ATTACHMENT E

ACN 160888

MEMORANDUM OF UNDERSTANDING AMONG SANDAG-ARJIS AND MEMBER AGENCIES FOR USE AND ACCESS OF REGIONAL DATA IN AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM ENTERPRISE

This Memorandum of Understanding ("MOU" or "Agreement") is made and entered into between the San Diego Association of Governments, a California Public Agency ("SANDAG"), on behalf of the Automated Regional Justice Information System, a California Joint Powers Agency ("ARJIS"), collectively referred to herein as "SANDAG-ARJIS," Contributing Member Agencies ("CMAs") that contribute law enforcement data to the ARJIS Enterprise, and Participating Member Agencies ("PMAs") and is made with reference to the following:

RECITALS

WHEREAS, SANDAG is empowered to enter into this MOU on behalf of ARJIS pursuant to the ARJIS Joint Powers Agreement and the California Public Utilities Code section 132354; and

WHEREAS, the CMAs, as defined in Part I.A. of this MOU, are empowered to enter into this MOU for the sharing of criminal justice information pursuant to California Penal Code Sections 11105 and 13300 and California Government Code Sections 26600, 26602, and 41601, and other statutes; and

WHEREAS, the CMAs asked SANDAG-ARJIS to develop and execute this MOU in order to share law enforcement information stored in the ARJIS Enterprise database, known as the ARJIS Operational Store (AOS) and any other data repository, system, tools or applications residing behind the ARJISNET firewall, (including but not limited to COPLINK, i2 Analyst Notebook, SRFERS (State, Regional, Federal Enterprise Retrieval System), License Plate Reader data, Tactical Identification System (TACIDS), and the COGNOS reporting system), collectively referred to as "ARJIS Enterprise"; and

WHEREAS, the PMAs are ex-officio members of the ARJIS Joint Powers Agency (JPA) with law enforcement responsibilities that can be given permission to query information stored in ARJIS Enterprise, but do not themselves contribute crime and arrest incident data; and

WHEREAS, implementation of this MOU will substantially further the public safety, health, and welfare.

NOW, THEREFORE, it is mutually agreed by and between the undersigned parties as follows:

I. OVERVIEW

A. Background

1. ARJIS hosts a complex law enforcement information system that contains information about a variety of official police incidents generated by the law enforcement agencies in the San Diego region. There are currently eleven CMAs providing crime, arrest, and other incident data to ARJIS (with one of those agencies, the San Diego Sheriff's Department, providing contract services to nine incorporated cities within San Diego County).

2. Additionally there are 55 other ARJIS member agencies that do not currently provide crime and arrest incident data to ARJIS but access ARJIS regional data and utilize ARJIS

services. These additional agencies are referred to as PMAs for the purposes of this Agreement.

3. The regional data maintained by ARJIS includes, but is not limited to, police incidents entered by the CMAs such as crime reports, arrest reports, traffic citations, traffic accidents, and field interviews. These data are maintained in the AOS as part of ARJIS Enterprise. ARJIS Enterprise resides on a private network called ARJISNET, and is protected by firewalls, access control lists, and user authentication. ARJIS meets both the California Department of Justice (CalDOJ), and Federal Bureau of Investigations Criminal Justice Information Services (FBI CJIS) network security standards.

4. The AOS, as the primary ARJIS regional data warehouse for the integration and storage of San Diego regional law enforcement data, is the core component of ARJIS Enterprise designed to share regional law enforcement information. ARJIS regional data originate from the CMAs and are standardized and integrated to provide a comprehensive criminal justice view for the region. Regional data stored in ARJIS Enterprise is used for tactical day-to-day law enforcement activities as well as regional and agency specific analyses. In addition to the regional tools and applications, some CMAs have purchased and/or developed their own applications and have requested global access to the regional ARJIS data to employ these products.

B. Purpose

1. The parties hereby agree that any mutual data access or exchange that occurs among them will be used for the sole purpose of law enforcement investigative analysis and crime analysis.

2. Moreover, the purpose of this MOU is to set forth the policies and the procedures for the sharing of law enforcement information by the participating CMAs and PMAs, including the declaration of ownership, warranties, allocation of liabilities, and policies governing the use of shared information.

C. Acceptable Use Policies

1. SANDAG-ARJIS has adopted, and will continue to adopt and update Acceptable Use Policies (AUPs), which set forth conditions under which ARJIS systems may be accessed and defining how they are maintained. AUPs are not operational policies that govern the use in the field of data obtained using ARJIS systems by law enforcement agencies as those policies are the responsibility of the CMAs and PMAs. The AUPs are prepared with input from ARJIS member agencies and are intended to delineate where the roles and responsibilities of SANDAG-ARJIS end and other agencies' begin. The AUPs also are intended to clarify that SANDAG-ARJIS should not be liable for the conduct of a law enforcement officer in the field. As such, the CMAs and PMAs who are parties to this MOU hereby agree to comply with existing, added and updated AUPs and understand that their respective continued agreement to comply with the AUPs is a condition of continued access to ARJIS Enterprise. The AUPs adopted as of the time of execution of this MOU are attached as MOU Exhibit 1.

2. A copy of proposed amendments to an AUP or any new AUP shall be forwarded by SANDAG-ARJIS to the official representative of each signatory to this MOU at the same time as the proposed amendments are mailed as a report attachment to the agenda for recommendation for approval by the SANDAG Public Safety Committee (PSC). The proposed draft amendment or new AUP also shall be posted on the ARJIS website. The final version of all AUPs shall be posted on the ARJIS website after adoption by the SANDAG Board of Directors.

3. If at any time a CMA or PMA fails to comply with an AUP or indicates that it anticipates or condones non-compliance with an AUP, that party may be deemed in material breach of this MOU by SANDAG-ARJIS.

D. Governance of ARJIS

1. ARJIS is a JPA and is governed by the terms of a joint powers agreement, by any policies passed and adopted by the ARJIS governing board, and by the statutes, rules, regulations, policies or procedures that govern SANDAG. SANDAG serves as the Administrator of the JPA.

2. The ARJIS governing board is the SANDAG Public Safety Committee (PSC), formed under SANDAG Board Policy No. 026, and advises the SANDAG Board of Directors on matters concerning ARJIS and the SANDAG Criminal Justice Division. The Chiefs'/Sheriff's Management Committee is a standing committee established to support the PSC. Each member of the Chiefs'/Sheriff's Management Committee (all are CMAs) has an equal vote; and is authorized to forward recommendations to the PSC on policies and procedures set forth in this MOU.

3. The Chiefs'/Sheriff's Management Committee appoints members to standing working groups known as the Technical and Business working groups. The membership of these working groups is composed of representatives of each of the eleven CMAs. Each member of these working groups has one vote. These working groups forward technical and administrative recommendations to the Chiefs'/Sheriff's Management Committee.

4. Most policy decisions must be made by the SANDAG Board of Directors, including approvals of AUPs. Typically, matters begin in the Chief's/Sheriff's Management Committee, which makes a recommendation to the PSC. The PSC then either makes a final decision or the matter is sent to the SANDAG Board of Directors in accordance with Board Policy No. 026.

5. Pursuant to Government Code Section 6509, which requires that the powers of a JPA be limited by the legal restrictions placed upon a named member of the JPA, the powers of ARJIS are subject to those legal restrictions imposed upon SANDAG by the Constitution of the State of California and the laws governing SANDAG.

II. OWNERSHIP, ENTRY AND MAINTENANCE OF INFORMATION

A. Each CMA retains sole ownership, responsibility and exclusive control and disposition over the content of the information it contributes, and may, at will, at any time, update, correct or delete any of its information in the ARJIS Enterprise entirely. All system entries are identifiable to the CMA that contributes the entries. The content of the information remains the sole responsibility of the CMA that contributed the data, under an express promise of confidentiality.

B. Each CMA shall maintain "system discipline," defined as the maintenance of information in the ARJIS Enterprise that is 1) timely, 2) accurate, 3) complete and 4) relevant. In order to maintain system discipline, contributors shall submit data, including any updates or changes to the original submission, while performing modifications as often as a contributor can feasibly execute them.

