Memorandum of Understanding
Sacramento County Sheriff's Department Business Systems Cost Recovery
With (El Dorado County Sheriff's Office)

THIS MEMORANDUM OF UNDERSTANDING (hereinafter referred to as "MOU") is made and entered into on this 18 day of June, 2012, by and between the SACRAMENTO COUNTY SHERIFF"S DEPARTMENT, a political subdivision of the State of California (hereinafter referred to as "County") and the Eldorado County Sheriff's Department (hereinafter referred to as "Outside Agency").

RECITALS

WHEREAS, County has put forth the effort to identify, procure, and implement Business Systems which serve County and its constituents; and

WHEREAS, Technology exists which would allow Outside Agency to use these systems without compromise to the information collected by both parties; and

WHEREAS, Outside Agency believes that use of Business Systems will improve its operations / delivery of service; and

WHEREAS, the County of Sacramento, acting by and through the Sheriff's Department, believes it to be mutually beneficial to both the County and Outside Agency to allow the use of Business Systems operated by the County; and

WHEREAS, County and Outside Agency desire to enter into this MOU on the terms and conditions set forth herein; and

NOW, THEREFORE, in consideration of the mutual promises hereinafter set forth, County and Outside Agency agree as follows:

1. DEFINITIONS

A. COUNTY is defined as the County of Sacramento, including its departments, subdivisions, agencies, instrumentalities, elected representatives, directors, officers, employees, servants, contractors, volunteers, and agents.

B. OUTSIDE AGENCY is defined as the "Outside Law Enforcement Agency's" employer, its successors, and assigns.

C. OUTSIDE AGENCY EMPLOYEE is defined as an employee or agent of "Outside Agency", his or her guardians, executors, administrators, heirs, and assigns.

D. BUSINESS SYSTEMS is defined as any application, program, software, or network which was either procured or created for use within the County of Sacramento, by the Sacramento County Sheriff's Department (SSD).

E. MOU is defined as this Memorandum of Understanding.

F. LIKE COMPUTER EQUIPMENT is defined as a computer which is of like manufacturer, model, and accessories as SSD has in service. Specifications are available from SSD upon request, additional information is included in Section 6.

G. CAD is defined as the Computer Aided Dispatch System SSD procured from, and continues to pay maintenance fees to a vendor. CAD includes:

1) Mobile CAD - an application which is loaded on the like computer equipment which utilizes a Vehicle Radio Modem (VRM) in order to communicate. This application provides full functionality for field support.

2) Remote CAD - an application which is loaded on a computer which has a secure connection to the SSD law enforcement network. This application allows full interaction with the CAD for use within a facility.

3) CAD Browser - an application which allows no interaction, just displays the current information active in CAD

H. RMS is defined as the Records Management System SSD procured from, and continues to pay maintenance fees to a vendor.

I. AFR is defined as the Automatic Field Reporting System SSD procured from, and continues pay to maintenance fees to a vendor.

J. WebKPF is defined as a web based application which keeps "Known Persons" information. The system is maintained by the County of Sacramento.

K. iMUG is defined as a web based application which provides "Mug Shots" of persons who were incarcerated in most of California.

L. RECON is defined as a web based photographic imaging (mugshot) application designed to assist with the identification or investigation of a subject.

M. GRAB'EM is defined as a handheld Mobile Identification System used to identify unknown subjects in the field.

N. IBIS Generic Interface is defined as an identification interface and data format that allows third party systems to perform mobile identification searches through the IBIS Server.

2. TERM OF THE MOU

This Agreement is effective as of the day and year first hereinabove appearing and shall continue thereafter so long as the County Business Systems are in place.

If Outside Agency no longer wishes to use County Business Systems, they must submit a letter of intent not later than June 1, and must discontinue use of the County Business Systems not later than June 30. Because licensing is paid to the vendors each July, we are unable to recover any licensing expenses if Outside Agency chooses to discontinue use prior to June 30.

If applicable, a letter of intent not to use County Business Systems should be addressed to:

Information Technology Manager
Technical Services Bureau
Sacramento County Sheriff's Department
711 G Street
Sacramento, CA 95814

County will notify Outside Agency should it begin the process to either replace or discontinue any or all of its County Business Systems. The notification will be addressed to the Agency Head or Chief of Police on the date of the letter.

Outside Agency and the Outside Agency's employee understand and agree that the County may terminate this agreement at any time and for any reason, as the County determines appropriate in its sole discretion.

3. BACKGROUND CHECKS

It is expected that all Outside Agency employees who will be granted access to the County business systems will have completed a background investigation performed either by Outside Agency, the Sacramento County Sheriff's Department's Pre-Employment Unit, or by an agency with similar capabilities and experience. The background investigation should conform to California Government Code Sections 1029 and 1031, and follow the guidelines set forth by P.O.S.T. as described in the publication *POST Background Investigation Manual: Guidelines for the Investigator.*

Outside Agency will create an XREF in KPF adding a note that the Outside Agency's employee is employed by Outside Agency and request that Outside Agency be notified should Outside Agency's employee be arrested. Outside Agency will notify SSD as soon as

possible and reasonable after the arrest, and if appropriate, access to County Business Systems will be suspended for Outside Agency's employee.

4. USE OF COUNTY BUSINESS SYSTEMS

During the term of this MOU and so long as Outside Agency is not in breach of its terms and conditions, County grants to Outside Agency use of the County Business System(s) as defined in Section 5 which are selected by Outside Agency using Appendix B.

Outside Agency and Outside Agency's employees understand and agree that the there is no guarantee of performance associated with the use of County Business Systems.

