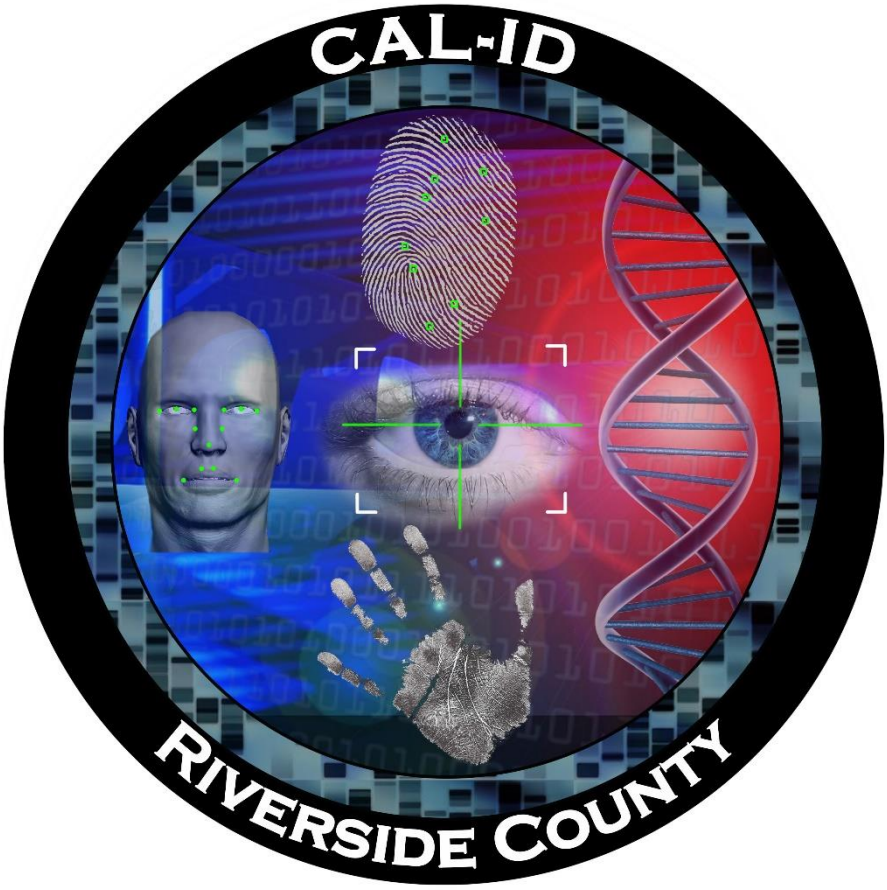

FACIAL RECOGNITION POLICY

Effective Date: March 23, 2020
Last Revised: November 2, 2023

Table of Contents

A. Preface

This policy has been developed by the Riverside Cal-ID Biometric Identification Network (CALID) and is approved for use and publication by the Riverside County Sheriff's Department (RCSD). CALID acknowledges it lacks authority to write policy for individual law enforcement agencies who may utilize CALID's facial recognition program or use its system. However, CALID is responsible for the governance, oversight and operation of its facial recognition system and the program which it provides to the law enforcement community inside and outside Riverside County. This policy shall be used as the foundation for those agencies that choose to utilize the CALID facial recognition system. This policy is intended for CALID personnel and any authorized law enforcement personnel accessing the facial recognition system. Participating agencies may choose to implement their own policy or impose greater restrictions on their employees' use of the CALID facial recognition system as desired. Subsequent agency policy shall not override this policy and all users of the CALID facial recognition system shall be bound by this policy. CALID retains exclusive rights to limit or prohibit an individual or agency's use of the facial recognition system as warranted.

B. Purpose Statement

Facial recognition (FR) technology involves the ability to examine and compare significant characteristics of the human face using biometric algorithms contained within a software application. This technology can be a valuable tool to create investigative leads, reduce an imminent threat to health or safety, and aid in the identification of persons unable to identify themselves or deceased persons. CALID has established access and use of a FR application to support the investigative efforts of law enforcement and public safety agencies within Riverside County. The DataWorks Plus facial recognition software application resides in the CALID digital mugshot system (DMS) and is also known as WebMug.

It is the purpose and intent of this policy to provide Riverside County law enforcement personnel with standards, guidelines, and recommendations for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of the FR program. This policy will ensure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals.