C. Each CMA has the sole responsibility for ensuring data entered into the ARJIS Enterprise has been obtained in compliance with federal, state, local, and/or tribal laws. Data must be

pertinent to and within the scope of the authorized law enforcement function of the CMA and meet ARJIS security standards.

D. Each CMA agrees that police incident data entered and/or uploaded to the ARJIS Enterprise is a copy or summary of information stored in and managed by the entering CMA's own records system(s), and that the contributing CMA is solely responsible and accountable for the accuracy and timeliness of the information it has submitted. Each CMA that is the source of the information should make every effort to ensure the contributed data reflects the substance of the source records. The data in ARJIS shall conform to ARJIS validations and standards.

E. ARJIS provides a suite of tools, to all member agencies (CMAs and PMAs) to access the regional data for the purposes of conducting complex investigative analyses and crime analysis functions. In addition, ARJIS provides crime statistics, crime mapping, and other applications to assist ARJIS member agencies and enhance the efficiency and effectiveness of their operations. Although ARJIS makes a good faith effort to ensure these tools, statistics, maps, applications, and all other information it provides to CMAs and PMAs are accurate and that the SANDAG-ARJIS systems are available for use at all times, SANDAG-ARJIS is a conduit for information prepared by others, which relies on the accuracy and timeliness of data prepared by others in order to allow sharing of data among agencies. Therefore, SANDAG-ARJIS disclaims any responsibility for the accuracy, correctness, or timeliness of the data. In no event shall SANDAG-ARJIS become liable to users of these data, or any other party, for any loss or damages, consequential or otherwise, including but not limited to time, money, or goodwill, arising from the use, operation or modification of the data. In using these data, users further agree that SANDAG-ARJIS shall have no liability of any nature arising out of or resulting from the lack of accuracy, correctness, or timeliness of the data, or the use of the data.

F. ARJIS programs may enhance and add value to the incident information provided by the CMA, including such functions as GEO Coding and data classification for UCR (Uniform Crime Reporting) reporting, as well as programmatic links between records and indexes. This added value, generated by the ARJIS programming and codes, is not reflected in the CMA's source data. CMAs will be allowed access to this value-added data through the AOS.

G. ARJIS shall follow the California mandated guidelines and purge most incident records 7 years from the record creation date. There are some record types that are excluded from purging or that are purged more often in accordance with laws or policies specific to record types. These are set forth in relevant AUPs or outlined in the 'Peace Officer Standards and Training Law Enforcement Records Management Guide'[1], which SANDAG-ARJIS shall follow.

H. PMAs may at any time request authorization to contribute crime, arrest, and other incident data to ARJIS. If the request receives a recommendation from the Chiefs'/Sheriff's Management Committee and an approval from the SANDAG Public Safety Committee, which serves as the ARJIS Board of Directors, the PMA may become a CMA for purposes of its treatment under this MOU in accordance with such other terms and conditions that may be required by SANDAG-ARJIS.

III. ACCESS TO, DISCLOSURE AND USE OF INFORMATION

The parties to this MOU agree:

[1] http://lib.post.ca.gov/Publications/Records_Management_Guide.pdf

A. To authorize every other CMA that has signed this MOU access to its law enforcement incident information shared in ARJIS Enterprise.

B. To authorize PMAs that have signed this MOU to access and utilize ARJIS regional data only via the established ARJIS applications such as COPLINK; PMAs may not extract, export, or use the ARJIS regional data with their own applications. There may be instances where some or all of the ARJIS regional data is requested by PMAs. These requests must be made using the ARJIS Data Request Form (Exhibit 2). The ARJIS Director will review each request on a case-by-case basis. A summary of data requests received will be provided as part of the quarterly ARJIS Management Report to the Chiefs'/Sheriff's Management Committee and the SANDAG Public Safety Committee, which serves as the ARJIS Board of Directors. PMAs also may request data extracts for a variety of purposes to include special studies, special analyses for specific investigations, and/or to populate an application not residing at ARJIS using this process.

C. To ensure that the use of ARJIS regional data is in accordance with applicable federal, state, and local statutes and complies with FBI CJIS Security policies, and CalDOJ Practices, Policies, and Procedures.

D. To authorize agency personnel access to ARJIS regional data, only after receiving appropriate training, and only when personnel have a legitimate need to know the information for an authorized and legal law enforcement purpose. Specifically, ARJIS regional data may be used to develop investigative and crime analyses.

E. That under no circumstance is a CMA or PMA to publicly report statistics using data from another jurisdiction obtained through operation of this MOU without prior written authorization from the CMA(s) which own(s) the data. This includes statistics of any kind for the entire jurisdiction or part of the jurisdiction; Uniform Crime Reporting (UCR) statistics and non-UCR statistics; and internal studies, published studies, maps or grant projects.

F. That the California Public Records Act (CPRA), commencing at Section 6250 of the Government Code, and other applicable statutes and case law, provides for public inspection and copying of "public records." The CPRA also identifies various records that are exempt from disclosure, including many related to law enforcement and public safety. These include, but are not limited to records of investigations, security information, critical infrastructure information, peace officer records, criminal offender records, and the names and addresses of victims of specified crimes.

G. That each CMA or PMA that receives a request for data or information, whether via a CPRA request or otherwise, that it has obtained via access through ARJIS, but which it does not own or is not the originating source, shall not release that information or data, but may refer the requestor to the CMA that is the source. Any CMA or PMA that receives a court order to release information in the ARJIS Enterprise which originated from another CMA shall (a) immediately provide a copy of the court order to the CMA that originated the information and to their Agency California Law Enforcement Telecommunications System (CLETS) Coordinator (ACC) or their designate and (b) request input from the originating CMA regarding the nature of any objections it feels it would be appropriate to make to the court; and 3) submit to the court in a timely manner all reasonable objections to the provisions of the underlying request. The originating agency shall reimburse the court ordered CMA or PMA all reasonable costs associated with the challenge or objection to the order that are not reimbursable by the requester within thirty days of being provided a detailed invoice of costs.

H. Language in Section 18(b) of the ARJIS Joint Powers Agreement provides that SANDAG-ARJIS does not own the records of the ARJIS member agencies and may not disclose ARJIS member agency records without their permission:

If pursuant to agreement, SANDAG-ARJIS serves as custodian of data it does not own, that data shall presumptively remain the property of the contributing entity and may not be treated as a public record. The ARJIS may not disclose electronic data or other intellectual property for which it is a custodian to third parties without the approval of the entity that owns the property.

The CPRA, however, generally provides that records prepared, owned, used, **or** retained by an agency such as SANDAG-ARJIS can be public records and as a result SANDAG-ARJIS receives records requests for records it does not own, but has retained. The Parties agree that SANDAG-ARJIS shall not have liability for Claims (as defined in Section VIII) arising from it providing responses to public records requests for records that are housed on SANDAG-ARJIS servers, but that were created and are owned by other agencies ("Non-SANDAG Records"). SANDAG-ARJIS does retain Non-SANDAG Records in its role as the Administrator, but it does not prepare, own or have the right to control the use of the records with regard to disclosure to non-parties, either directly or through another person. Accordingly the costs and liabilities associated with producing or refusing to produce Non-SANDAG Records should fall to the owner(s) of those records rather than SANDAG-ARJIS. Furthermore, pursuant to Government Code sections 6254(f) and 6255, ARJIS regional records should qualify for exemptions from the CPRA.

In the event SANDAG-ARJIS receives a request for records or information owned by a CMA, whether via a CPRA request or otherwise, it shall follow these procedures:

1. SANDAG-ARJIS will contact the Agency CLETS Coordinator (ACC) or his/her designate for the owner of the Non-SANDAG Records and request that the owner provide a written response to SANDAG-ARJIS within three business days regarding whether to provide the records, or withhold the records based one or more statutory exemptions that shall be identified by the CMA.