Outside Agency agrees to use County Business Systems for the purpose of law enforcement only. These systems have access to confidential criminal records, Department of Motor Vehicle records, or other criminal justice information which is controlled by statute. Misuse of such information may adversely affect an individual's civil rights. Outside Agency's employees must have a legitimate business purpose in accessing the information, and they must have the legal authority pursuant to both law and Outside Agency 's policy to access the information (Penal Code Sections 11105 and 13300).

Outside Agency agrees to, should the Outside Agency's employee not use County Business Systems accordingly, effect disciplinary action according with Outside Agency's policy or Penal Code Sections 11141-11143 and 11302-13304, Government Code Section 6200, and California Vehicle Code Section 1808.45.

County reserves the right to remove Outside Agency's employee's access to County Business Systems if Outside Agency does not effect the appropriate action.

5. COUNTY BUSINESS SYSTEMS OFFERED

County is able to allow access to CAD and AFR to all Outside Agency's employees who are sworn or provide direct support to persons in the field. RMS, WebKPF, iMUG, RECON, and GRAB'EM are available for Outside Agency's employees who are sworn and personnel that are providing immediate support for sworn field personnel.

Outside Agency will complete Appendix B which will be used both for equipment configuration and security / access to County Business Systems. Outside Agency will append Appendix B as it will be used for all additions, changes, or deletions of users and clients (like computer equipment).

Outside Agency will make every effort to properly identify the greatest number of Concurrent Licenses which are required for their use. A Concurrent License is based on the number of simultaneous users accessing the program. This does include any shift overlap, regardless of how brief the overlap may be. For example, if one employee must log onto the application before the other can log off, two Concurrent Licenses are required.

6. LIKE COMPUTER EQUIPMENT

County, in order to support its own personnel and deliver service to its constituents, will develop systems on specific hardware platforms. These platforms are kept in service for three to five years on average, depending upon the type of equipment.

Outside Agency is asked to procure / provide like computer equipment in order to facilitate installation / configuration of said equipment.

All equipment has been decided upon either through a request for bid or a request for proposal process. Outside Agency, if allowed, may work with our purchasing department in order to utilize any of these contracts.

County will not procure equipment on behalf of the Outside Agency, nor will it be responsible in any way for the delivery, repair, or return of said equipment. Any and all warrantees or maintenance contracts are the responsibility of Outside Agency, and not the County.

Appendix A reflects the equipment considered like computer equipment as of the date on the Appendix. County will update Appendix A as needed depending upon the equipment available in the market place.

County will configure equipment listed on the most current Appendix. County will make a best effort to configure equipment on any previous Appendix. County will not configure equipment not listed on any Appendix.

7. COST RECOVERY

County will update Appendix C which reflects the current costs County will need to pay out on behalf of Outside Agency and any internal costs expected for the following fiscal year. This will reflect real costs without any load.

County will send an invoice for the County Business Systems Outside Agency is using. The Invoice will be mailed not later than April 1, due on July 1, and late by August 1. Included will be a revised copy of Appendix B and Appendix C.

In the event of the failure of Outside Agency to make any payment required herein when due, County may discontinue access to County Business Systems, and / or bring an action for the recovery of such payment and interest thereon. The exercise of any right provided in this Agreement shall not preclude the County from exercising any other right so provided or at law, remedies provided herein or at law being cumulative and not exclusive.

8. MULTIPLE AGREEMENTS

Outside Agency and the County may have more than one agreement / MOU in place. Should any part of this MOU duplicate or replace any other agreement / MOU, clarification will be listed in Appendix D, Exceptions.

9. INDEMNIFICATION/INSURANCE

Outside Agency and Outside Employees agree to:

Outside Law Enforcement Agencies shall defend, indemnify and hold harmless County, its Board of Supervisors, officers, directors, agents, employees and volunteers from and against any and all demands, claims, actions, losses, liabilities, damages, and costs, including payment of reasonable attorneys' fees, arising out of or resulting from the performance of this MOU, except and in proportion to the extent caused by the negligence or willful misconduct of County, its Board of Supervisors, officers, directors, employees, agents or volunteers.

This Indemnification and Hold Harmless Agreement shall be broadly interpreted according to California state law. If any portion of this document is held invalid, the balance shall continue in full force and effect.

INSURANCE

Each Party, at its sole cost and expense, shall carry insurance –or self-insure - its activities in connection with this MOU, and obtain, keep in force and maintain, insurance or equivalent programs of self-insurance, for general liability, workers compensation, property, professional liability, and business automobile liability, adequate to cover its potential liabilities hereunder. Each party agrees to provide the other thirty (30) days' advance written notice of any cancellation, termination or lapse of any of the insurance or self-insurance coverages.

10. GOVERNING LAW

The interpretation and enforcement of the MOU shall be governed by the laws of the State of California, and where applicable, by federal law. The parties agree to submit any disputes arising under the MOU to a court of competent jurisdiction located in Sacramento, California.

11. ATTORNEYS' FEES

If any legal proceeding should be instituted by either of the parties hereto to enforce the terms of this Agreement or to determine the rights of the parties there under, the prevailing party in said proceeding shall recover, in addition to all court costs, reasonable attorneys' fees.

12. AMBIGUITIES

The parties have each carefully reviewed this MOU and have agreed to each term of this MOU. No ambiguity shall be presumed to be construed against any other party.

13. INTEGRATION

This MOU embodies the entire agreement of the parties in relation to the scope of services herein described, and no other agreement or understanding whether verbal, written or otherwise exists between the parties.

