Automated Regional Justice Information System (ARJIS)

Officer Notification System Policy

January 14, 2022

A. STATEMENT OF PURPOSE

This Acceptable Use Policy sets forth rules restricting how the Officer Notification System (ONS) may be accessed and used by authorized user agencies and defines how the ONS is maintained by ARJIS.

ARJIS, in cooperation with local, state, and federal law enforcement agencies, maintains this application to share information on persons, locations and vehicles 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 ONS. 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 integrity, and availability of service to authorized law enforcement users.

B. ONS OVERVIEW

Data is entered into ONS by ARJIS member agencies to alert law enforcement personnel about the status of a person, location, or vehicle and/or to request that law enforcement personnel follow directives in the ONS record Remarks section when they encounter that ONS entry. ONS records are stored in the ARJIS database and are accessible via the ONS application, other ARJIS applications and local law enforcement databases. ONS allows the user who entered the ONS record to be notified automatically via cell phone text message and/or email message regarding their record(s). If notification is enabled by the user, a text and/or email message will be sent to the user when a particular subject, location or vehicle connected to the ONS record is entered into the ARJIS database or when any user searches for that subject, location, or vehicle record in a local ARJIS database.

Access to the ONS is granted to law enforcement users by their Agency CLETS Coordinator or designee in accordance with state and federal guidelines.

Any alert provided by an ONS is only to be considered informational and advisory in nature and, unless specifically stated, it does not provide the basis for arrest or detention. Users must confirm the validity of an ONS record by contacting the entering agency prior to taking enforcement actions based solely on that record.

1. Specification of Use

Recognizing the public safety benefits that are achieved by effective sharing of ONS data, ARJIS established a regional server accessible to authorized agencies capable of receiving and storing ONS data as well as providing query and alerting functions. The data is transferred to the regional server via wireless or hard-wired encrypted communications.

The data entered into the ONS is stored in a stand-alone regional server. The regional server is designed to meet Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) and California Department of Justice (DOJ) requirements

The ONS 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 ONS data use in the region.

1. Alert law enforcement regarding the status of a person, location, or vehicle.
2. Enhance officer and public safety through regional information sharing within and between law enforcement agencies.

2. Privacy and Data Quality

2a. Privacy

ARJIS applications, such as ONS, adhere to the California Law Enforcement Telecommunications System (CLETS) Policies, Practices and Procedures (PPP).

ONS records include names, personal descriptions, vehicle information, addresses and photographs connected to these records. Records also include the username and agency submitting the record; remarks entered by the user in connection with a record; dates of entry into the system and purge dates for the entries; they may include a location, such as street address, cross street, or police beat. For a complete list of specific data elements, please see Appendix A.

2b. Source Data

Each agency contributing data retains control and ownership as the official custodian of its records. Prior to entering any data into ONS, an agency must comply with the following:

- Be an ARJIS Public Safety member agency.
- Be a CLETS-certified agency.
- Maintain compliance with applicable FBI CJIS security policies regarding law enforcement data.
- Exercise due diligence in entering data accurately into ONS and ensure that the appropriate ONS type is selected with matching purge criteria.
- Maintain or reference a master record for the data entered in the ONS entry.
- Include information in the Remarks section that is sufficient for agencies to take appropriate action and preserve officer safety.

3. Performance Evaluation

ARJIS staff regularly monitors the ONS for performance, reliability, and functionality. System-generated reports are produced on an as-needed basis for agencies and use by ARJIS staff.

4. 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.

5. Security

Regional ONS data is stored in a segregated server located in a secured law enforcement facility with multiple layers of physical security and round-the-clock security protections. Physical access is limited to law enforcement staff and select ARJIS technical staff who have completed background investigations and completed the required security awareness training.

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

Retention, Access, and Use of ONS Data

6a Retention

Agencies are responsible for designating the appropriate record retention schedule based upon that agency's specific need. For a complete list of retention periods by ONS Subtype, please see Appendix B.

ONS is designed to purge records automatically at the preset purge date entered for the corresponding ONS record type. ARJIS is responsible for ensuring the preset purge dates are enforced within ONS. Agencies are responsible for promptly removing outdated or no longer applicable ONS records.

Once the retention period has expired, the record will be purged from the active database. If an agency determines select ONS data is relevant to a criminal investigation, it is the responsibility of that agency to maintain that data in ONS in accordance with the agency's policies regarding records retention.