2. SANDAG shall respond based on the record owner's discretion and direction. Notwithstanding the foregoing sentence if the owner does not respond within the timeframe requested by SANDAG-ARJIS or the records requested belong to more than one owner and the owners are not unanimous in the direction provided to SANAG-ARJIS, SANDAG-ARJIS will exercise its own discretion regarding whether to release the Non-SANDAG Records.

3. If SANDAG-ARJIS does not release some or all of the Non-SANDAG Records and SANDAG-ARJIS receives a court order to release records or information in the ARJIS Enterprise that originated from a CMA SANDAG-ARJIS shall (a) immediately provide a copy of the court order to the CMA that originated the information and to its ACC or designate and (b) request input from the originating CMA regarding the nature of any objections it feels it would be appropriate to make to the court; and 3) submit to the court in a timely manner all reasonable objections to the provisions of the underlying request. The originating CMA shall reimburse SANDAG-ARJIS all reasonable costs associated with the challenge or objection to the order within thirty days of being provided a detailed invoice of costs. In the event SANDAG-ARJIS is a party to litigation due to a public records request or its conduct taken in accordance with this section of this MOU, the provisions of Section VIII (B)(4) shall apply.

IV. USER ACCESS

A. Login Application Process

Each CMA and PMA shall appoint its own ACC (or their designate) who is responsible for management of user accounts at that CMA or PMA. An overall agency-specific Network System Administrator also will be identified to assist with any ARJISNET network issues. In order to access ARJIS regional data and any of the ARJIS applications, each user must submit a request for a user login identification ("login ID") and password to their Agency ACC (or their designate). Each CMA and PMA agrees that for use of all ARJIS regional data and applications, users shall meet the guidelines specified in Section V.C. of this document and be authorized to access and review police incident data for legitimate purposes. The ACC (or their designate) may deny or revoke individual access in their sole discretion.

B. Login Assignment

Each individual user of ARJIS regional data at a CMA and PMA will be issued a login ID and a default password by their ACC (or their designate). Users also may be assigned to groups that have different access rights to the information in the system based on the level of restriction of the information.

C. Provisions of Policy

Each agency shall be responsible for ensuring each of their authorized users knows the terms and conditions of this MOU. Each CMA and PMA shall require each of its users to agree to comply with the provisions of the SANDAG-ARJIS AUPs prior to being granted access to any ARJIS databases.

D. Audit Trail

1. For each CMA or PMA accessing ARJIS regional data directly, each transaction will be logged and an audit trail created and maintained by SANDAG-ARJIS for a minimum of three years, in conformance with the CalDOJ Policies, Practices, and Procedures, attached hereto as MOU Exhibit 2. All monitoring of successful and unsuccessful ARJIS logon attempts, file access, correlations, transaction types, and password changes will be established and maintained by SANDAG-ARJIS regardless of access means. All audit trail files shall be protected to prevent unauthorized changes or destruction. Requests for audits shall be made in writing through the requestor's chain-of-command to their ACC (or their designate), and forwarded to SANDAG-ARJIS for processing.

2. Each CMA and PMA receiving an export of ARJIS data to utilize through its own applications, will be responsible for providing audit capabilities that meet the Cal DOJ Policies, Practices, and Procedures, and will maintain the audit logs for a minimum of three years. This will include making available the activity history for individual users when a request is made in writing through the requestor's chain-of-command to their ACC (or their designate). CMAs and PMAs must ensure that all audit trail files will be protected to prevent unauthorized changes, unauthorized destruction and unauthorized dissemination.

E. Termination of Logins

CMAs and PMAs, through their ACCs (or their designates) will be responsible for immediate suspension and/or removal of any login accounts of users who leave the CMAs or PMAs employment, face disciplinary action, or have failed to meet the requirements for access to the Login Application Process.

V. SECURITY

A. All CMAs must comply with the CalDOJ and FBI CJIS practices, policies, procedures, and guidelines as they relate to the access and use of justice data, when applicable.

B. Each CMA and PMA will be responsible for designating the employees who should have access to ARJIS regional data. This MOU was developed with security in mind, and each CMA and PMA should ensure that access to system information is in accordance with Section III.C-D and all other provisions of this MOU, and that all information is treated as law enforcement sensitive.

C. Each CMA and PMA agrees to use the same degree of care in protecting the information accessed under this MOU that it exercises for its own sensitive information. Each CMA and PMA agrees to restrict access to such information to only its officers, employees, detailees, agents, representatives, task force members, contractors/subcontractors, consultants, or advisors with a "need to know" such information for the performance of their duties and only to the extent permitted by law. Each of these persons will have passed background clearances and met all requirements as required by local, state and federal statute to allow access and use of the secured data. These requirements also apply to SANDAG-ARJIS and its officers, employees, agents, representatives, contractors/subcontractors, consultants, or advisors with a need to know such information.

D. CMAs and PMAs are responsible for training those users authorized to access ARJIS regional data on the use and dissemination of information obtained from the system (for example, CORI). Specifically, users must have a clear understanding of the need to verify the reliability of information with the source agency that contributed the information, when using the information for purposes such as obtaining search and arrest warrants, affidavits, subpoenas, etc. Parties must also fully brief accessing users regarding the proscriptions for using third party information.

VI. SYSTEM ACCESS

A. Network Access

Access to ARJIS regional data will be provided utilizing the secure ARJISNET network. All CMAs and PMAs are to ensure that all end user and sub-administrator workstations accessing ARJIS regional data and/or servers that CMAs and PMAs utilize to store ARJIS regional data shall utilize recognized industry-standard anti-virus, firewall, and user authentication software. Terminals that access the ARJISNET network should follow the same guidelines required by CLETS.

B. System Availability

The ARJIS regional data will be available on a 24-hour-a-day, 7-days-a-week basis with downtime limited to those hours required for any necessary system maintenance activities. The parties agree to inform each other in advance, whenever possible, of scheduled system downtimes. In cases of unscheduled outages, all efforts will be made to make notice to all users and parties that the outage has occurred (including estimated outage length) and notice will be given when applications have been returned to normal operation.

VII. SANCTIONS

A. Violation of an AUP or of any law or regulation applicable to access to or use of ARJIS Enterprise or ARJIS regional data (hereinafter referred to as "Misuse") by a party to this MOU

or one of its staff or agents, whether authorized or unauthorized, may lead to suspension or termination of an agency or particular user's access to ARJIS Enterprise.

B. In the event a party to this MOU discovers suspected or actual Misuse of ARJIS Enterprise or ARJIS regional data, it will immediately inform the Director of ARJIS, who will in turn immediately notify the SANDAG Director of Technical Services and SANDAG Executive Director. In the event SANDAG-ARJIS discovers suspected or actual misuse of ARJIS Enterprise, the Director of ARJIS will immediately notify the SANDAG Director of Technical Services, the SANDAG Executive Director, and the member agency. The SANDAG Director of Technical Services, in consultation with the Director of ARJIS or their designees, and with input from the subject CMA or PMA, will determine whether to suspend or terminate access and if so for whom the suspension or termination will apply and will notify the affected member agency. The affected member agency will be notified of the decision by SANDAG-ARJIS and then will have 10 calendar days to appeal the decision to the SANDAG Executive Director. The Executive Director shall have final decision-making authority, however, such decision shall be reported out to, and subject to ratification or modification by, the PSC at its next regular meeting.

C. Any supervisor, law enforcement officer, employee, agent, representative, task force member, contractor/subcontractor, or consultant, who by virtue of his employment or official position, has possession of, or access to, ARJIS regional data that contain individually identifiable information, the disclosure of which is prohibited by law, agreement, this MOU, the AUPs, rules, or regulation and who, knowing that the disclosure of the information is prohibited, willfully or recklessly discloses the material in any matter, including oral communication, may be prosecuted or fined under any applicable federal or state law, or may be subject to administrative or disciplinary action by their member agency.

D. An individual CMA's or PMA's participation in this MOU also may be terminated involuntarily by a decision of the SANDAG Board of Directors for repeated failures to meet the terms of this MOU or an AUP. The terminated CMA or PMA will continue participation, financial or otherwise, up to the effective date of termination.