14. AMENDMENT AND WAIVER

Except as provided herein, no alteration, amendment, variation, or waiver of the terms of this Agreement shall be valid unless made in writing and signed by both parties. Waiver by either party of any default, breach or condition precedent shall not be construed as a waiver of any other default, breach or condition precedent, or any other right hereunder. No interpretation of any provision of this Agreement shall be binding upon COUNTY unless agreed in writing by DIRECTOR and counsel for COUNTY.

ADMINISTRATOR: The El Dorado County Officer or employee with responsibility for administering this Agreement is John D'Agostini, Sheriff, or successor

IN WITNESS WHEREOF, the parties have entered into this Agreement on the day and year first hereinabove appearing.

COUNTY OF SACRAMENTO
a Political Subdivision of
the State of California

By:_____
Scott R. Jones, SHERIFF

Approved as to Form

By: _____
Supervising Deputy County Counsel

OUTSIDE AGENCY
El Dorado County Sheriff's
Office

By:_____
John D'Agostini, SHERIFF

Approved as to Form

By:_____
Legal Counsel

--COUNTY OF EL DORADO--

Dated: 6/18/13

By: _____
RON BRIGGS, Chair
Board of Supervisors
"County"

ATTEST:
James S. Mitrisin
Clerk of the Board of Supervisors

By: _____ Date: 6/18/13
Deputy Clerk

Appendix #A (July 1, 2012)
Like Computer Equipment Specifications

Desktop:

HP Compaq 8200 Elite Convertible MinitowerPC
Win 7 Home Premium OS
Intel® Core i7-2600 Processor (SIPP Processor)
Intel vPro Technology
8GB DDR3 non-ECC (2x4GB)
500GB 7200RPM SATA 6.0 Gb/s NCQ, SMART IV
NVIDIA NVS 300 PCIe x16 - 1st Card
DMS-59 to Dual DVI Cable Kit
HP SATA SuperMulti DVD Writer Drive
22-in-1 3.5" Media Card Reader
HP USB Standard Keyboard
HP USB 2-Button Optical Scroll Mouse
HP Compaq 8200 Elite CMT HE Chassis
Single Unit (CMT) Packaging
5/5/5 CMT Warranty
HP Compaq 8200 Elite Country Kit (Docs)

Mobile Computer:

Panasonic CF-31JBGEC1M: MK2
Windows 7 Professional
Intel Core i5 2520M 2.50GHz
13.1" XGA Touchscreen LCD
320GB Shock mounted HDD (7200rpm)
4GB
Wi Fi
Bluetooth
AT&T 4G LTE
GPS Receiver
Dual Pass (Upper WWAN / Lower Selectable)
TPM 1.2
Backlit Emissive Keyboard
Toughbook Preferred

Air Cards:

AT&T USBConnect Momentum 4G

Mobile Identification System:

MorphoTrust RDT - Extreme (fingerprint capture wand – wireless)
MorphoTrust BTO – 500 (USB fingerprint capture – single print)
MorphoTrust DFR – 2100 (USB fingerprint capture – single print)
Zoom 4314 USB Class 1 Bluetooth adapter

Appendix #B (April 1, 2010)
County Business Systems, User List and Client List

			User						System						
Last Name	First Name	X-REF	Sworn	Security Officer	Dispatcher	Records Officer	RECON	GRABEM	RMS	AFR	Mobile CAD	iMUG	WebKPF	RECON	GRABEM
Bragg	Adam	3952857	x							x	x		x		
Correa	Ralph	2370127	x							x	x		x		
Diller	Shane	2960170	x							x	x		x		
Gregorio	Michael	137355	x							x	x		x		
McClintock	Kristofer	3731689	x							x	x		x		
Pierce	Kenneth	3916189	x							x	x		x		
Tom	Thomas	4312169	x							x	x		x		

Concurrent License Count

Mobile CAD allows for Concurrent Licenses. What is the greatest number of users scheduled?

Sworn	3
Security	
Dispatch	
Records	

Licenses Required
3

RMS allows for Concurrent Licenses. What is the greatest number of users scheduled?

Sworn	
Security	
Dispatch	
Records	

Licenses Required
0

Computers

Laptop	Mobile	Desktop	Computer Serial Number	System: Mobile CAD	RMS	AFR	WebKPF	iMUG	RECON	GRABTEM	Modem (Air Card) Information: Phone Number	IMEI	SIM
x			Not Yet Delivered 1	x		x	x				TBD	TBD	TBD
x			Not Yet Delivered 2	x		x	x				TBD	TBD	TBD
x			Not Yet Delivered 3	x		x	x				TBD	TBD	TBD
x			Not Yet Delivered 4	x		x	x				TBD	TBD	TBD

This modification of Appendix B is made and entered into on this _____ day of _____, 2012, and is mutually agreed upon by both County and Outside Agency. Outside Agency agrees to reimburse County for any and all costs which may result in the addition of users or equipment upon the receipt of an invoice detailing said changes.

