BOARD OF DIRECTORS AGENDA

Friday, February 13, 2015
10 a.m. to 12 noon
SANDAG Board Room
401 B Street, 7th Floor
San Diego

AGENDA HIGHLIGHTS

- **REVIEW OF DRAFT AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM ACCEPTABLE USE POLICIES**

PLEASE SILENCE ALL ELECTRONIC DEVICES DURING THE MEETING

YOU CAN LISTEN TO THE BOARD OF DIRECTORS MEETING BY VISITING OUR WEBSITE AT SANDAG.ORG

MESSAGE FROM THE CLERK

In compliance with Government Code §54952.3, the Clerk hereby announces that the compensation for legislative body members attending the following simultaneous or serial meetings is: Executive Committee (EC) $100, Board of Directors (BOD) $150, and Regional Transportation Commission (RTC) $100. Compensation rates for the EC and BOD are set pursuant to the SANDAG Bylaws and the compensation rate for the RTC is set pursuant to state law.

MISSION STATEMENT

The 18 cities and county government are SANDAG serving as the forum for regional decision-making. SANDAG builds consensus, makes strategic plans, obtains and allocates resources, plans, engineers, and builds public transit, and provides information on a broad range of topics pertinent to the region's quality of life.

San Diego Association of Governments · 401 B Street, Suite 800, San Diego, CA 92101-4231
(619) 699-1900 · Fax (619) 699-1905 · sandag.org

Welcome to SANDAG. Members of the public may speak to the Board of Directors on any item at the time the Board is considering the item. Please complete a Speaker's Slip, which is located in the rear of the room, and then present the slip to the Clerk of the Board seated at the front table. Members of the public may address the Board on any issue under the agenda item entitled Public Comments/Communications/Member Comments. Public speakers are limited to three minutes or less per person. The Board of Directors may take action on any item appearing on the agenda.

Public comments regarding the agenda can be sent to SANDAG via comment@sandag.org. Please include the agenda item, your name, and your organization. Email comments should be received no later than 12 noon, two working days prior to the Board of Directors meeting. ***Any handouts, presentations, or other materials from the public intended for distribution at the Board of Directors meeting should be received by the Clerk of the Board no later than 12 noon, two working days prior to the meeting.***

In order to keep the public informed in an efficient manner and facilitate public participation, SANDAG also provides access to all agenda and meeting materials online at www.sandag.org/meetings. Additionally, interested persons can sign up for e-notifications via our e-distribution list at either the SANDAG website or by sending an email request to webmaster@sandag.org.

SANDAG operates its programs without regard to race, color, and national origin in compliance with Title VI of the Civil Rights Act. SANDAG has developed procedures for investigating and tracking Title VI complaints and the procedures for filing a complaint are available to the public upon request. Questions concerning SANDAG nondiscrimination obligations or complaint procedures should be directed to SANDAG General Counsel, John Kirk, at (619) 699-1997 or john.kirk@sandag.org. Any person who believes himself or herself or any specific class of persons to be subjected to discrimination prohibited by Title VI also may file a written complaint with the Federal Transit Administration.

In compliance with the Americans with Disabilities Act (ADA), SANDAG will accommodate persons who require assistance in order to participate in SANDAG meetings. If such assistance is required, please contact SANDAG at (619) 699-1900 at least 72 hours in advance of the meeting. To request this document or related reports in an alternative format, please call (619) 699-1900, (619) 699-1904 (TTY), or fax (619) 699-1905.

SANDAG agenda materials can be made available in alternative languages. To make a request call (619) 699-1900 at least 72 hours in advance of the meeting.

Los materiales de la agenda de SANDAG están disponibles en otros idiomas. Para hacer una solicitud, llame al (619) 699-1900 al menos 72 horas antes de la reunión.

如有需要, 我们可以把SANDAG议程材料翻译成其他語言.

请在会议前至少 72 小时打电话 (619) 699-1900 提出请求.

SANDAG offices are accessible by public transit. Phone 511 or see* 511sd.com *for route information. Bicycle parking is available in the parking garage of the SANDAG offices.