VIII. INDEMNIFICATION

A. Indemnification Related to Workers Compensation and Employment Issues

1. CMAs and PMAs, and each of them (which for purposes of this Section VIII, shall include their officers, officials and employees), shall fully indemnify and hold harmless SANDAG-ARJIS, its officers, employees and agents, from any claims, losses, fines, expenses (including reasonable attorneys' fees and court costs or arbitration costs), costs, damages or liabilities arising from or related to (1) any workers' compensation claim or demand or other workers compensation proceeding arising from or related to, or claimed to arise from or relate to, employment which is brought by an employee of CMAs or PMAs, or each of them, or any contract labor provider retained by CMAs or PMAs, or each of them, or (2) any claim, demand, suit or other proceeding arising from or related to, or claimed to arise from or relate to, the status of employment (including without limitation compensation, demotion, promotion, discipline, termination, hiring, work assignment, transfer, disability, leave or other such matters), which is brought by an employee of a CMAs or PMAs, or each of them, or any contract labor provider retained by a CMAs or PMAs, or each of them.

2. SANDAG-ARJIS (which for purposes of this Section VIII shall include its officers, officials and employees) shall fully indemnify and hold harmless CMAs or PMAs, or each of them, its officers, employees and agents, from any claims, losses, fines, expenses (including reasonable attorneys' fees and court costs or arbitration costs), costs, damages or liabilities arising from or related to (1) any workers' compensation claim or demand or

other workers compensation proceeding arising from or related to, or claimed to arise from or relate to, employment, which is brought by an employee of SANDAG-ARJIS or any contract labor provider retained by SANDAG-ARJIS, or (2) any claim, demand, suit or other proceeding arising from or related to, or claimed to arise from or relate to, the status of employment (including without limitation compensation, demotion, promotion, discipline, termination, hiring, work assignment, transfer, disability, leave or other such matters), which is brought by an employee of SANDAG-ARJIS or any contract labor provider retained by SANDAG-ARJIS.

B. Defense And Indemnity; Acts And Omissions

1. Claims, Actions or Proceedings Arising From Acts or Omissions of One or More CMAs or PMAs

   Each CMA and PMA hereby agrees to defend and indemnify SANDAG-ARJIS, its agents, officers and employees, from any claim, action or proceeding against SANDAG-ARJIS, arising out of the acts or omissions of said CMA or PMA, its agents, officers or employees in the performance of this MOU, and all expenses of investigating and defending against same, provided, however, that a CMA's or PMA's duty to indemnify and hold harmless shall not include any claim or liability arising from the established sole negligence or willful misconduct of SANDAG-ARJIS, its agents, officers or employees. At its sole discretion, SANDAG-ARJIS may participate at its own expense in the defense of any claim, action or proceeding, but such participation shall not relieve the CMA or PMA of any obligation imposed by this MOU. SANDAG-ARJIS shall notify affected CMA(s) or PMA(s) promptly of any claim, action or proceeding and cooperate fully in the defense.

2. Claims, Actions or Proceedings Arising From Acts or Omissions of SANDAG-ARJIS

   SANDAG-ARJIS hereby agrees to defend and indemnify the CMAs and PMAs, their agents, officers and employees, from any claim, action or proceeding against one or more CMAs or PMAs, arising out of the acts or omissions of SANDAG-ARJIS, its agents, officers or employees in the performance of this MOU, and all expenses of investigating and defending against same with the limitations described in subsection B(4), provided, however, that SANDAG-ARJIS's duty to indemnify and hold harmless shall not include any claim or liability arising from the established sole negligence or willful misconduct of CMAs or PMAs, or their agents, officers or employees. At its sole discretion, an affected CMA or PMA may participate at its own expense in the defense of any claim, action or proceeding, but such participation shall not relieve SANDAG-ARJIS of any obligation imposed by this MOU. CMA or PMA shall notify SANDAG-ARJIS promptly of any claim, action or proceeding and cooperate fully in the defense.

3. Claims, Actions or Proceedings Arising From Concurrent Acts or Omissions

   CMAs and PMAs hereby agrees to defend themselves, and SANDAG-ARJIS hereby agrees to defend itself, from any claim, action or proceeding arising out of the concurrent acts or omissions of one or more CMAs or PMAs and SANDAG-ARJIS with the limitation described in subsection B(4). In such cases, CMAs, PMAs and SANDAG-ARJIS agree to retain their own legal counsel, bear their own defense costs, and waive their right to seek reimbursement of such costs, except as provided in subsection 5 below (referring to joint defense agreements and reimbursement and/or reallocation).

4. Presumption of Defense And Indemnification of SANDAG-ARJIS by CMA(s) or PMA(s) When SANDAG-ARJIS Is Named As a Party to a Claim, Action or Proceeding In Certain Circumstances

The relevant CMAs or PMAs shall indemnify, defend, and hold SANDAG-ARJIS harmless where the asserted SANDAG-ARJIS liability is based on one or more of the following three circumstances:

(1) A third-party sues SANDAG-ARJIS based on its contractual relationship with the CMAs and PMAs under this MOU;

(2) A third-party sues SANDAG-ARJIS due to its possession or use of records or information owned or originated by one or more CMAs or PMAs;

(3) The conduct alleged to be that of the SANDAG-ARJIS is, in fact, the conduct of one or more CMAs or PMAs.

Unless there is a conflict of interest as between SANDAG-ARJIS and the relevant CMA(s)/PMA(s): the relevant CMA(s)/PMA(s) shall control litigation strategy and selection and retention of defense counsel; the relevant CMA(s)/PMA(s) shall keep SANDAG-ARJIS's Office of General Counsel apprised of the status of the matter, which shall include advance discussion of any proposed terms of settlement; and SANDAG-ARJIS shall reasonably cooperate in the defense.

5. Joint Defense

Notwithstanding subsection 3 above, in cases where one or more CMAs or PMAs and SANDAG-ARJIS agree in writing to a joint defense, CMAs, PMAs and SANDAG-ARJIS may appoint joint defense counsel to defend the claim, action or proceeding arising out of the concurrent acts or omissions of SANDAG-ARJIS, CMAs and PMAs. Joint defense counsel shall be selected by mutual agreement of the effected parties. The affected parties agree to share the costs of such joint defense and any agreed settlement in equal amounts, except that the parties further agree that none of the parties to the joint defense may bind the other(s) to a settlement agreement without the written consent of the other(s). Additionally, where a trial verdict or arbitration award, in a joint defense case, allocates or determines the comparative fault of the parties, the parties may seek reimbursement and/or reallocation of defense costs, judgments and awards, consistent with such comparative fault.

IX. DISPUTE RESOLUTION

Disputes among any of the parties arising under or relating to this MOU shall be resolved via consultation at the lowest practicable level by and between the affected parties and sponsoring agencies (or as otherwise may be provided under any separate governance procedures). If such parties are unable to resolve their dispute at the lowest practicable level, the dispute shall be referred to the PSC for a resolution. If the PSC is unable to resolve the dispute, the matter shall be referred to the SANDAG Board of Directors. Only if the PSC and Board of Directors are unable to resolve the parties' dispute may the disputing parties seek judicial resolution of their dispute. Each affected party will pay the fees of its respective legal counsel, accountants, advisors, etc., as well as all of its respective out-of-pocket costs and expenses.

X. OPERATING COSTS

A. Unless otherwise provided herein or in a supplementary writing, each CMA and PMA shall bear its own costs in relation to this MOU and continued participation in or access to ARJIS Enterprise System is conditioned upon timely payment of those costs by each CMA and PMA. Even in circumstances in which a party has agreed (or later does agree) to assume a particular financial responsibility outside of those responsibilities covered by this MOU, the affected party's express written approval must be obtained before the incurring by another of each expense associated with the responsibility. All obligations of and expenditures by the parties

will be subject to their respective budgetary and fiscal processes and subject to availability of funds pursuant to all laws, regulations, and policies applicable thereto. The parties expressly acknowledge that this MOU in no way implies that any funds have been, or will be appropriated for such expenditures.