By: _____ By: N/A

Scott R. Jones, SHERIFF John D'Agostini, SHERIFF

Date: _____ Date: _____

Appendix #C (July 1, 2012)
Costs for Fiscal Year 2012/2013

RMS	AFR	Mobile CAD	WebKPF	RECON	GRAB'EM	IBIS Interface
Charges are for the first system granted, there are no additional charges for additional systems						
2nd Factor Authentication Token (Security) - One Time $20.00 per user 2nd Factor Authentication User License (Security) - Yearly $8.00 per user Net-Motion (Security) - Yearly $154 per computer			None	None	None	None
Trend Micro (Anti Virus) - Yearly $10 per computer			None	None	None	None
Microsoft - $647.15 per addition (true up) $158.41 per existing device		None	None	None	None	None
VPN Client Licensing						
$32.03 per user		None	$32.03 per user	None	None	None
SSD Cost Reimbursement - One Time, First System						
$32.03 per user		None	$32.03 per user	$512.48	$512.48	$512.48
SSD Cost Reimbursement - Yearly						
Account Maintenance - $32.03 per year				None	None	None
None	None	$128.10 per year	None	None	None	None
SSD Cost Reimbursement - Technical Projects / Engineering						
$64.05 per hour						
Dispatch Services - Yearly						
		$2359.37 per vehicle				
Software Licensing, Concurrent Users - Yearly						
$1,160		$1,660		Should your agency's needs expand beyond the original design, necessary expenses will be paid directly to the vendor, DataWorks Plus, MorphoTrust, or Computer Deductions Incorporated.		
Software Licensing, Per Computer or User - Yearly						
	$340 per client		$3,804.00			

Appendix #D

Exceptions

Outside Agency understands and agrees that, due to the nature of the RECON and GRAB'EM systems, some costs associated with the Outside Agency's use of those systems are outside the scope of this MOU and must be paid by the Outside Agency directly to those system providers. Such costs may include the following:

Common

A. Connectivity cost to SSD (e.g. T-1 line, VPN tunnel, Microwave, etc.)
B. Any customization desired specific to the OUTSIDE AGENCY that will not be system – wide. Any potential customization is prohibited from negatively impacting or compromising the core RECON or GRAB'EM system, or its functionality, its data integrity, or its end users.

RECON

A. Application Program Interface (API) cost to connect to RECON application. Refer to DataWorks Plus for details and clarification charged by DataWorks Plus.
B. Initial template fees (per image cost) to import the OUTSIDE AGENCY images into the RECON – and 2D recognition database if the OUTSIDE AGENCY desire to search their images in the 2D Recognition database charged by DataWorks Plus. If the OUTSIDE AGENCY does not desire to search images in the 2D Facial Recognition database, there will be no per image template fee.
C. PRO RATA annual maintenance cost for templates (as applicable) charged by DataWorks Plus.
D. Seat Licensing – if the OUTSIDE AGENCY requires additional concurrent users, they agree to purchase additional licenses charged by DataWorks Plus.

GRAB'EM

A. Cost of any server hardware/software necessary to authenticate/administrate user security.
B. Any expenses to register, support, or maintain biometric capture devices charged by CDI and MorphoTrust.

By: _____ By: _____
Scott R Jones, SHERIFF John D'Agostini, SHERIFF

Date: _____ Date: 12/10/12

ATTACHMENT 1
RECON TECHNICAL DESCRIPTION

1. PURPOSE

This document has been created by the Sacramento County Sheriff to inform Outside Agencies of the details and technical skills needed in order to implement the Regional Consolidated Mugshot System (hereinafter referred to as "RECON").

2. BACKGROUND

The Sacramento Cal-ID Program (hereinafter, referred to as Sac Cal-ID) and the SSD has built and deployed a regional consolidated mugshot system that contains facial images from four (4) counties: El Dorado, Placer, Sacramento, and Yolo Counties – with potential future additional agencies/counties. The intent is to give all officers in those agencies access to a facial image database for law enforcement purposes and further, give all the participating agencies the ability to perform 2D facial recognition searches against a single central database. This system known as RECON was developed by, and is supported by, DataWorks Plus, (hereinafter referred to as DWP), Sac Cal-ID and the SSD. RECON was funded by Sac Cal-ID trust funds at the direction of the Sacramento Remote Access Network (hereinafter referred to as Sac RAN Board) and by Outside Agencies.

The contact for this is through the Sacramento County Sheriff's Department Technical Services Help Desk at (916) 874-4999.

Access to GRAB'EM and the associated databases will be restricted to only the Outside Agencies that are signatories to the Sacramento County Sheriff's Department Memorandum of Understanding for Business Systems Cost Recovery.

3. DESCRIPTION

RECON – Is a photographic imaging (mugshot) application that includes sophisticated functionality including facial image searching, creation of lineups, 2D facial image searching/matching, etc. via a web based client using a concurrent user license model. It consists of a large image database, server hardware, application software, and a 2D facial image search engine. The primary system being located at the Sacramento County Sheriff's Department Headquarters Building, 711 G Street, Sacramento, CA. The secondary system resides at the Sacramento City Police Department Headquarters Building, 5770 Freeport Boulevard, Sacramento, CA. Both agencies have warm-standby servers for backup/redundancy purposes. The Outside Agencies will be connecting to, and accessing, the primary RECON System located at the SSD.

4. PERFORMANCE AND TIMELINESS

The data is provided by a variety of sources including, but not limited to, the SSD and the Sacramento County Criminal Justice Information System (CJIS). Information from partner systems is sometimes delayed. Once the information is received by RECON, it will be returned to the user that requested the information. Most information returns in less than one minute, but some responses have been delayed and not returned for several minutes.

5. ACCURACY OF INFORMATION

The data provided by RECON is assumed to be accurate. The Outside Agencies representatives are encouraged to participate in testing sessions to ensure information is accurate, particularly following major releases. The Outside Agency understands that data inaccuracies can arise for multiple reasons (e.g. data entry errors, etc.). It is considered best practice for the Outside Agencies to confirm the accuracy of the information with the source agency (e.g. Placer County Sheriff, Yolo County Sheriff, Roseville Police Department, etc.). It is also best practice to put forth a best effort to ensure the integrity of the data being uploaded into RECON and perform error corrections in a timely and diligent manner as errors are discovered and identified.