Further, this policy will delineate how FR requests are received, processed, stored, and responded to. The California Criminal Offender Records Information (CORI) Information Bulletin 13-04-CJIS and the United States Federal Trade Commission's Fair Information Practice Principles (FIPP) form the core of the privacy framework for this policy.

This policy assists Riverside County law enforcement agencies and its personnel in:

- Increasing public safety and improving state and local security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.

- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

All deployments of the FR application are for official use only and considered law enforcement sensitive. The provisions of this policy are provided to support authorized uses of FR information.

C. Policy Applicability and Legal Compliance

This policy was established to ensure that all images are lawfully obtained, including FR probe images obtained or received, accessed, used, disseminated, retained, and purged by CALID. This policy also applies to:

- Images contained in the known identity face image repository, WebMug.
- The face image searching process.
- Any results from FR searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by CALID.
- Lawfully obtained probe images of unknown suspects. Probe images will **not** be stored to an unsolved image file (i.e. watch list), for future searches.

All CALID personnel and authorized users working in direct support of their unit or agency, personnel providing information technology services to CALID, and private vendors, will comply with this FR Policy. Authorized law enforcement personnel tasked with processing FR requests must complete the specialized training referenced in ***Item J.*** prior to using or accessing the FR system.

D. Acquiring and Receiving Facial Recognition Information

CALID's FR system can access and perform FR searches for investigative leads only, utilizing the following CALID owned photograph repositories:

- DataWorks Plus Digital Mugshot System, known as WebMug.

In addition, CALID is authorized to access and perform FR searches for investigative leads only utilizing the following external mugshot repositories:

- Los Angeles County
- Sacramento County
- San Bernardino County
- Santa Barbara County
- San Joaquin County

CALID has authorized the external law enforcement agencies listed below to access the CALID mugshot repository (WebMug) for investigative leads only:

- Los Angeles County
- Sacramento County
- San Bernardino County
- Santa Barbara County
- San Joaquin County

For the purpose of performing FR searches, authorized law enforcement personnel will submit probe images directly through the FR application in DMS for the authorized uses only as described in this policy.

CALID personnel, and authorized requesting or participating agencies, will not violate the First, Fourth, and Fourteenth Amendments and will not perform or request FR searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

CALID will contract only with commercial FR companies or subcontractors that provide an assurance that their methods for collecting, receiving, accessing, disseminating, retaining, and purging FR information comply with applicable local, state, and federal laws, statutes, regulations, and policies and that these methods are not based on unfair or deceptive information collection practices.

E. Use of Facial Recognition Information

Access to or disclosure of FR search results will be provided only to those individuals who are authorized to have access, for legitimate law enforcement purposes (e.g., enforcement, reactive investigations, records) only, and to IT personnel charged with the responsibility for system administration and maintenance.

CALID will prohibit access to and use of the FR system, including dissemination of FR search results, for the following purposes:

- Non-law enforcement (including but not limited to personal purposes), CORI violation.
- Any purpose that violates the U.S. Constitution or laws of the State of California, or United States, including the protections of the First, Fourth, and Fourteenth Amendments.
- Harassment and/or intimidation of any individual or group.
- Solely for immigration enforcement purposes.
- ~~Searches of facial images obtained from body-worn cameras (BWC). Video footage, or still images from video footage, obtained on BWC shall not be run through the automated facial recognition system and manual requests will not be processed by an examiner~~ (Pursuant to AB 1215. SB 1038 failed to extend AB 1215 indefinitely, the ban expired January 1, 2023.)
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

CALID's FR system is ***not*** connected to the Department of Motor vehicles (DMV) photo repository. CALID's FR system does not search against publicly available social media or other photo repositories. CALID does not connect the DMS system to any interface that performs live video surveillance, including but not limited to, surveillance cameras, license plate readers, drone footage, and BWC. The DMS system is configured to conduct FR analysis from a recorded video or still image(s). Recorded video is uploaded into the DMS system, a selected frame is captured from the video and submitted for a FR search.