B. Any ARJIS system enhancements, modifications, updates, or implementation of new features to enhance regional ARJIS applications must be reflected either in the annual SANDAG-ARJIS overall work plan and budget, or in an amendment thereto. After approval by the PSC and if necessary the SANDAG Board of Directors, costs associated with these enhancements will be billed to CMAs and PMAs in accordance to criteria set forth in the ARJIS Joint Powers Agreement. Invoices will include reasonable documentation explaining the expenses incurred.

XI. TERM OF AGREEMENT

A. This MOU shall be effective as of the last signature date of at least five of the CMAs and will be reviewed every three years thereafter for updates and consistency with applicable statutes and policies.

B. For parties who join subsequent to the date in Section I(B)(1), this MOU shall become effective when it has been signed by the parties' duly authorized representatives and countersigned by SANDAG-ARJIS.

C. In the event that one or more CMAs or PMAs withdraw their participation from this MOU and are no longer parties to this Agreement, this MOU shall survive and continue to be fully effective and will bind the parties that remain signatories.

D. The MOU will terminate automatically when all members have withdrawn their participation from the MOU.

E. Upon termination for cause or convenience, the terminated party's access to ARJIS Enterprise and ARJIS regional data also shall be terminated.

F. 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.

XII. VOLUNTARY WITHDRAWAL OF MEMBERSHIP

Any CMA or PMA may withdraw from this MOU upon ninety (90) days written notice to the PSC. All rights, obligations, responsibilities, limitations, and other understandings with respect to the disclosure and use of all information received during a CMAs or PMAs participation in this MOU shall survive any termination.

XIII. AMENDMENT OF MOU

This MOU may be amended by a written document signed by all parties. No oral understanding or agreement shall be binding on the parties.

XIV. SEVERABILITY

This MOU is subject to all applicable laws and regulations. If any provision of this MOU is found by any court or other legal authority, or is agreed upon by the parties, to be in conflict with any law or regulation, then the conflicting provision shall be considered null and void. If the effect of nullifying any conflicting provision is such that a material benefit of this MOU to either party is lost,

then the MOU may be terminated at the option of the affected party, with the notice as required in this MOU. In all other cases, the remainder of this MOU shall be severable and shall continue in full force and effect.

XV. NO THIRD-PARTY BENEFICIARIES

This MOU is intended solely for the benefit of the parties to this MOU. Any benefit to any third party is incidental and does not confer on any third party to this MOU any rights whatsoever regarding the performance of this MOU. Any attempt to enforce provisions of this MOU by third parties is specifically prohibited.

XVI. WAIVER

A waiver by a party of a breach of any of the covenants to be performed by party shall not be construed as a waiver of any succeeding breach of the same or other covenants, agreements, restrictions, or conditions of this MOU. In addition, the failure of either party to insist upon strict compliance with any provision of this MOU shall not be considered a waiver of any right to do so, whether for that breach or any subsequent breach. The acceptance by a party of either performance or payment shall not be considered a waiver of the other party's preceding breach of this MOU.

XVII. AUTHORITY OF SIGNATORY TO BIND ENTITY

By signing below, each signatory warrants and represents that he/she executed this MOU in his/her authorized capacity and that by his/her signature on this MOU, he/she has the legal authority, or has received such authority from the entity, to bind the entity upon whose behalf he/she executed this MOU.

We the undersigned hereby agree, on behalf of our respective offices, agencies, districts and departments, to this Memorandum of Understanding and certify that the agreement made herein will be honored.

This Memorandum of Understanding may be executed in counterparts.

IN WITNESS WHEREOF, the parties have executed this Memorandum of Understanding by the signatures of the duly authorized representative of each CMA and PMA on the dates indicated. A photocopy or facsimile signature is as valid as the original.

SANDAG-ARJIS

_____ _____

Gary L. Gallegos, Executive Director
SANDAG-ARJIS

Date

_____ _____

Julie Wiley, Special Counsel
SANDAG-ARJIS

Date

City of Carlsbad

Title:
City of Carlsbad

Date

City Attorney
City of Carlsbad

Date

City of Coronado

Title:
City of Coronado

Date

City Attorney
City of Coronado

Date

City of Chula Vista

D. [signature]

Title: POLICE CHIEF
City of Chula Vista

7-19-16
Date

City Attorney
City of Chula Vista

Date

City of El Cajon

Title:
City of El Cajon

Date

City Attorney
City of El Cajon

Date

City of Escondido

_____ _____

Title: Date
City of Carlsbad

_____ _____

City Attorney Date
City of Carlsbad

City of La Mesa

_____ _____

Title: Date
City of La Mesa

_____ _____

City Attorney Date
City of La Mesa

City of National City

_____ _____

Title: Date
City of Nation City

_____ _____

City Attorney Date
City of National City

City of Oceanside

Title:
City of Oceanside

Date

City Attorney
City of Oceanside

Date

Unified Port of San Diego

Title:
Unified Port of San Diego

Date

Attorney
Unified Port of San Diego

Date

County of San Diego

Title:
County of San Diego

Date

County Counsel
County of San Diego

Date

City of San Diego

_____ _____

Title: Date
City of San Diego

_____ _____

City Attorney Date
City of San Diego

PMA signature pages to follow

Automated Regional Justice Information System (ARJIS)
Acceptable Use Policy for
Facial Recognition

Revised: 02/13/2015

A. STATEMENT OF PURPOSE

The purpose of this document is to outline the responsibilities of the Automated Regional Justice Information System (ARJIS) in its role as a law enforcement information technology services provider for mobile facial recognition efforts in San Diego County. ARJIS has implemented a regional facial recognition system known as Tactical Identification System (TACIDS) in support of law enforcement efforts to enhance positive identification and improve public safety.

ARJIS provides the secure network infrastructure, technical standards, security protocols, controlled access, database administration, and configuration of mobile devices for access to this system. Included in the support of the secure infrastructure are ongoing system procedures, maintenance, user access, and security monitoring of the circuits, hubs, routers, firewalls, databases, etc. These components that comprise the ARJIS Enterprise ensure the priority, integrity, and availability of services to authorized law enforcement users. This Acceptable Use Policy sets forth rules restricting how TACIDS may be accessed and defines how it is maintained by ARJIS.

The Regional Facial Recognition Operational Protocol under development by the San Diego County Chiefs' and Sheriff's Association outlines facial recognition best practices and standard operating procedures for those agencies that utilize facial recognition in the field.

B. FACIAL RECOGNITION OVERVIEW

Facial recognition refers to an automated process of matching facial images, utilizing algorithms and biometric scanning technologies. A biometric indicator is any human physical or biological feature that can be measured and used for the purpose of automated or semi-automated identification.

During enrollment, the facial recognition system acquires a facial image and measures distinctive characteristics including but not limited to the distance between the eyes, width of the nose, and the depth of the eye sockets. These characteristics are known as nodal points and each human face has multiple nodal points recognizable by facial recognition software.

The nodal points are extracted from the facial image and are transformed through the use of algorithms into a unique file called a template. A template is a reduced set of data that represents the unique features of the enrolled person's face. For identification purposes, the facial recognition system compares the biometric template created from the image captured in the field with all biometric templates stored in the database. For verification purposes, the biometric template of the claimed identity will be retrieved from the database and compared with the biometric template data created from the recently captured facial image.

1. Specification of Use

There are two primary objectives of the TACIDS application. The first is assisting in the identification of individuals who have been detained based on reasonable suspicion, and are lacking and/ or not forthcoming with their identification, or who appear to be using someone else's identification or a false identification. Often times, these situations require officers to escort individuals to a police station to verify their identification. This is a time consuming process that involves taking police resources off the streets which can impact resource

availability and subsequent response time. TACIDS enhances field operations in these cases. The second objective is to assist in identifying persons who are incapacitated or otherwise unable to provide identification, including deceased or incapacitated individuals.

Officers from authorized agencies use an ARJIS enabled tablet or smartphone to access TACIDS to take a photograph of the individual. Once the photo has been submitted to TACIDS, a biometric algorithm compares the image to the local San Diego booking database (currently about 1.4 million images) and potential matches are returned within 10 to 15 seconds, in ranked order, based on the confidence level of the match.