6. STATUTORY INFORMATION

The information obtained from RECON is intended for official purposes only and should comply with all Federal and State statutes applicable to the dissemination of Criminal Offender Record Information (CORI). See U.S. Code Title 28, Chapter 1, Part 20 and California Penal Code Sections commencing with § 11105 and § 13320.

7. SECURITY ADMINISTRATION

Each Outside Agency will need to have an Account Administrator within that agency. SSD will provide Security System administration training for Agency Administrator(s) and the CAL ID Unit will provide user application training. The Agency Account Administrator(s) have the responsibility to ensure that all users have the right to access, and the need to access, law-enforcement data and will need to maintain a user agreement form for each user. User Agreement forms will need to be attached to the user's online security account such that audits can be performed without site visits. Agency Account Administrators are also responsible for the timely removal of any user accounts associated with users who have separated with the agency. A user agreement form may be obtained by contacting the SSD Agency CLETS Coordinator (ACC) at acc@sacsheriff.com or visiting the website at sacjustice.ca.gov, User Compliance link.

8. SUSPENSION OF SERVICES

At the direction of the Sac RAN Board and/or the SSD, participation by the Outside Agency may immediately be suspended for the purpose of protecting the integrity and efficiency of RECON. Appropriate reasons for such suspension include, but are not limited to, failure by the Outside Agency to comply with: the best practices listed in this document; any rule, policy, or procedure adopted for RECON operation; or any State or Federal law relating to the security and privacy of RECON information. Any such suspension may terminate based on satisfactory assurance that the apparent problem has been corrected.

9. BROWSER SUPPORT

The RECON application has been developed to operate on Microsoft Internet Explorer (hereinafter referred to as IE); other browsers will not be supported. Further, only two (2) versions of IE will be supported, typically, the two (2) most recent versions. Within one (1) year of the launch/release of a new version of IE, the new version will be supported as well as the previous two versions. At the end of the one (1) year period after a new release, the oldest version of the three (3) will no longer be supported.

10. EFFORTS NECESSARY OF OUTSIDE AGENCY

The Outside Agency will need to:

A. Provide and maintain connectivity from their agency to the SSD and RECON
B. Upload their county's mugshot images into the RECON database through DWP
C. Perform ongoing error corrections of their data in a timely and diligent manner as errors are discovered and identified
D. Capture facial images (mugshots) in National Institute of Standards and Technology (NIST [FBI]) Best Practice Recommendation Format

11. HELP DESK SUPPORT

Each Outside Agency should have information technology professionals that can perform trouble shooting steps on their equipment in attempt to resolve client related issues. If the Outside Agency believes the issue to be system wide, technical professionals should contact SSD's help desk at 916-874-4999 during business hours, 0800-1700 Monday through Friday excluding County Holidays. If it is after hours, e-mail can be sent to helpdesk@sacsheriff.com.

ATTACHMENT 2
GOLD REGION AGGREGATE BIOMETRIC ENFORCEMENT MATRIX
Technical Description

1. PURPOSE

This document has been created by the Sacramento County Sheriff to inform Outside Agencies of the details and technical skills needed in order to implement the GOLD REGION AGGREGATE BIOMETRIC ENFORCEMENT MATRIX System (hereinafter referred to as "GRAB'EM").

2. BACKGROUND

The Gold Region Aggregate Biometric Enforcement Matrix (hereinafter referred to as GRAB'EM) was created by the Sacramento County Cal-ID Program (hereinafter referred to as Sac Cal-ID) and the Sacramento County Sheriff's Department (hereinafter referred to as SSD) at the request of the Sacramento County Users' Group (all law enforcement agencies in the county served by Sac Cal-ID), and in cooperation with law enforcement agencies in El Dorado, Placer, and Yolo Counties, and at the direction of the Sacramento County Remote Access Network (hereinafter referred to as RAN) Board. Expansion of the GRAB'EM System to other counties in the region is anticipated.

GRAB'EM is designed to be an effective and beneficial tool available to law enforcement agencies in the participating counties. GRAB'EM was architected to effectively and efficiently identify recidivist criminal offenders through the electronic capture, transmission, comparison, and verification of thumb and index fingerprints via wired and wireless networked devices. The system consists of a pooled, centralized fingerprint image base, called the Recidivist Database, and a search engine, called Positive Identification (PID), networked to criminal justice databanks. GRAB'EM will allow Outside Agencies to remotely search the centralized image database and associated databases.

This system known as GRAB'EM was primarily developed by, and is supported by, NEC, Identix (now known as MorphoTrust), Computer Deductions, Inc., Sac Cal-ID and the SSD and interacts with a variety of other vendors/systems. GRAB'EM was funded by Sac Cal-ID trust funds at the direction of the Sacramento Remote Access Network (hereinafter referred to as Sac RAN Board), by Federal Grant monies, and by participating agencies.

The Sacramento County Sheriff's Department, the Sacramento County Cal-ID Program and the Sacramento County RAN Board are referred to jointly as the Sacramento County Entities. The contact for this is through the Sacramento County Sheriff's Department Technical Services Help Desk at (916) 874-4999.

Access to GRAB'EM and the associated databases will be restricted to only the Outside Agencies that are signatories to the Sacramento County Sheriff's Department Memorandum of Understanding for Business Systems Cost Recovery.

3. DESCRIPTION

GRAB'EM – Is a Mobile Identification System (hereinafter referred to as MID) that can also be accessed from a desktop wired platform. Its main function is to identify unknown subjects in the field. The System maintains a pooled, centralized fingerprint image database known as the Recidivist Fingerprint Database (hereinafter referred to as RFD). The RFD is consolidated at one central primary site located at the Sacramento County Sheriff's Department Headquarters Building, 711 G Street, Sacramento, CA 95814. The secondary redundant RFD resides at the Sacramento County Sheriff's Department Central Division, Florin Station, 7000 65th Street, Sacramento, CA 95823.