BOARD OF DIRECTORS

Friday, February 13, 2015

ITEM NO. **RECOMMENDATION**

1. PUBLIC COMMENTS/COMMUNICATIONS/MEMBER COMMENTS

Public comments under this agenda item will be limited to five public speakers. Members of the public shall have the opportunity to address the Board on any issue within the jurisdiction of SANDAG that is not on this agenda. Other public comments will be heard during the items under the heading "Reports." Anyone desiring to speak shall reserve time by completing a "Request to Speak" form and giving it to the Clerk of the Board prior to speaking. Public speakers should notify the Clerk of the Board if they have a handout for distribution to Board members. Public speakers are limited to three minutes or less per person. Board members also may provide information and announcements under this agenda item.

REPORTS

+2. REVIEW OF DRAFT AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM ACCEPTABLE USE POLICIES (Lemon Grove Mayor Mary Sessom, Public Safety Committee Chair; Kurt Kroninger) — APPROVE

SANDAG has developed Acceptable Use Policies (AUPs) that outline ARJIS responsibilities and limitations in its role as the service provider for regional public safety-related technologies and applications. Staff will present the proposed AUPs for Facial Recognition, as implemented in the Tactical Identification System, and for the License Plate Reader (LPR) System. The Public Safety Committee recommends that the Board of Directors approve: (1) the ARJIS Acceptable Use Policy for Facial Recognition; and (2) the ARJIS Acceptable Use Policy for the Regional LPR System.

+3. PROPOSED FY 2015 PROGRAM BUDGET AMENDMENT: URBAN AREA SECURITY INITIATIVE TACTICAL IDENTIFICATION SYSTEM PROJECT (Lemon Grove Mayor Mary Sessom, Public Safety Committee Chair; Kurt Kroninger) — APPROVE

The Public Safety Committee recommends that the Board of Directors approve an amendment to the FY 2015 Program Budget to accept $99,000 for system maintenance of the Tactical Identification System.

4. CONTINUED PUBLIC COMMENTS

If the five speaker limit for public comments was exceeded at the beginning of this agenda, other public comments will be taken at this time. Subjects of previous agenda items may not again be addressed under public comment.

5. UPCOMING MEETINGS — INFORMATION

The next Board Business meeting is scheduled for Friday, February 27, 2015, at 9 a.m.

6. ADJOURNMENT

+ next to an agenda item indicates an attachment

SANDAG

AGENDA ITEM NO. 15-02-2

BOARD OF DIRECTORS
FEBRUARY 13, 2015

ACTION REQUESTED – APPROVE

REVIEW OF DRAFT AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM ACCEPTABLE USE POLICIES

File Number 7350100

Recommendation

The Public Safety Committee recommends that the Board of Directors approve: (1) the Automated Regional Justice Information System (ARJIS) Acceptable Use Policy for Facial Recognition (Attachment 1); and (2) the ARJIS Acceptable Use Policy for the Regional License Plate Reader System (Attachment 2).

Introduction

A key priority for SANDAG is the development and implementation of policies that outline the responsibilities of the Automated Regional Justice Information System (ARJIS) Division as the regional public safety information technology services provider for public safety-related technologies and applications. These technologies have proven to be instrumental in assisting agencies in addressing critical public safety issues, while enhancing overall performance. The responsibilities of ARJIS as it relates to these technologies are limited to providing a secure network infrastructure, implementing data privacy and security protocols, and controlling access to authorized users, while ensuring system performance and reliability.

Operational protocols for how these technologies are utilized by law enforcement agencies and their officers are dictated by those individual agencies, and must be consistent with the Regional Operational Protocols (currently in development by the County Chiefs' and Sheriff's Association); California Law Enforcement Telecommunications System Policies, Practices, Procedures, and Statutes (published by the California Department of Justice); and the Criminal Justice Information Services Security Policy (published by the Federal Bureau of Investigation).

This report is focused on proposed ARJIS Acceptable Use Policies (AUPs) for Facial Recognition (Attachment 1) and the Regional License Plate Reader System (Attachment 2). In accordance with the process outlined in Board Policy No. 026: Public Safety Policy Advisory Committee, these proposed AUPs are being presented to the Board of Directors for review and approval.

