIFF'S OFFICE AND THE ARIZONA COUNTER TERRORISM
INFORMATION CENTER**

PREAMBLE

This Memorandum of Understanding (MOU) is entered into by the Joint Automated Booking System (JABS) Program Management Office (PMO) of the Department of Justice, the Maricopa County Sheriffs Office (MCSO), and the Arizona Department of Public Safety's Arizona Counter Terrorism Information Center (DPS ACTIC). This MOU outlines a cooperative effort by JABS to share law enforcement information with DPS ACTIC. JABS will support DPS ACTIC through timely and accurate information sharing. This MOU reaffirms the Department of Justice's (Department) continued commitment to the exchange of law enforcement information between the Department and state and local agencies.

This MOU outlines which parties have access to JABS information, how this information can be used by its recipients, and what measures must be taken to ensure compliance with all applicable privacy laws and the Department security requirements.

ARTICLE 1: INTRODUCTION

A. PARTICIPATING PARTIES

The participating parties to this MOU are JABS, MCSO and DPS ACTIC. This MOU anticipates that other organizations will become participating parties as described in ARTICLE 2, SECTION D.

B. BACKGROUND

JABS is an important Department information sharing project among its law enforcement components: Bureau of Prisons (BOP), Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), U.S. Marshals Service (USMS), and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). Additionally, the customs and border security functions within the Border and Transportation Security (BTS) Directorate of the Department of Homeland Security (DHS) are primary users of JABS. JABS provides the Department's "front end" to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) by providing an automated process for the collection and transmission of fingerprint, photographic, and biographical data. The mission of the JABS information sharing system is to (1) automate the booking process, (2) enable each agency to share and exchange booking information, (3) establish a federal offender tracking capability, and a recently identified new mission goal of (4) information sharing with other law enforcement systems.

The JABS Program directly supports the President's Homeland Security initiative by automating the booking process and providing a secure mechanism to rapidly and positively identify an individual based on a fingerprint submission to IAFIS. The JABS-IAFIS interface has reduced the time to identify an individual from several weeks for a paper fingerprint submission to less than one hour. Additionally, JABS supports an IAFIS query transaction for DHS that reduces the identification processing time to less than 10 minutes. Equally important, the JABS booking submissions provide a "real-time" updating of the FBI's criminal master files that are available to all federal, state, and local law enforcement agencies.

DPS ACTIC is the State of Arizona's central analysis hub for real-time crime and terrorism-related intelligence and information. The mission of DPS ACTIC is to protect the citizens and critical infrastructure of Arizona and to coordinate information sharing among state, local, and tribal law enforcement authorities in order to deter terrorist activities. DPS ACTIC was the first state fusion center to include complete integration of the Federal Bureau of Investigation's Joint Terrorism Task Force.

C. PURPOSE

This MOU establishes and delineates the party's rights and obligations with respect to their participation in JABS or use of JABS data. This MOU is not intended, nor should it be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party to this MOU against the parties, the United States, or the officers, employees, agents, or other associated personnel thereof.

This MOU shall be carried out in accordance with all law, regulations, and guidelines applicable to each party. In the event applicable laws, regulations, or guidelines preclude implementation of any part of this MOU or a project/initiative, the participating parties will restructure this MOU or the project/initiative, if possible, to conform to the applicable law and/or policy.

The purpose of this MOU is to outline and formalize the relationship between the participating parties in order to maximize cooperation and to promote effective government information sharing.

D. SCOPE

This MOU will not affect any pre-existing, independent relationships or obligations between and/or among the participating parties or between the participating parties and any third parties.

E. AUTHORITIES

DPS is authorized and empowered to enter into this MOU pursuant to A.R.S. § 41-1713. The Agency is authorized and empowered pursuant to 28 U.S.C. 533 and 534; Presidential Decision Directives 39 and 62; the Memorandum of the Deputy Attorney General of December 21, 2006, regarding law enforcement information sharing policy and directives; 95 U.S.C. 552a, Privacy Act of 1987; Title 28, CFR, Part 20, Criminal Justice Information Systems.