The GRAB'EM business logic is to: capture a biometric fingerprint on a hand held, wireless livescan capture device; remotely deliver that biometric to the server/controller known as Integrated Biometric Information System (hereinafter referred to as IBIS) via a blue tooth connection to a laptop or directly via a smart phone/hand-held computer. IBIS logs the transaction and sends the image to the Consolidated Transaction Management Controller (hereinafter referred to as CTMC).

The CTMC interfaces with the fingerprint search engine PID, passing through the fingerprint to be searched against the PID database. The PID fingerprint database archives searchable fingerprint minutia from five (5) counties; El Dorado, Placer, Sacramento, Solano, and Yolo – with potential future additional counties. PID is populated directly from the whole fingerprint images in RFD. PID sends a response back to the CTMC. If the fingerprint is known to the system, CTMC searches: Web-KPF (a regionalized known persons system); the Regional Consolidated Mugshot System, (hereinafter referred to as RECON); and the Fingerprint Identification Numbers Database (FIND).

CTMC will extract relevant data from the systems and return the data to the IBIS server. IBIS parses the data and packages it for delivery back to the originating device. The RFD database is updated with new images and corresponding data by Participating User Agencies at regular intervals. The originating device displays the subject's true identity along with an accompanying photo, demographic data (i.e. date of birth, social security number, driver license information, etc.) as well as warrant information, when applicable, to the end - user.

4. PERFORMANCE AND TIMELINESS

The data is provided by a variety of sources including, but not limited to, the SSD and the Sacramento County Criminal Justice Information System (CJIS). Information from partner systems is sometimes delayed. Once the information is received by GRAB'EM, it will be returned to the user that requested the information. Most information returns in less than one minute, but some responses have been delayed and not returned for several minutes.

5. ACCURACY OF INFORMATION

The data provided by GRAB'EM is assumed to be accurate. The Outside Agency representatives are encouraged to participate in testing sessions to ensure information is accurate, particularly following major releases. The Participating User Agency understands that data inaccuracies can arise for multiple reasons (e.g. data entry errors, etc.). It is the responsibility of the Outside Agency to confirm the accuracy of the information with the source agency (e.g. Placer County Sheriff, Yolo County Sheriff, Roseville Police Department, etc.). The SSD shall not be held responsible for any defect in the GRAB'EM services or the accuracy of provided data, irrespective of its nature or its

cause. The Outside Agency and the SSD will put forth a best effort to ensure the integrity of the data being uploaded into GRAB'EM/RFD and mutually agree to perform error corrections in a timely and diligent manner as errors are discovered and identified.

6. STATUTORY REQUIREMENTS

The information obtained from GRAB'EM is intended for official purposes only and should comply with all Federal and State statutes applicable to the dissemination of Criminal Offender Record Information (CORI). See U.S. Code Title 28, Chapter 1, Part 20 and California Penal Code Sections commencing with § 11105 and § 13320.

7. SECURITY ADMINISTRATION

Each Participating User Agency will need to have an Account Administrator(s) within that agency. SSD will provide Security System administration training for Agency Administrator(s) and the CAL ID Unit will provide user application training. The Agency Account Administrator(s) have the responsibility to ensure that all users have the right to access, and the need to access, law-enforcement data and will need to maintain a user agreement form for each user. User Agreement forms will need to be attached to the user's online security account such that audits can be performed without site visits. SSD is not responsible for ensuring that users have the right to, and the need to, access law-enforcement information. Agency Account Administrators are also responsible for the timely removal of any user accounts associated with users who have separated with the agency. A user agreement form may be obtained by contacting the SSD Agency CLETS Coordinator (ACC) at acc@sacsheriff.com or visiting the website at sacjustice.ca.gov, User Compliance link.

8. SUSPENSION OF SERVICES

At the direction of the Sac RAN Board and/or the SSD, participation by the Outside Agency may be suspended for the purpose of protecting the integrity and efficiency of GRAB'EM. Appropriate reasons for such suspension include, but are not limited to, failure by the Outside Agency to comply with: the best practices listed in this document; any rule, policy, or procedure adopted for GRAB'EM operation; or any State or Federal law relating to the security and privacy of GRAB'EM information. Any such suspension may terminate based on satisfactory assurance that the apparent problem has been corrected.

9. OPERATING SYSTEM SUPPORT

The GRAB'EM application has been developed to operate on Microsoft Windows Operating System XP and Windows 7 (hereinafter referred to as OS); other versions may not be supported. As new versions/releases of OS are made available, GRAB'EM software may be developed and made available, with older OSs eventually being phased out and no longer supported.

10. RESPONSIBILITIES

The Outside Agency must:

A. Allow for the upload all new fingerprint images to the RFD on a periodic interval, not to exceed two (2) days from date of capture.

B. Install and maintain a telephone (data) line or network connection to the Central Site (Sacramento Sheriff's Department Telecommunications Neutral Zone.)
C. Maintain a server/computer to administrate security (for user authentication and to delete/expunge records.)
D. Be identified by its NCIC ORI number.
E. Capture fingerprints images in National Institute of Standards and Technology (NIST [FBI]) Best Practice Recommendation Format.
F. Perform ongoing error corrections of their uploaded data in a timely and diligent manner as errors are discovered and identified

11. REGISTRATION OF BIOMETRIC CAPTURE DEVICES

The Outside Agency will need to contact CDI and MorphoTrust for all device registrations and deactivations. The method of device registration/deactivation along with the device ID format are to be defined amongst the Participating User Agency, CDI, and MorphoTrust.