Discussion

Facial Recognition and the Tactical Identification System

Facial recognition technology has been available for use by law enforcement throughout the United States for the past decade. It has gained importance in recent years given vast improvements in the technology (lower cost, expanded capabilities, enhanced accuracy, and reliability) and in the

investigative value it provides in addressing the need for accurate identification tools. ARJIS implements facial recognition technology through the Tactical Identification System (TACIDS).

A National Institute of Justice technology grant enabled ARJIS to research, test, and implement a mobile application that assists officers with identifying subjects in the field. TACIDS allows an officer to use a smartphone or tablet to photograph an individual when the officer has detained the individual and verification of an individual's identity is not otherwise possible, or when the officer reasonably suspects the self-reported information is false. The image is instantly compared to the San Diego County Sheriff's booking photo database (currently about 1.4 million images) and potential matches are returned within 10 to 15 seconds.

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. At all times the officer must follow the operational protocols of his/her agency in utilizing the system to verify an individual's identity.

To date there are approximately 800 registered TACIDS users representing 28 law enforcement agencies in the San Diego region. Since August 2012, more than 17,000 image submittals have resulted in approximately 4,700 potential matches. Many of these matches resulted in the arrest of persons who were not truthful about their identities and also were wanted felons and/or parolees at large. TACIDS also has been instrumental in the identification of several deceased individuals.

License Plate Reader

In use nationally for the past decade, License Plate Reader (LPR) systems have been regarded as effective tools for identifying and recovering stolen vehicles and/or vehicles that are wanted in conjunction with a crime. LPR systems consist of specially designed, high-speed cameras combined with sophisticated computer algorithms capable of randomly capturing an image of a license plate and converting the plate characters into computer-readable data. The text files can then be sent to a computer and compared against pre-existing data files, such as 'hot lists' 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 law enforcement agency) is notified by an audible alert and an associated notation on the user's computer screen.

In 2008, San Diego County law enforcement agencies began procuring their own LPR systems. During this same time, ARJIS partnered with the National Institute of Justice to develop a national LPR standard for sharing LPR data among agencies. In 2009, Urban Area Security Initiative funds were awarded to ARJIS to procure a regional server to share LPR data among its member agencies. During calendar years 2009-2014, 11 ARJIS member agencies continued to expand their number of LPR cameras and to develop interfaces to feed their LPRs in real-time to the regional server. Decisions regarding the number of cameras capturing LPR data and its placement are made by the ARJIS member agencies. The ARJIS role is to provide a mechanism for the member agencies to share LPR data, allowing law enforcement collaboration across jurisdictional boundaries.

Policy Development

Prior to implementing each of these technologies, ARJIS partnered in the national Privacy Impact Assessment development efforts led by the International Association of Chiefs of Police (IACP). The initial policies for these technologies, approved by the Chiefs'/Sheriff's Management Committee in 2012 and 2013, broadly governed both the technical and operational aspects of the technologies.

In 2014, recognizing the need to focus on those technical areas under the responsibility of ARJIS, updated policies were developed. As "acceptable use" policies, these documents set forth rules restricting how the TACIDS and LPR systems may be accessed and defining how they are maintained. In accordance with Board Policy No. 026: Public Safety Policy Advisory Committee, these AUPs have been recommended by the Chiefs'/Sheriff's Management Committee and the Public Safety Committee, and are being presented to the Board of Directors for review and approval.

Operational policies governing the use in the field of LPR and TACIDS by law enforcement agencies and their officers are the responsibility of those agencies (for use within their jurisdictions) and the County Chiefs' and Sheriff's Association (for region-wide operational protocols).

This distinction between the purpose of an acceptable use policy and that of an operational policy is important both in establishing who is responsible for drafting and implementing each and in delineating where the roles and responsibilities of one agency ends and another begins. The AUP establishes SANDAG responsibilities, while the operational policies describe the responsibilities of the agencies using the data. The AUP is intended to clarify that SANDAG should not be liable for the conduct of a law enforcement officer in the field.

To ensure ARJIS policies are consistent with those at the state and federal levels, ARJIS has collaborated with the IACP and followed the IACP Technology Policy Framework in its development. For example, the Framework calls for the use of nine universal principles as a guide in development of effective technology policies:

1. Specification of Use
2. Policies and Procedures
3. Privacy and Data Quality
4. Data Minimization and Limitation
5. Performance Evaluation
6. Transparency and Notice
7. Security
8. Data Retention, Access and Use
9. Auditing and Accountability.