The confidence score is mathematically calculated based on the accuracy of the biometric algorithm. If the system determines that there are potential matches, the photo captured in the field and the matching booking photos can be viewed side by side to further assist the officer in determining whether there is an actual match. Data from the booking records are displayed along with the images to assist the officer in identifying the individual.

All potential matches are considered advisory in nature and any subsequent verification of the individual's identify and/or follow-on action should be based on an agency's standard operating procedures.

2. Privacy and Data Quality

2a. Privacy

Prior to the implementation of TACIDS, in December 2010, ARJIS participated in a Privacy Impact Assessment (PIA) effort led by the International Justice and Public Safety Network, in cooperation with the United States Department of Homeland Security. This effort involved the review of existing local, state, and federal laws, and the resulting PIA contributed to the development of this Policy.

Access to and use of TACIDS data is for official law enforcement purposes only. Accessing and/or releasing data from TACIDS for non-law enforcement purposes is prohibited. TACIDS data access and use is governed by the California Department of Justice (CalDOJ) California Law Enforcement Telecommunications System (CLETS) Polices, Practices and Procedures (PPP) (current rev. 09/2014), via a Master Control Agreement (MCA) between the San Diego County Sheriff's Department (Sheriff) and ARJIS. The CLETS PPP further references the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (current rev. 5.3, 8/4/2014).

2b. Source Data and Photo Enrollment Method

ARJIS relies on the Sheriff's booking system to provide the booking images and associated data fields that are utilized in the system for matching of field-generated photos. The booking images conform to National Institute of Standards and Technology standards. Each booking photo is enrolled by utilizing a complex mathematical algorithm to convert the photo into a set of alphanumeric characters that represent the features on the subject's face. These photos are received daily from the Sheriff through a secure automated interface. The photos are stored in a regional database, hosted, and

maintained by ARJIS. Only select ARJIS authorized technical staff has access to the booking photo database.

3. Data Limitation

The TACIDS system exists for the sole purpose of identifying individuals for authorized public safety purposes. The photographs taken in the field are matched only against the Sheriff's booking photo database. No other databases, such as drivers' licenses photo databases, are linked to or accessible via TACIDS. In addition there is no interface of TACIDS to any form of video surveillance.

4. Performance Evaluation

In addition to audit reports, ARJIS staff regularly monitors the TACIDS system for performance, reliability, and functionality. Staff also provides system generated management reports for the participating agencies that highlight agency use, the number of matches with a 90 percent or better confidence rating, and any technical issues identified during the reporting period. Other system-generated reports are produced on an as-needed basis.

5. Transparency and Notice

ARJIS is a Joint Powers Agency governed by the San Diego Association of Governments (SANDAG) Public Safety Committee, which includes elected officials representing the subregions of San Diego County and public safety officials.

The acquisition of TACIDS was a competitively bid procurement. A PIA was completed and published prior to implementation of TACIDS.

This policy, the associated PIA, and other governing documents are currently posted on the ARJIS website – ARJIS.org.

6. Security

ARJIS is responsible for the maintenance of the TACIDS server, software upgrades, network infrastructure, and the coordination of system access.

TACIDS is hosted within the ARJIS secure infrastructure and is physically located in a secured law enforcement facility with multiple layers of physical security and 24/7 security protections. Physical access is limited to authorized personnel that have completed background investigations and completed the relevant FBI CJIS training.

ARJIS utilizes strong multi-factor authentication, encrypted communications, firewalls, and other reasonable physical, technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system.

ARJIS meets both the CalDOJ CLETS and FBI CJIS Security Policies, which include certified FIPS 140.2 compliance (U.S. Government computer security standard), antivirus, and mobile device management software. The ARJIS mobile platform currently provides a set of statically

assigned IP address blocks to each regional agency, and working with the mobile data partners, ARJIS has established a Mobile Provider Network (MPN).

The MPN solution provides a pathway for any device that is provisioned with the ARJIS MPN configuration to directly connect and route data from the mobile device, to the carrier's cellular tower and straight through to the ARJIS network, without interruption. ARJIS chose to use statically assigned IP addresses specifically to address any potential security concerns and to maintain the most complete control over the network and data security. This also provides ARJIS with the ability to control the flow of data traffic to the device.

Effectively, ARJIS considers any device provisioned within the ARJIS MPN solution to be a client device, and as such maintains several layers of security that allow ARJIS to stop, re-route, or terminate service to any one agency at any time, while continuing to provide service to other participating agencies. Since ARJIS is responsible for device configuration and IP assignment, ARJIS is able to immediately suspend or terminate a device without relying on mobile carriers to make changes.

7. Retention, Access, and Use Of Facial Recognition Data

7a. Retention

Data retained within TACIDS includes the following, with corresponding retention periods:

1. Initial booking records, including booking photos that are sent by the Sheriff – this data is owned and managed by the Sheriff, who sets its retention schedule

2. Internal roster of system users – continually maintained and updated as users are added/deleted

3. Activity logs – retained for a minimum of three years

4. Images on mobile devices - deleted per the law enforcement agencies' Regional Facial Recognition Operational Protocol schedule (currently proposed at 24 hours)

7b. Requirements for All Users Accessing TACIDS

Prior to utilizing TACIDS an agency must comply with the following:

- Be an ARJIS public safety member agency
- Be a CLETS-certified agency
- Comply with applicable FBI CJIS security policies
- Designate a security officer, responsible for authorizing system access and managing user accounts

Only those authorized law enforcement personnel who have met the minimum requirements of completing CLETS certification, FBI CJIS Security Awareness Training, and background checks required for access to criminal justice data may access TACIDS. Authorization is managed by each agency's security officer.

Authorized users must have an ARJIS account and are mandated to follow the procedures for establishing complex passwords that must be changed every 90 days. TACIDS users are required to sign an agreement upon issuance of a TACIDS-enabled device certifying that they have read and will comply with this Policy. All access and use is logged and subject to audit in accordance with the procedures outlined in the audit section below.

7c. Use of TACIDS Data

TACIDS is to be used solely to assist law enforcement officers in the identification of individuals consistent with the Specification of Use set forth above.

Potential matches presented by TACIDS are considered advisory in nature and any subsequent verification of the individual's identify and/or follow-on action should be based on an agency's standard operating procedures.

8. Auditing and Accountability

TACIDS also includes preset queries to the database for auditing and other tracking functions. Capabilities include: tracking accounts, general usage, session logs, enrolled devices, and other key system components.

Access to, and use of, facial recognition data is logged for audit purposes. Audit logs shall be maintained for a minimum of three years. Audit reports are structured in a format that is understandable and useful and will contain at minimum:

- The name and ARJIS ID of the law enforcement user;
- The name of the agency employing the user;
- The date and time of access
- A copy of the biometric template created at the time of the photo capture

ARJIS will provide specific information regarding individual access and query upon request from the associated member agency. Identifying and addressing intentional misconduct is the responsibility of the individual agency. Notwithstanding the agency's responsibility with regard to misconduct, ARJIS reserves the right to enforce this Policy as described below.

9. Enforcement of Policy

Violation of this Policy by an ARJIS member agency or its staff may lead to suspension or termination of an agency or particular agency staff person's access to TACIDS. In the event a

member agency discovers suspected or actual misuse of TACIDS, it will immediately inform the Director of ARJIS, who will in turn immediately notify the SANDAG Director of Technical Services and SANDAG Executive Director. In the event ARJIS discovers suspected or actual misuse of TACIDS, the Director of ARJIS will immediately notify the SANDAG Director of Technical Services, the SANDAG Executive Director, and the member agency. The Technical Services Director, in consultation with the Director of ARJIS, or their designees, will determine whether to suspend or terminate access and if so for whom the suspension or termination will apply and will notify the affected member agency. The affected member agency will be notified of the decision by SANDAG and then will have 10 calendar days to appeal the decision to the SANDAG Executive Director. The Executive Director shall have final decision-making authority.