F. Requests for Facial Recognition Services

Law enforcement personnel (police, sheriff, state, and federal) may request FR searches to assist with identifying a person who has been lawfully detained or for an investigative lead through CALID. Automated search requests may be sent via the employee's agency email to: facerec@riversidesheriff.org. Manual search requests to be completed by CALID FR unit staff may be sent via the employee's agency email to: photoid@riversidesherif.org. Law enforcement personnel submitting manual search requests will require the following minimum information:

- Requesting Agency
- Requester Name
- Requester Phone Number
- Requester Email
- Request Date
- Reason For Search
- Case/File Number, if applicable
- Number of Images Submitted

CALID personnel and authorized users will review each request prior to processing to ensure compliance with this policy and applicable laws. Authorized users unsure if a FR search request conforms to this policy should seek guidance from the CALID Manager prior to conducting the requested search.

A FR search result (automated or manual) provided by CALID or authorized users is an investigative lead only. The lead is **NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT, NOR PROBABLE CAUSE TO ARREST.** Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

CALID personnel and participating agency personnel working in direct support of their unit or agency, personnel providing information technology services to CALID, or private contractors, will comply with applicable laws and policies concerning privacy, civil rights, and civil liberties (P/CRCL) of individuals, including, but not limited to:

- California's Criminal Offender Record Information (CORI)
- Office of Privacy and Civil Liberties, U.S. Department of Justice, Criminal Justice Information Services (CJIS) Security Policy
- Fair Information Practice Principles
- Code of Federal Regulations (CFR), Title 28 (28 CFR) – Judicial Administration, Department of Justice
- Health Insurance Portability and Accountability Act (HIPPA) Privacy Rule: A Guide for Law Enforcement, U.S. Department of Health and Human Services (HHS)
- Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S.C. 2721 and 2725

G. Acceptable Search Reasons

The following search reasons are acceptable for an authorized user to access, conduct, or request a search within the DMS FR application:

- A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a credible threat to any individual, the community, or the nation and that the information is

relevant to the criminal conduct or activity.

- An active or ongoing criminal investigation.
- To assist in the identification of a person who has been legally detained by law enforcement for investigative and/or enforcement purposes.
- To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.
- To assist in the identification of a person who lacks capacity or is otherwise unable to identify him or herself (such as an incapacitated, deceased, or otherwise at-risk person).
- To investigate and/or corroborate tips and leads.
- For comparison to determine whether an individual may have obtained one or more official state driver's licenses or identification cards that contain inaccurate, conflicting, or false information.
- To assist in the identification of potential witnesses and/or victims of violent crime, or human trafficking.
- To support law enforcement and other public safety agencies in critical incident responses.

H. Automated Facial Recognition Searches

CALID provides mobile automated FR searches to authorized law enforcement personnel to assist in determining the identity of individuals they come in contact within the field. All potential candidates are considered **advisory in nature only** and any subsequent verification of the individual's identity, such as a mobile fingerprint identification, or follow-up investigative action, is based on the participating agency's standard operating procedures. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods. No individual shall be arrested **solely** on the FR results.

Automated FR searches may be performed by law enforcement personnel while on duty and in their lawful and official capacity. Automated FR searches can be conducted for investigative and/or enforcement purposes and may also be used in a non-mobile environment when useful and applicable. Legitimate law enforcement purposes include, but are not limited to (refer also to ***Use of Facial Recognition Information, Item E. and Acceptable Search Reasons, Item G.***):

- For persons who are legally detained for offenses that:
  - Warrant arrest or citation.
  - Are subject to lawful identification requirements and are lacking positive identification in the field.
- For a person who an officer reasonably believes is concealing his or her identity and has a reasonable suspicion the individual has committed a crime other than concealing his or her identity.
- For persons who are unable or unwilling to identify themselves and who are a danger to themselves or others.
- For the identification of a person who lacks capacity to identify him or herself (such as a special needs individual or an elderly person with dementia).
  - In this instance, another separate FR database dedicated strictly to the Special Needs Registration Program (SNRP) may be utilized to try and identify the subject. The separate SNRP database is only to be searched when there is reason to believe the individual may be registered with the SNRP. See the RCSD Department Standards Manual, Policy 336 for further information regarding the

SNRP and its use of photos in an FR database.

- For those who are deceased and not otherwise identified.

CALID has established the following **guidelines** for automated FR searches:

- Authorized law enforcement personnel (requester/s) may utilize the automated facial recognition application only via a department or government-authorized and managed email system.
- Automated searches shall only be performed pursuant to a requester's lawful duties.
- Automated searches are recommended for field citation releases.
- Prior to utilizing a facial recognition search, an officer should first attempt to ascertain an individual's identity by means other than a facial recognition search, such as requesting identification, using a mobile fingerprint scanner, etc.
- Prior to capturing an individual's image, officers must have a lawful detainment or meet the "No Consent" criteria described as:
    - Individuals who lack the capacity or ability to identify themselves and who are a danger to themselves or others.
    - Those individuals who are deceased and not otherwise identified.
- Generally, force should not be used to capture a subject's image. Officers are directed to follow their agency's use of force policy.