These principles were followed in the development of both AUPs presented in this report.

Reducing Risk for SANDAG

Section 11 of both AUPs is entitled "Indemnification" and contains the following language:

> Each user of the [TACIDS/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 use of the [TACIDS/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 [TACIDS/Regional LPR] system, as well as each individual person with access to the [TACIDS/Regional LPR] system.

Users of each of these systems who are individuals will be required to acknowledge reading the associated AUP and assent to comply with all of its provisions. An ARJIS Data-Sharing Memorandum of Understanding (MOU) is under development that will spell out the responsibilities of SANDAG and data sharing agencies with regard to liability for the data shared on the TACIDS and Regional LPR systems. The MOU also will include provisions concerning public records request procedures.

Next Steps

Upon approval by the Board of Directors, these AUPs would immediately go into effect. Both AUPs would be incorporated by reference in the ARJIS Data-Sharing Memorandum of Understanding, which will be brought forward to the Public Safety Committee and Board of Directors for review and approval in the fourth quarter of FY 2015. All ARJIS member agencies will be required to sign the MOU once approved.

GARY L. GALLEGOS
Executive Director

Attachments:
1. Draft ARJIS Acceptable Use Policy for Facial Recognition
2. Draft ARJIS Acceptable Use Policy for the Regional License Plate Reader System

Key Staff Contact: Kurt Kroninger, (619) 699-6996, kurt.kroninger@sandag.org
Pam Scanlon, (619) 699-6971, pam.scanlon@sandag.org

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

DRAFT
12/03/2014

This document is in DRAFT form and is intended for review and comment only.

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 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
Acceptable Use Policy for the Regional License Plate Reader System
DRAFT
01/16/2015

This document is in DRAFT form and is intended for review and comment only.

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 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.

AGENDA ITEM NO. 15-02-3

BOARD OF DIRECTORS
FEBRUARY 13, 2015

ACTION REQUESTED – APPROVE

PROPOSED FY 2015 PROGRAM BUDGET AMENDMENT: URBAN AREA SECURITY INITIATIVE TACTICAL IDENTIFICATION SYSTEM PROJECT

File Number 7351901

Introduction

SANDAG received approval at the April 18, 2014, Public Safety Committee meeting to seek Urban Area Security Initiative (UASI) funds for the Tactical Identification System (TACIDS) facial recognition maintenance agreement. The Automated Regional Justice Information System (ARJIS) applied for and was subsequently awarded $99,000 to continue maintaining this system throughout 2015.

Recommendation

The Public Safety Committee recommends that the Board of Directors approve an amendment to the FY 2015 Program Budget to accept $99,000 for system maintenance of the Tactical Identification System.

Background

The TACIDS project started as a research and development grant from the National Institute of Justice. The objective of the grant was to demonstrate the ability for an officer in the field to take a photo on a mobile device and submit it for biometric comparison against the region's booking photos. The photos would be returned based on the confidence rating of the match and would serve as a tool for assisting officers in identifying individuals. As a part of this process, a vendor was needed to assist with the implementation of the biometric algorithm for facial recognition. A competitive bid process was completed, and FaceFirst LLC was identified as the vendor most suited for this role.

A provisional license agreement with FaceFirst allowed ARJIS to deploy the application to 250 officers in the field for the duration of one year. The feedback was instantaneous, with users reporting on the effectiveness of the application in assisting with positive identification and in time saved by eliminating the need to take individuals to the station to determine who they were. An unanticipated outcome reported was that the application assisted in officer safety by eliminating the need for officers to use hands-on approaches to obtain identification information.

The demand for the application was so high that the number of users requesting access soon exceeded the 250 permitted in the FaceFirst contract. The solution was to seek UASI grant funds to procure an enterprise license that would provide all ARJIS mobile users with access to the application. The license was procured January 1, 2014, and included one year of maintenance support.

Discussion

To date, there are approximately 800 registered TACIDS users representing 28 agencies. Since August 2012, more than 17,000 image submittals have resulted in approximately 4,700 potential matches. A potential match is defined in which the confidence score produced by the system at the time of submittal reaches or exceeds 90 percent.