12. HELP DESK SUPPORT

Each Outside Agency should have information technology professionals that can perform trouble shooting steps on their equipment in attempt to resolve client related issues. If the participating agency believes the issue to be system wide, technical professionals should contact SSD's help desk at 916-874-4999 during business hours, 0800-1700 Monday through Friday excluding County Holidays. If it is after hours, e-mail can be sent to helpdesk@sacsheriff.com.

ATTACHMENT 3
IBIS Generic Interface
Technical Description

1. PURPOSE

As part of the Sacramento County IBIS Solution, L-1 Identity Solutions – Biometrics Division is providing a set of standard mobile identification interfaces and data formats to allow third party systems to perform mobile identification searches through the IBIS Server.
The primary purpose of this document is to specify the steps a vendor must follow to properly submit searches and receive responses from the generic interface.

2. GENERIC INTERFACES

This section will describe the steps necessary for a vendor to submit and receive transactions as described in the Sacramento generic Interface ICD Document

A. FTP

This section describes the FTP interface based on the CALDOJ Global Transaction Control (GTC), Part VI: Live Scan Interface Version 5, January 21, 2010 Document

Steps to be taken before submission is allowed

Contact L-1 Field service with the Livescan ID of the new Device that wishes to submit to the generic interface

L-1 field service will: Create a new directory under the submission directory named after the

Livescan ID received from the customer

Add user name and password and assign them to the correct group on the FTP server

Add the Livescan ID to the allowed livescan ID's configuration section of the IBIS Server.

Contact the customer to inform them the server is ready for submittal

FTP Communication

Client devices communicate with the IBIS SERVER by reading from and writing to the submission directory that resides on the IBIS SERVER. In order to facilitate understanding of this communication process, the layout of the submission directory is described next, followed by the details of data transmission.

B. SUBMISSION DIRECTORY

As described earlier, Client/IBIS SERVER communication involves reading from and writing to directories that reside on the IBIS SERVER and that are accessed by client

devices. The IBIS SERVER uses some of these directories to receive submissions from devices on the network. The number of submission directories may be increased at the discretion of L-1 as needed to support the workload.

Each group of client devices is assigned to a single submission directory in which those client devices and the IBIS SERVER write the files that they use to communicate with each other. Figure 2 shows the general form of a submission directory. In every submission directory there are one or more group directories and one signal directory. Each group directory contains a sub-directory for each client device in the group, and each client sub-directory contains directories below it named in and out.

When a new submission is written to the disk, its filename is determined by the time stamp taken at that time. This time stamp is in the form DDHHMMSS described below:

DD the two digit day of the month (i.e. 25 describes the 25th of any month)

HH the hour of day in military time (i.e. 13 describes 1:00 p.m.)

MM the minute (i.e. HHMM = 0915 describes 9:15 a.m.)

SS the second (i.e. HHMMSS = 091500 describes 9:15 a.m. exactly)

This filename uniquely identifies the new submission throughout the communication process. The signal file to IBIS SERVER that accompanies the submission carries the same name with a three-character extension that is the device ID of the client that made the submission. Acknowledgments and responses from the IBIS SERVER are named like the signal file.

In the event that an expected acknowledgment is not received within the prescribed time frame, and resubmission is deemed necessary, the following protocol shall be utilized. In such a case the client device shall resubmit the original submission using the original time stamp. Using this approach of overwriting the original file leaves no possibility of duplicate entries.

In the event an error occurs preventing the transmission of a signal file after the submission file has been deposited, it is important that the device recover gracefully. It is most important to avoid at all costs an orphaned submission.

Figure 2 shows an example in which the client device LS1 in-group grp1 has submitted a NIST file named 06113000 (this name tells us that the submission was created on the 6th of the current month at 11:30 a.m. exactly). The newly submitted file has been written to the client's dedicated directory, after which a signal file called 06113000.ls1 was written to the directory's signal file directory to notify the IBIS SERVER of the new submission. Signal files from other client devices in other groups have also been written to this directory. If the IBIS SERVER accepts the submission it will write an acknowledgment to the client's out directory named 06113000.ls1. This process is explained in greater detail in the next section.

Figure 2. Submission directory layout

dir4 (submission directory #4)

sigfiles (signal files)

06113000.ls1

06113100.abc

06113130.xyz

grp1 (grp1 directory)

ls1 (submissions from ls1)

06113000 (nist submission file)

in (reserved)

out (IBIS SERVER messages)

06113000.ls1

lsn (nth client in grp1)

in

out

grpn (nth group in this directory)

C. DATA TRANSMISSION PROCESS

The following table shows the chronological order in which files are created and deleted during a client/IBIS SERVER communication session, along with the location and naming scheme of the newly created files. The example used is LS1's submission named 06113000, the same example shown in Figure 2.

Step Taken	New File Name and Location	
i.	LS1 writes a NIST-format submission.	/dir4/grp1/ls1/06113000
ii.	LS1 writes a signal file.	/dir4/sigfiles/06113000.ls1
iii.	IBIS SERVER scanner detects the signal file.	

iv. IBIS SERVER uses the signal file name to locate the NIST submission.

v. IBIS SERVER deletes the signal file.

vi. IBIS SERVER acknowledges receipt of the submission and writes an acknowledgment file. /dir4/grp1/ls1/out/06113000.ls1

vii. IBIS SERVER moves NIST file to another location, deleting the copy in submission directory (IBIS SERVER deletes the submission file either now or after processing the NIST record).

viii. If IBIS SERVER rejects the submission it will write one or more messages back to the originating device. /dir4/grp1/ls1/out/mxxnnnnn

ix. Client reads and deletes acknowledgement or message file(s).