CALID has established the following **procedure** for automated FR searches and system response:

- The requester will submit the probe image to the automated facial recognition system via email, which will compare the probe image against the templates of known images contained in the CALID DMS repository without human intervention.
- The requester will receive an email response providing a link to view the list of most likely candidate image(s), ranked by a computer-evaluated similarity score.
    - If no viable candidate(s) are found, the requester will be informed of the negative results. Requesters may then forward the submission to the CALID FR unit for a manual search to be conducted by an examiner, if desired.
- The requester should complete a basic visual comparison of the candidate images to the subject to make a visual judgment, as well as use standard investigative techniques to determine whether the subject is the same person as a candidate image.
- If the requester is not satisfied with the results of the automated facial recognition search, and does not request a manual search, they shall follow department protocols as if an automated facial recognition search was not available.
- The requester should delete the probe image once the investigation has been completed, unless the image is to be retained as evidence.
- All personnel receiving the results of an automated FR search are cautioned that the resulting candidate leads do not provide positive identification of any subject, are considered advisory in nature as an **investigative lead only**, and do not establish probable cause to obtain an arrest warrant without further investigation.

I. Manual Facial Recognition Requests

- Authorized law enforcement personnel (requester/s) will submit a probe image of a subject of interest via their department or agency email.
- Trained CALID users and/or participating agency's authorized trained users (also called

face examiners) will initially submit probe images without filters, and use a filtered search as a secondary search, if needed. The resulting candidates, if any, are then visually compared with the probe images and thoroughly examined. Examiners shall conduct a morphological comparison of the images, biometric identifiers, and biometric information in accordance with their training.

  - If a viable candidate is found, a Manual Search Report (refer to ***Item S.*** Appendices) will be generated by the examiner and disseminated to the requester, providing an image of the candidate lead, demographic information for the candidate lead and other pertinent information.
  - If no viable candidate(s) are found, the requester will be provided a negative Manual Search Report by the examiner. In the case of a negative result, the known images examined by the user will not be provided on the report.

- Examiners may submit search and subsequent examination results for a peer review of the probe and candidate images for validation by other authorized, trained users in the event a candidate lead is provided.
- All personnel receiving the results and/or reports of a manual FR search are cautioned that the resulting candidate leads do not provide positive identification of any subject, are considered advisory in nature as an **investigative lead only**, and do not establish probable cause to obtain an arrest warrant without further investigation.

J. Training

CALID requires that local law enforcement personnel who will be users of the FR software and completing face comparisons attend training prior to accessing the FR system. Courses presented by the Federal Bureau of Investigation's (FBI) Biometric Training Unit and other reputable training companies are suitable for this requirement. The training should follow the recommendations of the Facial Identification Scientific Working Group (FISWG) *"**Minimum Training Criteria for Usage of Facial Recognition Systems***." If an agency creates their own additional training, it should not conflict with CALID's policies or training.

Before access to CALID's FR software is authorized, the CALID Manager requires individuals to acknowledge the implementation of and their adherence to this facial recognition policy. CALID will provide all authorized users with a printed or electronic copy of this FR policy and require a written acknowledgment of receipt of this policy. CALID personnel will retain all written acknowledgements for reporting purposes as required by law or requested by RCSD Administration or an outside agency department head.

CALID's policy on FR training ensures:

- The user is familiar with the history of facial comparisons in forensic science to include past methods, such as the Bertillon method, and their shortcomings.

  The user understands common terminology and is able to define facial comparison and automated facial recognition as well as explain the differences between the two processes.