Over the past year, 56 percent of the technology-related success stories reported to ARJIS were attributed to TACIDS. Of these, 91 percent involved individuals providing false or no identification and the remaining 9 percent involved deceased or incapacitated individuals. Many of these individuals were wanted felons, parolees at large, and/or had outstanding warrants.

To continue providing users with access to this successful application, ARJIS must pay an annual software maintenance fee. The Regional Technology Partnership and the Urban Area Working Group recognized this need and allocated $99,000 in FY 2014 UASI funding for one year of system maintenance.

GARY L. GALLEGOS
Executive Director

Attachment: 1. Work Element 73519.01 Budget

Key Staff Contact: Katie Mugg, (619) 699-6979, katie.mugg@sandag.org

WORK ELEMENT: **73519.01 NEW - ARJIS: Regional Data Sharing III**

FY 2015 BUDGET: **~~$0~~ 99,000**

AREA OF EMPHASIS: **Regional Operations and Services**

Amendment Title: Accept UASI funds for ARJIS TACIDS Facial Recognition License

Funds Source				
	Prior	**FY 2015**	FY 2016	Total
U.S. Department of Justice	$0	$~~0~~99,000	$0	$~~0~~99,000
TOTAL	**$0**	$~~0~~99,000	**$0**	$~~0~~99,000

Funds Application				
	Prior	**FY 2015**	FY 2016	Total
Equipment	$0	$~~0~~99,000	$0	$~~0~~99,000
TOTAL	**$0**	**$~~0~~99,000**	**$0**	**$~~0~~99,000**

OBJECTIVE

The objective of this work element is to coordinate, develop, and implement applications that enhance public safety throughout the San Diego region. The Department of Homeland Security's Urban Area Security Initiative (UASI) addresses this need by funding agencies to implement projects that target information sharing in San Diego County and bordering regions. The emphasis in FY 2015 is to continue providing maintenance support for the Tactical Identification System (TACIDS) facial recognition software.

PREVIOUS ACCOMPLISHMENTS

The Automated Regional Justice Information System (ARJIS) has developed a robust mobile program that has greatly enhanced public safety throughout the region by enabling officers to obtain critically needed data in the field. A facial recognition component has been piloted that is assisting with positive identifications in the field.

Project Manager: Mugg, Katie
Committee(s): Public Safety Committee
Working Group(s): ARJIS Business Working Group, Chiefs'/Sheriff's Management Committee

PRODUCTS, TASKS, AND SCHEDULES FOR FY 2015

Task No.	% of Effort	Task Description/Product/Schedule	
1	100	**Task Description:**	Maintain the TACIDS facial recognition software used by ARJIS mobile users.
		Product:	Continued system support
		Completion Date:	6/30/2015

1

ARJIS DRAFT ACCEPTABLE USE POLICIES

SANDAG

2

ARJIS Serves as the Regional Public Safety IT Provider

- JPA among the 18 cities, the County, and SANDAG
- Provides secure network and IT infrastructure for 82 agencies
- Receives and validates public safety data
- Provides regional public safety tools and technologies
- Develops technical policies
  - Aligned with state and federal policies
- Implements privacy and security protocols
- Authorizes access and audits usage
- Ensures performance and reliability

SANDAG

3

Process for ARJIS Policy Development

- Collaborate with the International Association of Chiefs of Police (IACP)
  - Largest membership organization of police executives
  - Develops national policies and protocols
  - Technology Policy Framework
- Refer to:
  - Federal Bureau of Investigation - Criminal Justice Information System (FBI-CJIS) Security Policies
  - California Department of Justice (CAL-DOJ) California Law Enforcement Telecommunications System (CLETS) Policies, Practices, and Procedures

SANDAG

4

IACP Technology Policy Framework

- Universal principles developed by the IACP as a guide in the development of effective technology policies
  - Specification of use
  - Policies and Procedures
  - Privacy and Data Quality
  - Data Minimization and Limitation
  - Performance Evaluation
  - Transparency and Notice
  - Security
  - Data Retention, Access and Use
  - Auditing and Accountability