10. Policy Revisions

The Acceptable Use Policy for Facial Recognition will be brought to the SANDAG Public Safety Committee and the SANDAG Board of Directors at least once per year for review and determination regarding the need for amendments.

Updates regarding the TACIDS system will be provided to the SANDAG Public Safety and Chiefs'/Sheriff's Management Committees annually or upon request.

11. Indemnification

Each user of the TACIDS system (User) agrees to indemnify and hold SANDAG and ARJIS, and each of their personnel, harmless from any claim or demand, including reasonable attorneys' fees, made by any third-party in connection with or arising out of use of the TACIDS system, User's violation of any terms or conditions of this Policy, User's violation of applicable laws, regulations or other policies, or User's violation of any rights of another person or entity. The term "Users" is defined to include each agency accessing the TACIDS system, as well as each individual person with access to the TACIDS system.

Automated Regional Justice Information System (ARJIS)
Acceptable Use Policy for the Regional License Plate Reader System

A. STATEMENT OF PURPOSE

The purpose of this document is to outline the responsibilities of the Automated Regional Justice Information System (ARJIS) in its role as a law enforcement information technology provider for the Regional License Plate Reader (LPR) data storage system (LPR system). ARJIS, in cooperation with local, state, and federal law enforcement agencies, maintains a regional server as a LPR data repository in support of law enforcement efforts to improve public safety.

ARJIS provides the secure network infrastructure, technical standards, security protocols, controlled access, and database administration for the LPR system. Included in the support of the secure infrastructure are ongoing system updates, maintenance, disaster recovery, and security monitoring of the circuits, hubs, routers, firewalls, databases, and other components that comprise the ARJIS Enterprise, ensuring the priority, integrity, and availability of service to authorized law enforcement users. This Acceptable Use Policy sets forth rules restricting how the LPR system may be accessed by authorized user agencies (agencies) and defines how the LPR system is maintained by ARJIS.

The Regional LPR Operational Protocol under development by the County Chiefs' and Sheriff's Association outlines LPR best practices and standard operating procedures for those agencies that utilize LPR in the field.

B. LPR OVERVIEW

LPR data is collected by agencies utilizing specially-designed cameras to randomly capture an image of a vehicle license plate and convert the plate characters into a text file using optical character recognition technology. The text file can then be sent to a computer and compared against pre-existing data files, such as databases containing records of stolen or wanted vehicles as well as vehicles associated with AMBER alerts, missing children, wanted subjects, or other criteria. If a match is found, the LPR user (law enforcement officer or agency) is notified by an audible alert and an associated notation on the user's computer screen.

LPR cameras can be mobile (mounted on vehicles) or fixed (mounted to a structure) as determined by the agency that owns the cameras.

Mobile LPR systems scan plates, notify the user of a vehicle alert, and store the plate scan data for upload or transfer to an agency LPR server or the regional LPR server. LPRs in fixed positions link to an LPR server at the agency owning the fixed camera for updates, transmission of scanned plate data in real- time or near-real time, and alert notifications. The LPR data from agency LPR servers is replicated (copied) to the regional server in near real time. The alerting functionality resides with the agencies, not with ARJIS.

The alert lists against which license plate reads are checked may include (but are not limited to) the Stolen Vehicle System and Felony Warrants System, provided by the California Department of Justice (Cal DOJ); and downloaded four times a day. LPR users are required to take into account the potential for lag time between the last update and an alert provided by the LPR system on a stolen or wanted vehicle. Any alert provided by an LPR system is to be considered informational and advisory in nature only and any subsequent action in the field will be based on a law enforcement

agency's standard operating procedures.

1. Specification of Use

Recognizing the public safety benefits that could be achieved by the effective sharing of LPR data, ARJIS established a regional server accessible to authorized agencies capable of receiving and storing LPR data as well as providing query and alerting functions. The data is transferred to the regional server via wireless or hard-wired encrypted communications. Some of the agencies send their scanned plates directly to the regional server, while most of the larger agencies send their LPR scans to their agency-specific server first. The data is then uploaded to the regional server, in near-real time.

The plates scanned by the LPR systems are stored in a stand-alone regional server. The regional server is designed to meet Federal Bureau of Investigation Criminal Justice Information System (FBI CJIS) and Cal DOJ requirements, policies, and procedures, and is not connected to any other server.

The LPR system is restricted to legitimate criminal justice uses for the purpose of furthering law enforcement goals and enhancing public safety. There are two primary objectives of LPR data use in the region. The first is to identify stolen or lost vehicles and license plates, and wanted or missing persons, by matching the LPR data to the alert lists downloaded by Cal DOJ. The second objective is the ability to query LPR data to assist officers with ongoing criminal investigations, crime prevention and detection, and aid in the prosecution of crimes involving vehicles. LPR data is queried only if there is a reasonable suspicion that a vehicle is involved in criminal activity and the requestor has a legitimate need to know.

2. Privacy and Data Quality

2a. Privacy

In October 2008, prior to the implementation of the LPR system, ARJIS participated in a Privacy Impact Assessment (PIA) effort led by the International Association of Chiefs of Police. This effort involved the review of existing local, state, and federal laws, and American Civil Liberties Union privacy concerns. The resulting PIA, published in 2009, provided background for the development of this Policy.

Access to and use of LPR data is for official law enforcement purposes only. Accessing and/or releasing data from the LPR system for non-law enforcement purposes is prohibited. LPR data access and use is governed by the Cal DOJ California Law Enforcement Telecommunications System (CLETS) Polices, Practices and Procedures (PPP) (current rev. 09/2014), via CalMaster Control Agreement between the San Diego County Sheriff's Department (Sheriff) and ARJIS. The CLETS PPP further references the FBI CJIS Security Policy (current rev. 5.3, 8/4/2014).

The data records stored on the regional LPR server include photographs of the vehicle (close-up of the license plate and context photo of the rear of the vehicle)

and accompanying license plate number, date, time, and location in the field, and do not directly identify a particular person.

2b. Source Data

Each agency contributing data retains control and ownership as the official custodian of its records. Prior to sending any data to the regional LPR database, an agency must comply with the following:

- Be an ARJIS Public Safety member agency.
- Be a CLETS-certified agency.
- Be the owner, operator, manager, or controller of the LPR equipment that captures the contributed data.
- Maintain compliance with applicable FBI CJIS security policies regarding law enforcement data.
- Provide only LPR data that is in a format consistent with the National Information Exchange Model (NIEM) standard, or data that is readily capable of conversion to a NIEM-compliant format.
- Provide LPR data that includes, at a minimum, the time, date, and location of capture as well as a unique identifier of the equipment used to capture the information.
- Ensure that LPR equipment utilized by the agency is in full compliance with any requirements or standards established by the United States Department of Justice in regard to LPR systems.
- It is recommended that agencies that do not operate their own LPR server will implement a real time or near-real time data transfer to the regional server, via encrypted communication infrastructure, approved by Cal DOJ. This ensures the timeliness and effectiveness of the alert lists and provides maximum public safety benefit.

3. Data Limitation

The regional LPR server is not to be accessed for the purpose of monitoring individual activities protected by the First Amendment to the United States Constitution. The regional server does not contain alert lists for any of the following activities: insurance issues, parking scofflaws, deadbeat parents, and/or vehicle impounds.

The LPR system exists for the sole purpose of assisting law enforcement officers with ongoing criminal investigations and only for authorized public safety purposes.

4. Performance Evaluation

In addition to audit reports, ARJIS staff regularly monitors the LPR system for performance, reliability, and functionality. Staff also provides system-generated management reports for the participating agencies that highlight agency use, the number of license plate reads on file, and any technical issues identified during the reporting period. Other system-generated reports are produced on an as-needed basis.

5. Transparency and Notice

ARJIS is a Joint Powers Agency governed by the San Diego Association of Governments (SANDAG) Public Safety Committee, which includes elected officials representing the sub-regions of San Diego County and public safety officials.

LPR systems managed and hosted by individual law enforcement agencies existed within San Diego County prior to implementation of the LPR system. A PIA and Regional LPR Guidelines were completed prior to implementation of the LPR system.