- The user demonstrates an understanding of the basics of image science including components of digital images, properties of video, and detection of alteration within images.
- The user is familiar with the proper handling of evidentiary media, protection of evidentiary media, and generating working copies.
- The user understands the principles of comparison. These principles include:

    - Process of the scientific method Analysis, Comparison, Evaluation and Verification (ACE-V).
    - Assessment of image quality to determine the value for comparison based on visibility of facial features.
    - Methods of comparison, such as morphological analysis (the FISWG recommended technique)
    - The differences between class and individual characteristics, as well as those of transient and stable characteristics.
    - The value of verification by a second trained reviewer.
    - The effects of cognitive bias, to include confirmation bias.
- The user has a general knowledge of automated facial recognition systems including system operation, input/output, and facial recognition algorithm limitations such as image conditions and obstructions (e.g., glasses, hats, scarves)
- The user is familiar with basic image processing operations such as brightness and contrast adjustments, rotations, and cropping.
- The user has basic knowledge of the bones that comprise the skull and the overlying musculature.
- The user has a basic knowledge of the FISWG Facial Image Comparison Feature List of Morphological Analysis.
- The user is aware of the variable nature of the human face over time, the level of permanence of individual features, and understands the results of aging.
- The user is aware of alterations of the face, both temporary and permanent.
- The user is prepared for court testimony in regard to FR, regardless of their specific job duties. Note: Basic training for court testimony, including knowledge of individual agency policies and procedures is beyond the scope of this document and is the responsibility of the user's agency.

K. Sharing and Disseminating Facial Recognition Information

CALID has established requirements for external law enforcement agencies to request FR searches. (Refer to ***Requests for Facial Recognition Services, Item F.)***

California DOJ's CORI Information Bulletin 13-04-CJIS cites California Penal Code 11105 which identifies who has access to DOJ CORI and under what circumstances it may be released. Access is based upon the "right to know" and the "need to know." The "right to know" is defined as "authorized access to such records by statute" and the "need to know" is defined as "the information is required for the performance of official duties or functions."

FR search information **will not** be:

- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by CALID's agreement with a commercial vendor.

- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, CALID and the originating agency may agree in writing in advance that CALID will disclose FR search information as part of its normal operations, including disclosure to an external auditor of the FR search information.
- Disclosed to unauthorized individuals or for unauthorized purposes.

Per California DOJ's CORI Information Bulletin 13-04-CJIS, CALID will not confirm the existence or nonexistence of FR information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

L. Data Quality Assurance

Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and should be documented to indicate what enhancements were made including the date and time of change.

Authorized users will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a FR search. It is recommended that the results of this process be documented for court testimony purposes, if later required.

Authorized users acknowledge the results, if any, of a FR search to be advisory in nature as an investigative lead only. FR search results are NOT considered positive identification of a subject.

CALID and its vendor will perform routine maintenance, upgrades/enhancements, testing, and refreshes of the FR system to ensure proper performance, including the following:

- Designated, trained personnel shall assess the FR system on a regular basis to ensure performance and accuracy.
- Malfunctions or deficiencies of the system will be reported to CALID staff (951-955-2740) as they arise. Any malfunction or deficiency not repaired within 48 hours will be reported to the CALID Manager.

The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of poor-quality leads or inclusion of individuals as candidates. CALID will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of FR information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. CALID will correct the information or advise the process for obtaining correction of the information.

M. Disclosure Requests

CALID will disclose FR information to the public in accordance with DOJ's CORI Information Bulletin 13-04-CJIS, the RCSD Media Information Bureau (MIB), and the RCSD Information Services Bureau (ISB) policy when applicable. California Public Records Act (CPRA) requests can be made to the CPRA unit via the official RCSD website or emailing CPRA@riversidesheriff.org. CALID will work jointly with the Department's CPRA unit and participating agencies in receipt of a CPRA request to provide the requested information. CALID will keep a record of all information provided to the CPRA unit to comply with requests and the CPRA unit will keep a record of what information is disclosed.

N. Security and Maintenance

CALID will comply with the CJIS and RCSD Technical Services Bureau security policies, to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity.

CALID and the DMS vendor will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor 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. Access to FR information from outside the facility will be allowed only over secure networks.

All results produced by participating agencies as a result of a FR search are disseminated by secured electronic means (such as official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.

All individuals with access to information or information systems, including the FR system will report a suspected or confirmed breach to the CALID Manager as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

Following the assessment of a suspected or confirmed breach and as soon as possible, the CALID Manager will notify the originating agency from which the entity received FR information of the nature and scope of a suspected or confirmed breach of such information.

CALID adheres to DOJ's CORI Information Bulletin 13-04-CJIS. CALID will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

All FR equipment and FR software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

CALID and the DMS vendor, will store FR information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.

Authorized access to the FR system will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check through their agency. Usernames and passwords to the FR system are not transferable, must not be shared by and between personnel, and must be kept confidential.