SANDAG

5

Process for ARJIS Policy Development

- Identify operational vs. technical policy components
- ARJIS is responsible for the technical aspects of the regional technologies it develops and maintains
- Operational policies are the responsibility of individual agencies

SANDAG

6

Policy Distinction

Acceptable Use Policy

- Secure network infrastructure
- Authorized access
- System performance
- Data security and privacy

Operational Policy

- Equipment deployment
- Identification verification
- Response to alerts
- Certification and training of users

SANDAG

7

ARJIS Acceptable Use Policy Approval
(reflects 9/2014 revision of Board Policy No. 026)

- Policy review and approval
  - SANDAG legal counsel and internal review
  - Chiefs' Sheriff's Management Committee (CSMC) review and recommend
  - PSC to approve or recommend Board of Directors approval
- Policies reviewed annually

SANDAG

8

ARJIS AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM

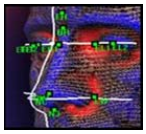
DRAFT Acceptable Use Policy for Facial Recognition

SANDAG

9

ARJIS Facial Recognition Background

- National Institute of Justice (NIJ) grant, entitled Tactical Identification System (TACIDS) resulted in:
  - Market survey
  - PIA and policy guidelines
  - Proof of concept application



- 2013 pilot project
- In 2014, the U.S. Department of Homeland Security provided funding for production system

SANDAG

10

TACIDS Functionality

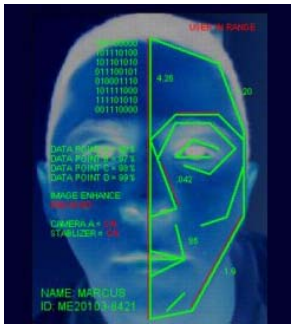
- Officers use a smartphone to photograph an individual when:
  - Individual is detained based on reasonable suspicion, and
    - Verification of an individual's identity is not possible, or
    - Officer suspects the self-reported information is false
  - Individual is incapacitated or otherwise unable to provide ID
    - Ill, injured, deceased
- Image submitted for comparison against the San Diego County Sheriff's booking database (currently about 1.4 million images)
  - ARJIS receives booking photos daily from the Sheriff's Department

SANDAG

11

TACIDS Functionality

- System utilizes a mathematical algorithm for biometric comparison
- Records returned by level of confidence - highest to lowest
- Potential matches considered advisory in nature
- Subsequent verification of the individual's identify and/or follow-on action based on an agency's standard operating procedures



SANDAG

12

TACIDS Policy Background

- 2013 Pilot leveraged:
  - 2010 National Policy Guidelines by the International Justice and Public Safety Network (Nlets)
  - 2011 PIA by Nlets
- Initial policy, approved by CSMC in 2013, broadly governed technical and operational aspects of the pilot TACIDS project
- Refined in September 2014:
  - ARJIS Acceptable Use Policy for Facial Recognition sets forth rules restricting how the system may be accessed and defining how it is maintained
  - Excludes operational aspects which are covered by law enforcement agency standard operating procedures

SANDAG

13

Specification of Use

- Two primary objectives for using TACIDS
  - Identification of individuals not forthcoming or dishonest with their IDs
  - Identification of individuals who are incapacitated or otherwise unable to provide ID

SANDAG

14

Privacy and Data Quality

- Access to TACIDS is governed by:
  - FBI CJIS Security Policy
  - CalDOJ CLETS Polices, Practices and Procedures
  - Master Control Agreement with the Sheriff
- ARJIS uses the Sheriff's booking system to provide the booking images and associated metadata
- Photos are stored in a regional database, hosted, secured, and maintained by ARJIS
- Accessing and/or releasing data from TACIDS for non-law enforcement purposes is prohibited

SANDAG

15

Data Limitation

- TACIDS exists for the sole purpose of identifying individuals for public safety purposes
- Photographs taken in the field are matched only against the Sheriff's booking photo database
- No other databases, such as driver's license photo databases, are linked to or accessible via TACIDS
- No interface of TACIDS to any form of video surveillance

SANDAG

16

Performance Evaluation

- TACIDS monitored for performance, reliability, and functionality
- Staff provide system generated management reports
  - Agency use
  - Number of matches with a 90% or better confidence rating
  - Technical issues identified during the reporting period