This Acceptable Use Policy, the associated PIA, and other governing documents are currently posted on the ARJIS website at ARJIS.org.

6. Security

Regional LPR data is stored in a segregated server located in a secured law enforcement facility with multiple layers of physical security and 24/7 security protections. Physical access is limited to law enforcement staff and select ARJIS technical staff who have completed background investigations and completed the relevant FBI CJIS state and federal training.

Authorized ARJIS technical staff shall have the responsibility for managing the LPR system and associated infrastructure. ARJIS utilizes strong multi-factor authentication, encrypted communications, firewalls, and other system auditing, physical, administrative, and security measures to minimize the risks of unauthorized access to the system.

7. Retention, Access, and Use of LPR Data

7a. Retention

LPR data sent to ARJIS and stored on the regional server will be retained for a period of twelve months. The retention policy is consistent with the policies of the majority of agencies in California that have implemented LPR systems as of January 2015. Once the retention period has expired, the record will be purged from the active database. If an agency determines select LPR data is relevant to a criminal investigation, it is the responsibility of that agency to document and retain those records on its own server in accordance with the agency's policies regarding records retention. In the event California passes pending LPR legislation, this provision will automatically incorporate the retention period mandated in the legislation and will

supersede the 12-month period set forth above.

7b. Requirements for All Users Accessing Regional LPR data

Various measures are taken by ARJIS to limit access to the regional LPR server to prevent unauthorized access. Only those authorized personnel who have met the minimum training, certification, and background checks required for access to criminal justice data may access the regional LPR server. These requirements concerning the security and confidentiality of all 'justice data' are set forth in the FBI CJIS Security Policy and the CLETS PPP.

Authorized users must have an active account in the ARJIS Security Center, are mandated to follow the procedures for establishing complex passwords that must be changed every 90 days, and must enter a reason for access to LPR data prior to executing a query. These requirements are all built into the LPR system and are enforced using data entry fields that users must populate in order to access the regional LPR server. All queries for LPR data are subject to audit and kept in audit logs in accordance with the procedures outlined in the audit section below.

7c. Use of LPR data

LPR data is for official law enforcement purposes only. Participating law enforcement agencies will not share LPR data with commercial or private entities or individuals. However, participating law enforcement agencies may disseminate LPR data to governmental entities with an authorized law enforcement or public safety purpose for access to such data, in accordance with existing FBI and Cal DOJ policies, and their agency's standard operating procedures. ARJIS assumes no responsibility or liability for the acts or omissions of such agencies in disseminating or making use of the LPR data.

8. Auditing and Accountability

ARJIS has developed preset queries to the regional LPR server for auditing and other tracking functions. Included are audit capabilities for individual user activity, management reports of interface functionality and reliability, reports from session logs, and other key system metrics.

Access to, and use of, LPR data is logged for audit purposes. Audit logs are maintained for a minimum of three years. Audit reports are structured in a format that is understandable and useful and will contain, at a minimum:

- The name and agency of the user
- The date and time of access
- The specific data queried

- The justification for the query including a relevant case number if available at the time.

ARJIS will provide specific information regarding individual access and queries upon request from any agency. Identifying and addressing intentional misconduct is the responsibility of the individual agency. Notwithstanding the participating agency's responsibility with regard to misconduct, ARJIS reserves the right to enforce this Policy as described below.

9. Enforcement of Policy

Violation of this Policy by an ARJIS member agency or its staff may lead to suspension or termination of an agency or particular agency staff person's access to the regional LPR system. In the event a member agency discovers suspected or actual misuse of the regional LPR system, it will immediately inform the Director of ARJIS, who will in turn immediately notify the SANDAG Director of Technical Services and SANDAG Executive Director. In the event ARJIS discovers suspected or actual misuse of the regional LPR system, the Director of ARJIS will immediately notify the SANDAG Director of Technical Services, the SANDAG Executive Director, and the agency. The Technical Services Director, in consultation with the Director of ARJIS, or their designees, will determine whether to suspend or terminate access and if so for whom the suspension or termination will apply and will notify the affected agency. The affected agency will be notified of the decision by SANDAG and then will have 10 calendar days to appeal the decision to the SANDAG Executive Director. The Executive Director shall have final decision-making authority.

10. Policy Revisions

The Acceptable Use Policy for the Regional LPR System will be brought to the SANDAG Public Safety Committee and the SANDAG Board of Directors at least once per year for review and determination regarding the need for amendments.

Updates regarding the LPR system will be provided to the SANDAG Public Safety and Chiefs'/Sheriff's Management Committees annually or upon request.

11. Indemnification

Each user of the Regional LPR system (User) agrees to indemnify and hold SANDAG and ARJIS, and each of their personnel, harmless from any claim or demand, including reasonable attorneys' fees, made by any third-party in connection with or arising out of User's use of the Regional LPR system, User's violation of any terms or conditions of this Policy, User's violation of applicable laws, regulations or other policies, or User's violation of any rights of another person or entity. The term "Users" is defined to include each agency accessing the LPR system, as well as each individual person with access to the LPR system.

Kerry Bigelow

From: Kerry Bigelow
Sent: Friday, July 08, 2016 4:23 PM
To: Brittany.Huth@sandag.org
Subject: FW: SANDAG-Automated Regional Justice Information System (ARJIS) Data Sharing Memorandum of Understanding (MOU) with The City of Chula Vista

Hi Brittany,
I understand the signed MOU has been sent to you. Would it be possible to send back the fully signed version for our records, once you have received signatures from all interested parties?

Thank you,
Kerry

Kerry Bigelow
Assistant City Clerk
(619) 407-3590

From: Huth, Brittany
Sent: Monday, June 20, 2016 3:27 PM
To: 'dnorris@chulavistaca.gov'
Cc: 'dbejarano@chulavistapd.org'
Subject: SANDAG-Automated Regional Justice Information System (ARJIS) Data Sharing Memorandum of Understanding (MOU) with The City of Chula Vista

Dear City Clerk Norris:

The attached ARJIS Data Sharing MOU outlines the responsibilities of SANDAG and ARJIS and the law enforcement agencies that contribute to and access data from the ARJIS Enterprise System. The MOU also incorporates Acceptable Use Policies (AUPs) that set forth the conditions under which ARJIS systems may be accessed, and the processing and maintenance requirements for records stored on the ARJIS Enterprise System.

Contributing Member Agency (CMA, a law enforcement agency that provides law enforcement incident data to ARJIS for sharing purposes) was contacted by SANDAG-ARJIS and asked to review and agree to the terms of the draft of the MOU. The ARJIS Data Sharing MOU was reviewed by each CMA, including their respective legal counsel, and all terms were orally agreed to based on our records. The ARJIS Board and the SANDAG Board of Directors recently approved the final version of the MOU, which is enclosed.

Your agency is one of the CMAs that needs to sign the MOU. SANDAG-ARJIS is sending the MOU to you as the City Clerk and seeks your assistance in ushering the agreement through your applicable approval process. SANDAG-ARJIS staff wish to thank each CMA staff and counsel for their cooperation and assistance over the past year in bringing this MOU to fruition.

Please return the MOU signed by a person with the authority to legally bind your agency. The signed signature page may be scanned and emailed to Brittany.Huth@sandag.org or mailed to the following address:

Brittany Huth
San Diego Association of Governments
401 B Street, Suite 800
San Diego, CA 92101

In addition, Police Chief David Bejarano has been cc'd on this email for his own reference to the ARJIS Data Sharing MOU documents.

If you have any questions, or if your governing body desires a short presentation on ARJIS and the MOU, please contact Kurt Kroninger, SANDAG Director of Technical Services, at 619-699-6996 or kurt.kroninger@sandag.org. We would be happy to answer questions or attend your meeting.

SANDAG seeks to finalize this MOU by no later than **October 31st**. Your assistance in the timely execution of this MOU will be greatly appreciated.

Sincerely,

Brittany Huth
SANDAG | Contract Analyst
Office: (619) 595-5669