O. Information Retention and Purging

All mugshot images are stored in the DMS indefinitely. Occasionally, images are sealed with a court order or removed for a variety of legitimate reasons (e.g., duplicate, test, inappropriate). CALID conducts periodic audits to remove such images or when directed to do so by a valid court order issued by a competent court of law.

P. Accountability and Enforcement

CALID is accountable to the RAN Board and the citizens of Riverside County. CALID will be accessible to the public regarding FR information collection, receipt, access, use, dissemination, retention, and purging practices via CPRA request. This FR Policy will be available in electronic form on the RCSD website.

The CALID Manager will be responsible for receiving and responding to general inquiries and complaints about the entity's use of the FR system, as well as complaints regarding incorrect information or P/CRCL protections in the image repository maintained by CALID. The CALID Manager may be contacted at P.O. Box 512 Riverside, CA 92502 (951) 955-2740.

CALID will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the FR system requirements and with the provisions of this policy and applicable law. This will include logging access to FR information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and may entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions.

CALID personnel or other authorized users shall report errors, malfunctions, or deficiencies of FR information and suspected or confirmed violations of the FR policy to the CALID Manager, or designee.

The CALID Manager, or designee, will review and update the provisions contained in this FR policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the FR system and public expectations. RCSD Administration reserves final decision making authority of the FR policy.

If CALID personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding FR collection, receipt, access, use, dissemination, retention, and purging, the CALID Manager will:

- Suspend or discontinue access to the FR system by the participating agency, or the authorized user.
- Notify the agency Department head of the suspected violation and initiate appropriate disciplinary/administrative actions, following a thorough review of the alleged policy violations.
- Refer the matter to agency criminal investigators for investigation and review to determine if criminal prosecution is appropriate.

CALID reserves the right to establish the qualifications and number of personnel having access to the FR system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this facial recognition policy.

Q. Governance and Oversight

CALID first purchased and utilized FR software in the year 2010. CALID enhanced the FR program, including new access to participating counties' mugshot repositories through the California Facial Recognition Interconnect (CAFRI), in the year 2013. All law enforcement personnel (police, sheriff, state, and federal) may request searches through the CALID FR system for lawful purposes related to their official duties. CALID retains ownership of the FR system and the management of the images and information it contains.

Primary responsibility for the operation of CALID; its FR program, application, system, operation, and coordination of personnel; the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of FR information; P/CRCL protections and the enforcement of this policy is assigned to the CALID Manager.

The CALID Manager will designate a FR unit staff member and/or systems administrator to be responsible for the following duties:

- Oversee CALID FR training, to ensure the policy information is disseminated and users are in compliance with the policy as well as applicable laws, regulations, and standards.
- Review the results of FR searches, to ensure the most likely candidate image lead, if any, is returned to the requesting agency.
- Confirm through random audits that protocols are followed, to ensure that FR information (including probe images) is purged in accordance with the CALID retention policy, unless determined to be of evidentiary value (refer to ***Information Retention and Purging, Item O.***)
- Conduct and document random evaluations of user compliance with system requirements, CALID's FR policy, and applicable laws, as appropriate (refer to ***Accountability and Enforcement, Item P.***)
- Ensure personnel seeking access to the FR system meet all prerequisites stated in this policy prior to being authorized to use the FR system, and document as such.

R. Definitions

Access—Information access is being able to get to particular information on a computer, usually requiring permission to use. Web access means having a connection to the internet through an access provider or an online service provider.

Agency— A law enforcement entity that is authorized to contribute images and/or biometric information to a facial recognition system and/or is authorized to access or receive, request, or use facial recognition information from CALID's facial recognition system for lawful purposes through its authorized individual users. Participating agencies adhere to conditions defined in a formal agreement (e.g., MOU or interagency agreement) between CALID, who operates the facial recognition program, and the participating agency.

Algorithm—An algorithm is a procedure or formula for solving a problem, based on conducting a sequence of specified actions. A computer program can be viewed as an elaborate algorithm. Algorithms can perform calculation, data processing, and automated reasoning tasks and are widely used throughout all areas of information technology.

Authorization—The process of granting a person, a computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, a computer process, or a device requesting access that is verified through authentication. See Authentication.