SANDAG

17

Transparency and Notice

- ARJIS is a Joint Powers Agency that is governed by the San Diego Association of Governments (SANDAG) Public Safety Committee (PSC)
- TACIDS was competitively bid
- Privacy Impact Assessment was completed and published prior to implementation of TACIDS
- Policies and related documentation are posted on the ARJIS website –ARJIS.org

SANDAG

18

Security

- ARJIS responsible for TACIDS server, software upgrades, network infrastructure, coordinating system access
- Secure law enforcement facility with 24/7 security protections
- Physical access is limited to authorized personnel
- Mobile Device Management (MDM)
  - Remotely manage devices
  - Send updates
  - Immediately disable

SANDAG

19

Retention

- Sheriff's booking records owned by the Sheriff's Department and comply with Sheriff's retention schedule
- Activity logs retained by SANDAG for three years

SANDAG

20

Access and Use of Data

- Must be an ARJIS member agency:
  - CLETS certified, FBI CJIS compliant
- Users must be authorized by agency security officer
- Follow the procedures for establishing complex passwords
- Must sign agreement acknowledging that he/she has read and agrees to comply with this Policy
- TACIDS is used solely to assist law enforcement officers in the identification of individuals
- Potential matches are advisory in nature and any subsequent verification and/or follow-on action should be based on agency standard operating procedures

SANDAG

21

Auditing and Accountability

- All transactions are logged
- Logs are retained for minimum of three years
- Minimum audit information:
  - Name and ARJIS ID of the law enforcement user
  - Name of agency employing the user
  - Date and time of access
  - Copy of the biometric template created at the time of the photo capture

SANDAG

22

Enforcement

- Violation may lead to suspension or termination of access
- Affected member agency has ten days to appeal
- SANDAG Executive Director has final decision-making authority

Indemnification

- Each user of the TACIDS system agrees to hold SANDAG-ARJIS harmless
- The term "user" is defined to include each agency accessing, as well as each individual person with access to the TACIDS system

SANDAG

23

DRAFT Acceptable Use Policy for the Regional License Plate Reader (LPR) System

SANDAG

24

LPR Overview

- Specially-designed cameras owned and operated by participating agencies systematically capture license plate images and convert the plate characters to a text file using optical character recognition technology
- Text file sent to a participating agency's computer and compared against databases containing records of:
  - Stolen or wanted vehicles
  - Vehicles associated with:
    - AMBER alerts
    - Missing children
    - Wanted subjects, or other criteria

SANDAG

25

LPR Overview

- If match occurs, officer or agency is notified by an audible alert and notation on the user's computer screen
- LPR data from participating agencies is transmitted to the regional ARJIS server
- LPR data is accessible by all 82 ARJIS members
- ARJIS does not operate or own any LPR cameras

Mobile

Fixed

SANDAG

26

LPR Participating Agencies

- Each agency contributing data retains control and ownership as the official custodian of its records. Agencies include:
  - Carlsbad Police Department
  - Chula Vista Police Department
  - Coronado Police Department
  - El Cajon Police Department
  - Escondido Police Department
  - La Mesa Police Department
  - National City Police Department
  - Oceanside Police Department
  - San Diego Harbor Police Department
  - San Diego Police Department
  - San Diego State University Police Department
  - San Diego County Sheriff's Department

SANDAG

27

LPR Timeline in the San Diego Region

- 2008: ARJIS collaborated on national LPR standard for data sharing
- 2008-2012: San Diego County agencies procured LPR cameras
- 2009: IACP LPR Privacy Impact Assessment
- 2009: PSC approves Urban Area Security Initiative (UASI) funds to procure a regional server
- 2010: IACP LPR Model Technology Policy Framework
- 2012: Initial LPR Policy
- 2014: Policy refined:
  - ARJIS Acceptable Use Policy

SANDAG

28

Specification of Use

- There are two primary objectives of LPR data use in the region:
  - Identify stolen or lost vehicles and license plates, and wanted or missing persons
    - Automated match of LPR data to the alert lists downloaded from California Department of Justice
  - Query LPR data to assist ongoing criminal investigations, crime prevention and detection, and prosecution of crimes involving vehicles
    - LPR data is queried only if there is a reasonable suspicion that a vehicle is involved in criminal activity