Now, in consideration of the mutual promises set forth herein, the parties to this Agreement hereby agree to the following terms and conditions:

ARTICLE 2: GOVERNANCE

A. JABS

The JABS Board of Directors maintains oversight authority on all policy matters and component operational requirements pertaining to the JABS Program. The JABS PMO has daily program management responsibility for all activities associated with the development, operations, and maintenance of JABS. Operational authority relevant to the actual transfer of information to DPS ACTIC and or any future participating party has been delegated to the JABS PMO.

B. DPS ACTIC

DPS ACTIC is an entity of the Arizona Department of Public Safety (DPS), and works to coordinate information sharing among state, local, and tribal law enforcement authorities in order to deter terrorist activities.

C. GOVERNING DOCUMENTATION

By entering into this MOU, the participating parties agree to incorporate by reference the JABS End User Rules of Behavior Statement, FBI/CJIS Security Policy, NCIC 2000 Operating Manual, and DPS ACTIC Policy and Procedure document.

D. FUTURE PARTICIPATING PARTIES

This MOU extends to DPS ACTIC and those agencies having signed agreements of participation with the DPS ACTIC. Inclusion of future participants in the DPS ACTIC program will require an amended agreement to be executed. Future participating parties will include but are not limited to law enforcement agencies from New Mexico, Texas, California, and Nevada.

ARTICLE 3: RESPONSIBILITIES

A. POINTS OF CONTACT

The participating parties will designate an information technology point of contact to work directly with support staff at the JABS PMO to ensure the Department's information is shared comprehensively and routinely and that the information shared is responsive to law enforcement needs.

B. ACCOUNTABILITY

The participating parties agree that all audit logs of disseminated JABS information shall be retained and subject at all reasonable times to inspection and audit by the Department.

The MCSO agrees to submit quarterly reports to the Department pertaining to the level of success JABS information has contributed to law enforcement activities.

C. National Information Exchange Model (NIEM) COMPLIANCE

All information exchanges will be specified as Information Exchange Package Descriptions (IEPD) utilizing the current version of NIEM. This exchange specification shall be built by the JABS PMO and DPS ACTIC working together and in consultation with the NIEM National Priority Exchange Panel (NPEP). The JABS PMO, in consultation with the Department's Enterprise Architecture PMO, may adopt an interim temporary

exchange if required to support mission requirements. However, the NIEM-based exchange must be specified and implemented with all deliberate speed.

ARTICLE 4: FUNDING

A. FUNDING

Each participating party to this MOU shall bear its own costs and expenses for the duration of this MOU, including personnel costs. Other expenditures by each party will be subject to each organization's budgetary processes and to the availability of funds and resources pursuant to applicable law, regulations, and policies.

The participating parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditure. The participating parties acknowledge that there is no intimation, promise, or guarantee that funds will be available in future years.

ARTICLE 5: INFORMATION SHARING

A. INFORMATION CONTRIBUTION

The JABS PMO will contribute the information delineated below to DPS ACTIC on an on-going basis, via the method and terms described in this MOU. The information will be contributed for the purpose of producing analytical products, including, but not limited to, investigative leads, target profiles, strategic reports, and field query reports. Information to be shared will include the following data items in XML format:

- Front photo/mug shot
- Date of photo
- Offender's name
- Offender's DOB
- Offender's height
- Offender's weight
- Offender's gender
- Offender's eye and hair color
- Arresting agency
- Arresting ORI
- Arresting agent's name and phone number
- Offender's FBI #

B. TRANSFER OF INFORMATION

The JABS PMO shall provide DPS ACTIC with an initial electronic transfer of JABS information described in ARTICLE 5, SECTION A. JABS information will be transmitted to DPS ACTIC via secured communication methods, including but not limited to Law Enforcement Online (LEO). The PMO will mark this information and provide relevant documentation to include a description of the data layout, description of the data that has been included or excluded, and any other information that will assist in understanding the information contained in the initial data set.

