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.