SANDAG

29

Privacy and Data Quality

- Access to and use of LPR data is governed by:
  - FBI CJIS Security Policy
  - CAL-DOJ CLETS Polices, Practices and Procedures
  - Master Control Agreement with the Sheriff
- Accessing and/or releasing data from the LPR system for non-law enforcement purposes is prohibited
- Participating agencies:
  - 12 ARJIS member agencies that contribute information
- Each agency retains control and ownership of its own data
- Data requirements:
  - Time, date, and location of capture and unique camera ID
  - Ensure equipment is in compliance with DOJ standards

SANDAG

30

Data Limitation

- The LPR system may only be used for authorized public safety purposes
- Not to be accessed for the purpose of monitoring individual activities protected by the U.S. Constitution
- Alert lists not provided in this region for any of the following activities: insurance issues, parking scofflaws, deadbeat parents, and/or vehicle impounds

SANDAG

31

Performance Evaluation

- LPR monitored for performance, reliability, and functionality
- Staff provide system generated management reports
  - Agency use
  - Number of license plate reads on file
  - Technical issues identified during the reporting period

Agency	Camera Name	LPR Reads This Month	# Of Days Reads Sent	No. of Alerts
Agency X	One	31080	27	13
Agency Y	Two	12841	17	10
Agency Z	Three	21025	17	12

Alert List Name	No. of Alerts
STOLEN VEHICLES	15
LOST OR STOLEN PLATES	20
Total	35

Duration: 12/2/2014 - 01/01/2015

SANDAG

32

Transparency and Notice

- ARJIS is a Joint Powers Agency that is governed by the SANDAG PSC
- A PIA and Regional LPR Guidelines were completed prior to implementation of the LPR system
- This Acceptable Use Policy, associated PIA, and other governing documents are currently posted on the ARJIS website at ARJIS.org

SANDAG

33

Security

- ARJIS responsible for LPR server, software upgrades, network infrastructure and authorized system access
- Secure law enforcement facility with 24/7 security protections
- Physical access is limited to authorized personnel
- ARJIS utilizes encrypted communications, firewalls, and other security measures to minimize the risks of unauthorized access

SANDAG

34

Retention

- LPR data retained for 12 months
  - Consistent with majority of LPR agencies
- Once the retention period is met, the record is purged
- If an agency determines select LPR data is relevant to a criminal investigation, it is the responsibility of that agency to retain those records as part of the investigation
- Provision to be superseded in the event the pending CA LPR legislation passes (Example: SB 34)

SANDAG

35

Access and Use of Data

- Must be an ARJIS member agency:
  - CLETS certified, FBI CJIS compliant
- Users must be authorized by agency security officer
- Follow the procedures for establishing complex passwords
- All queries must include a reason for search
- Participating agencies will not share LPR data with commercial or private entities or individuals
- Potential matches are advisory and any subsequent verification and/or action must be based on agency operating procedures

SANDAG

36

Auditing and Accountability

- All transactions are logged
- Logs are retained for minimum of 3 years
- Minimum audit information:
  - Name and agency of the user
  - Date and time of access
  - Specific data queried
  - Justification for the query including a relevant case number

SANDAG

37

Enforcement

- Violation may lead to suspension or termination of access
- Affected member agency has ten days to appeal
- SANDAG Executive Director has final decision-making authority

Indemnification

- Each user of the LPR system agrees to hold SANDAG-ARJIS harmless…
- The term "user" is defined to include each agency accessing, as well as each individual person with access to the LPR system

SANDAG

38

Next Steps

Upon approval by Board of Directors

- Most provisions would immediately go into effect
- Both AUPs would be incorporated by reference in the draft ARJIS Data-Sharing Memorandum of Understanding (MOU) to be presented to the PSC and Board of Directors for review and approval Q4 FY 2015
- Upon approval, all ARJIS member agencies would be required to sign the MOU

SANDAG

Recommendation

The Public Safety Committee recommends that the Board of Directors approve: (1) the Automated Regional Justice Information System (ARJIS) Acceptable Use Policy for Facial Recognition (Attachment 1); and (2) the ARJIS Acceptable Use Policy for the Regional License Plate Reader System (Attachment 2).

SANDAG