Thereafter, the JABS PMO will arrange for the electronic transfer to DPS ACTIC on an agreed upon schedule and consistent with existing technological capabilities. The transfer will be accomplished via a technical process that ensures secure and appropriate information transfer, of all updates to the initial JABS data set. In addition, the PMO will provide on an annual basis a complete historic information transfer for data synchronization purposes. The assistance provided pursuant to this SECTION B shall be subject, in all cases, to the resource constraints faced by the PMO, and the terms of applicable law to which JABS is subject.

C. USE OF INFORMATION AND REDISSEMINATION

DPS ACTIC will use JABS information it receives from the JABS PMO hereunder solely in support of the DPS ACTIC mission statement and consistent with ARTICLE 1, SECTION B and ARTICLE 5, SECTION E. The PMO understands that DPS ACTIC will incorporate JABS information into law enforcement leads and intelligence products that will be distributed to law enforcement agencies requesting JABS information in accordance with the provisions of this agreement.

D. TEST DATA

The JABS PMO will provide test data to DPS ACTIC by March 15, 2007. This test data shall consist of a minimum of one thousand (1,000) records of FD 249 data contained in the JABS database. This test data will be sanitized with fictitious identifiers in place of true identifiers, and will include representative data in the same format and adhering to the same business rules of the JABS data that will be provided by the PMO per ARTICLE

5, SECTION A and B. above. In addition, the PMO will provide documentation regarding the data layout and explaining each field contained in the test data. DPS ACTIC agrees to use this test data only for purposes of testing and development work to assist in the development of the DPS ACTIC database.

E. SECURITY

The sharing of information between the JABS PMO and DPS ACTIC will be conducted under applicable law. Information provided to DPS ACTIC will be appropriately safeguarded in accordance with applicable national information security laws, policies and procedures; Attorney General Guidelines; Department of Justice security policies and standards; and any policies and procedures required by the JABS PMO.

Data handled by JABS is Sensitive but Unclassified (SBU). JABS handles biographical, fingerprint, and photographic data collected by law enforcement agencies during the booking process. Misuse of or unauthorized access to JABS data could result in unauthorized disclosure of information subject to statutory protections.

DPS ACTIC and any future signatories to this MOU agree to physically and electronically safeguard JABS information received pursuant to this MOU in the same manner as other law enforcement sensitive information utilized by DPS ACTIC.

JABS data shall be used only for official criminal justice purposes or in support of authorized investigative activities. Unauthorized or improper release of JABS data may violate federal, state, or local laws or departmental policy. Secondary dissemination of JABS data outside DPS ACTIC to an authorized party shall be recorded.

DPS ACTIC shall notify the JABS PMO immediately if the former discovers any unauthorized access or use of JABS Information by any DPS ACTIC employee, or if DPS ACTIC imposes sanctions upon, or revokes the access of, any DPS ACTIC employee on account of misconduct in connection hereunder. The JABS PMO and DPS ACTIC shall impose sanctions for misuse to the full extent allowed by applicable law and shall refer individual cases for further investigation and/or prosecution where appropriate.

Failure to comply with security requirements pursuant to this MOU by DPS ACTIC or any participating party may violate the privacy rights and civil liberties of citizens. Non-compliance may violate criminal statutes, resulting in severe sanctions.

Each participating agency will be responsible for conducting any Privacy Impact Assessments which implementation of this MOU may trigger under laws, regulation, or policies applicable to the respective Party.

F. PRIVACY AND CIVIL LIBERTIES

The participating parties acknowledge that the JABS initiative involves the collection, retention and dissemination of information about U.S. persons, which may be protected by the Privacy Act of 1974 and/or Executive Order, EO 12333, and that all such information will be handled lawfully pursuant to the provisions thereof. JABS activities, including the collection, retention and dissemination of personal information, will be conducted in a manner that protects and preserves the constitutional rights and civil liberties of all persons in the United States.

The participating parties further acknowledge that this MOU may be subject to guidelines now or hereafter issued for the protection of privacy, civil liberties, and other rights in the Information Sharing Environment (ISE), and that the MOU will conform to any such guidelines.