6b. Requirements for All Users Accessing Regional ONS data

Various measures are taken by ARJIS to limit access to the regional ONS server to prevent unauthorized use. Only those authorized personnel who have met the background check and agency requirements for access to criminal justice information may access the regional ONS server. Requirements concerning the security and confidentiality of criminal 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, be required to follow the procedures for establishing and maintaining complex passwords and must be approved by their Agency CLETS Coordinator (ACC) or designee. The ACC or their designee will grant the appropriate level of ONS access based on their required job duties. All ONS entries and queries for ONS data are subject to audit and kept in audit logs in accordance with the procedures outlined in the audit section below.

6c. Use of ONS data

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

The ONS may not be used to enforce immigration laws pursuant to Senate Bill 54, the California Values Act.

7. Auditing and Accountability

ARJIS has developed preset queries to the regional ONS 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, ONS data is logged for audit purposes. Audit logs are maintained for a minimum of three years. Audit reports shall contain, at a minimum:

- The identification number and agency of the user
- The date and time of access, as well as purge date
- The specific data entered or queried
- The justification for the entry/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.

8. 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 ONS. In the event a member agency discovers suspected or actual misuse of the regional ONS, it will take appropriate action consistent with agency policy.

In the event ARJIS discovers suspected or actual misuse of the regional ONS, 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.

9. Policy Revisions

The Acceptable Use Policy for ONS will be brought to the SANDAG Public Safety Committee and the SANDAG Board of Directors at least every five years for review and determination regarding the need for amendments.

Updates regarding the ONS will be provided to the SANDAG Public Safety and Chiefs'/Sheriff's Management Committees at least every five years or upon request.

10. Indemnification

Each user of the ONS 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 from User's use of the ONS , 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 ONS as well as each individual person with access to the ONS.

APPENDIX A

Last Updated 6-24-21

List of Specific Data Elements in ONS Records:

PERSON OF INTEREST

Case Reference	Glasses
Notify Type	Physical Oddity Type
Related Crime	Physical Oddity Description
Unit	Nickname
Purge Date	Name Type – AKA or Alias
Officer ID	AKA or Alias Last Name
Remarks	AKA or Alias First Name
Last Name	AKA or Alias Middle Name
First Name	AKA or Alias Suffix
Middle Name	Street Number
Suffix	Street Direction
Subject Type	Street Name
Date of Birth	Street Type
Race	Unit Number
Sex	City
Height	State
Weight	Phone Number
Hair Color	Phone Type
Eye Color	Social Security Number
Build	Driver's License Number
Facial Hair	Driver's License State
Hair Length	Other ID Type
Hair Style	ID Number
Complexion	Person Image

VEHICLE OF INTEREST

License Plate
License Plate State
VIN Number
Vehicle Type
Vehicle Year
Vehicle Make
Vehicle Model
Vehicle Color Top
Vehicle Color Bottom
Vehicle Image

APPENDIX A (continued)

LOCATION OF INTEREST

Street Number
Street Direction
Street Name
Street Type
Cross Street Direction
Cross Street Name
Cross Street Type
Jurisdiction
Beat
Location Image

APPENDIX B

List of Retention Periods by ONS Subtypes:

ONS SUBTYPE	RETENTION PERIOD
CCW Notification	Five Years + One Month from Registration Date
Drug Court Offender	User Decision from Court Order
Evidence Notification	Six Months from Latest Record Entry Date
4th Waiver	Set Automatically Through Interface – Probation Record
Fugitive Notification	User Decision
Juvenile Court Orders	Set Automatically Through Interface - Court Order
Law Enforcement Applicant	User Decision
Parolee Notification	User Decision from Court Order
Probation High Risk	User Decision from Court Order, but no more than 10 years from Latest Record Entry Date
Registered Arsonist Offender	User Decision from Court Order
Registered Narcotic Offender*	User Decision from Court Order
Registered Sex Offender	User Decision from Court Order
Stay Away TRO	User Decision from Court Order
Special Investigations	Five Years from Latest Record Entry Date
Threat Assessment	Three Years from Latest Record Entry Date

*Users may no longer enter Registered Narcotic Offender records due to the end of registration requirements by new statute on January 1, 2020. Some records remain in ONS pending their purge date.