D. ACKNOWLEDGMENT FILES

At the time that the IBIS SERVER recognizes the new submission it writes an acknowledgment file like the one described in step 6, above, to the out directory of the originating client device. The name of the acknowledgment file is the same as the name of the submission file (DDHHMMSS.LLL), and the contents are as follows:

SCN:iiiyjjjhhmm

ARV:mmddyyhhmmss

The first line is the State Control Number, comprised of the three-character livescan ID, the last digit of the current year, the three-digit Julian date, and a four digit sequence number.

The second line is the arrival time of the submission as determined by the IBIS SERVER clock time with, in two digits each, the month, day, year, hours, minutes and seconds.

Each client device (except those using ftp) is responsible for deleting its own acknowledgment files as soon as it receives them.

Message Files

If IBIS SERVER rejects the new submission, one or more message files are written as described in step 8, above. The name of a message file follows the format mxxnnnnn described below:

m every completed message file begins with the letter "m" (while it is

being written, this character position in the filename contains the letter "t")

xx two-character message type identifier:

"rj" submission rejected

"ir" identification response

"gn" general notification

"al" notify all devices

nnnnn five-digit counter to ensure the uniqueness of message file names

A message file contains the response NIST file.

The client device, unless it uses ftp, must promptly delete all message files upon reading them.

E. EMAIL

This section describes the EMAIL interface based on the Criminal Justice Information Services (CJIS), Electronic Biometric Transmission Specification (EBTS), NIEM Information Exchange Package, BIO-DOC-02261-2.0, March 15, 2010

Steps to be taken before submission is allowed

Contact L-1 Field service with the Livescan ID and the ORI of the new Device that wishes to submit to the generic interface

L-1 field service will:

Create a new mailbox on the Generic Interface mail server in the format of LivescanID@LS-IBIS

Add the Livescan ID to the allowed livescan ID's configuration section of the IBIS Server.

Add the ORI and created email address LivescanID@LS-IBIS to the ORI-Email map configuration section of the IBIS Server

Contact the customer and inform them they can submit to GenericInterface_Inbound@LS-IBIS and receive their results at LivescanID@LS-IBIS

EMAIL Communication

Steps Taken

i. Email is sent to GenericInterface_Inbound@LS-IBIS

ii. Search is submitted by IBIS Server to Sacramento PID system

iii. Results from the search is received from the PID system by the IBIS Server

iv. Results are formatted and sent to the mapped ORI email address.

v. Client picks up the results email from its mailbox of LivescanID@LS-IBIS

F. WEB SERVICE

This section describes the WEB SERVICE interface based on the California Department of Justice, Transaction Router Gateway (TRG), General Information and Technical Specification, Version 1.1, December 22, 2010. The TRG interface has been extended to allow the caller to request the PID XML in addition to the formatted response.

Steps to be taken before submission is allowed

Contact L-1 Field service with the Livescan ID of the new Device that wishes to submit to the generic interface

L-1 field service will:

Add the Livescan ID to the allowed Livescan ID's configuration section of the IBIS Server.

Contact the customer and inform them they can submit to http://IBIS_SERVER:8080/ibar/services/SubmitService

Web Service Communication

Steps Taken

i. The "submit" method is called at http://IBIS_SERVER:8080/ibar/services/SubmitService to inject a search into the IBIS Server

ii. A search is submitted by IBIS Server to Sacramento PID system.

iii. Results from the search are received from the PID system by the IBIS Server

iv. Results are formatted and queued for pickup

v. Client calls the "queryTcn" until a result is returned.
Note: The client can also call the "queryTcnExt" method.

Building a client for the Web Service

A client built from the Gateway.wsdl and Gateway.xsd (described in the California Department of Justice, Transaction Router Gateway (TRG), General Information and Technical Specification, Version 1.1, December 22, 2010) will be able to communicate with the methods "submit" and "queryTcn".

A client built from http://IBIS_SERVER:8080/ibar/services/SubmitService?WSDL will be able to communicate with the methods "submit", "queryTcn" and "queryTcnExt". The method "queryTcnExt" adds a Boolean to allow the caller to select to receive the PID XML in addition to the formatted result.

G. INDICATING THE DATA FORMAT SUBMITTED

A client can submit a NIST file or an EBTS NIEM XML file to the Generic Web Service. The data format is indicated in the "ContentType" of the "Payload" submitted to the Generic Web Service. (For further information on the "ContentType" and "Payload" structures see the California Department of Justice, Transaction Router Gateway (TRG), General Information and Technical Specification, Version 1.1, December 22, 2010)

The Generic Web Service supports the following values for "ContentType":

"text/xml" indicates that an EBTS NIEM XML file is the content of the "Payload". If this is the case the response to this search will also be in EBTS NIEM XML format.

"ansi/nist-itl-1" or "ansi/nist-itl-2" indicates that an NIST file is the content of the "Payload". If this is the case the response will also be in NIST format.

3. HELP DESK SUPPORT

Each Outside Agency should have information technology professionals that can perform trouble shooting steps on their equipment in attempt to resolve client related issues. If the Outside Agency believes the issue to be system wide, technical professionals should contact SSD's help desk at 916-874-4999 during business hours, 0800-1700 Monday through Friday excluding County Holidays. If it is after hours, e-mail can be sent to helpdesk@sacsheriff.com.