The participating agencies agree to review and make appropriate changes, if any, to their privacy compliance documents, including applicable Privacy Act system of records notices, in advance of the implementation of this MOU to ensure that the scope and routine uses of such notices permit the collection, maintenance and sharing of personal information as set forth in this MOU.

Section (c) of the Privacy Act, 5 USC 552a, requires that any 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 whom the disclosure is made. The accounting must be retained for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made. Participating parties will be responsible for complying with any accounting requirements regarding any information it discloses under this MOU.

G. EXPUNGEMENTS

Within four weeks of receipt of an expungement request from the JABS PMO, DPS ACTIC agrees to delete all occurrences of the identified arrest(s) and related data from the DPS ACTIC system, including backups.

H. OWNERSHIP OF RECORDS

Any JABS Information obtained pursuant to this MOU will be deemed to constitute a record of JABS, and the JABS PMO will be deemed to have retained control of such information for purposes of the application of the provisions of the Freedom of Information Act, 5 U.S.C. 552, the Privacy Act, 5 U.S.C. 552a, and any requests or

demands for information made by any judicial or administrative process to DPS ACTIC. DPS ACTIC will notify immediately an individual to be designated by the PMO if DPS ACTIC is served with a subpoena or other request for JABS Information obtained by DPS ACTIC hereunder. DPS ACTIC will immediately advise the JABS PMO of any litigation in which the PMO or the United States Department of the Justice has been or may be named as a party by virtue of the PMO's provision of information hereunder. JABS will handle any requests for records including any pleadings, court appearances and litigation related to JABS records requests.

I. DISCLOSURE OF DATA

To the extent that any information is subject to a Freedom of Information Act, Privacy Act, or a Congressional inquiry, any disclosure may only be made after all parties that contributed data to the product have been consulted. The Department will handle any requests for records, including any pleadings, court appearances and litigation regarding the information in the JABS database.

J. MEDIA

Media releases will conform to Department and JABS PMO guidelines regarding press releases. No press releases will be issued without prior JABS PMO approval.

ARTICLE 6: DURATION AND LIABILITY

A. DURATION


The term of this MOU shall be for an indefinite period. The MOU may be terminated at will by any party, provided written notice is provided to the JABS PMO of not less than thirty (30) days. It is understood that the termination of this agreement by any one of the participating parties will have no effect on the agreement between the remaining participating parties. 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 of this MOU.

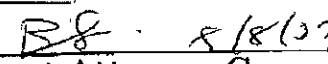

B. LIABILITY

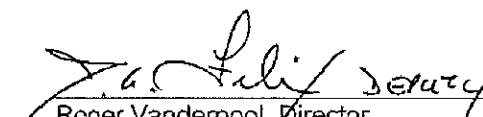
Each participating party acknowledges that financial and civil liability, if any and in accordance with applicable law, for the acts and omissions of their respective employees remains vested with his or her employing party. However, the Department may, in its discretion, determine on a case-by-case basis that an individual should be afforded legal representation, legal defense, or indemnification of a civil judgment, pursuant to federal law and Department policy and regulations.

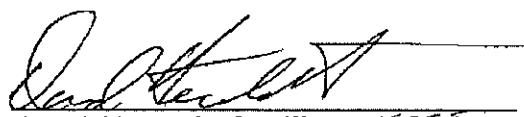
SIGNATORIES

This agreement between JABS PMO, MCSO and DPS ACTIC and future participating parties may be executed by each participating party signing a separate signature page.

 Dated this 5 day of Sept., 2007
Fred F. Baradari, Acting Assistant Director
Joint Automated Booking System Program Management Office


Assistant Attorney General
Approved as to Form 

 Dated this 13 day of August, 2007
Roger Vanderpool, Director
Arizona Department of Public Safety

 Dated this 22 day of August, 2007
Joseph M. Arpaio, Sheriff *CHIEF DEPUTY*
Maricopa County