Automated Facial Recognition—Automated facial recognition (AFR) software compares patterns within the field of computer vision. Such approaches do not rely upon intrinsic models of what a face is, how it should appear, or what it may represent. In other words, the matching is not based on biological or anatomical models of what a face, or the features that make up a face, look like. Instead, the algorithm performance is entirely dependent upon the patterns which the algorithm developer finds to be most useful

for finding similarities. The patterns used in AFR algorithms do not correlate to obvious anatomical features such as the eyes, nose or mouth in a one-to- one manner, although they are affected by these features.

Biometric Template—A biometric template is a set of biometric measurement data [or features] prepared by a facial recognition system from a face image. The prepared set can be compared to a probe image. An enrolled image, on its own, is not a biometric template.

Biometrics—A general term used alternatively to describe (1) a characteristic or (2) a process. (1) a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition or (2) automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Candidate Images—The possible results of a facial recognition search. When facial recognition software compares a probe image against the images contained in a repository, the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to or most likely resemble the probe image to warrant further analysis. A candidate image is an investigative lead only and does not establish probable cause to obtain an arrest warrant without further investigation.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term civil liberties refer to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first 10 amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights—The term civil rights refer to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federal- or state- protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term civil rights" involves positive (or affirmative) government action to protect against infringement, while the term civil liberties involve restrictions on government.

Comparison—The observation of two or more faces to determine the existence of discrepancies, dissimilarities, or similarities.

Consent—In general use, consent means compliance in or approval of what is done or proposed by another; specifically, the voluntary agreement or acquiescence by a person of age or with requisite mental capacity who is not under duress or coercion and usually who has knowledge or understanding. Related to automated facial recognition, consent means an individual agrees to have their photo taken.

Criminal Activity—A behavior, an action, or an omission that is punishable by criminal law.

Data Breach—The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for a purpose other than authorized purposes. An entity's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted.
- Posting such information on the internet.
- Unauthorized employee access to certain information.
- Moving information to a computer otherwise accessible from the internet without proper information security precautions.
- Intentional or unintentional transfer of information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail.
- Transfer of information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Data Quality—Refers to various aspects of the information, such as the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of data quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, data quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes, but which is not available to everyone.

DMS—Digital Mugshot System

Enhancement—Image enhancement is the process of adjusting digital images so that the results are more suitable for display or further image analysis. For example, removing noise, sharpening or brightening an image may make it easier to identify key features.

Enrolled Image—In FR context, biometric enrollment is capturing a face image, creating a biometric template from the image, and entering the template into a facial recognition repository. The biometric template from the enrolled image is used as a reference for facial recognition comparisons and searches. Enrolled images do not include probe images.

Examiner—An individual who has received training in the facial recognition system and morphological comparisons. Examiners have a working knowledge of the limitations of facial recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for facial recognition searches and to perform one-to-many and one-to-one face image comparisons. Examiners are also called trained users within this document.

Facial Comparison—The manual examination of the differences and similarities between two face images or a live subject and a face image for the purpose of determining if they represent the same or different persons.

Facial Recognition (FR)—The automated searching for a reference image in an image repository by comparing the facial features of a probe image with the features of images contained in an image repository. A facial recognition search will result in one or more likely candidate images, ranked by computer evaluated similarity or it will return a negative result.

Facial Recognition Program—An entity's facial recognition initiative that includes the management of human components (requesters, examiners, authorized users), ownership and management of the facial recognition system (technical components), and the establishment and enforcement of entity-wide processes, policies, and procedures.

Facial Recognition Software/Technology—Third party software that uses specific proprietary algorithms to compare facial features from one specific picture, a probe image, to many others that are stored in an image repository to determine most likely candidates for further investigation.

Facial Recognition System—The technical components of a facial recognition program, such as hardware, software, interfaces, image repositories, biometric templates, auto-generated candidate lists, etc. While some entities own such a system, others may only have authorized access to another entity's facial recognition system.

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are a set of eight internationally recognized principles that guide information privacy policies both within government and the private sector. FIPP elements are incorporated into information privacy laws, policies, and governance documents around the world. Law enforcement entities and all other integrated justice systems should endeavor to apply FIPPs where practicable and ensure compliance with applicable law.

The eight principles are:

1. Purpose Specification
2. Data Quality/Integrity
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards
6. Accountability/Audit
7. Openness/Transparency
8. Individual Participation

Features—Observable class or individual characteristics. The components of biometric templates.

Filtering—In the facial recognition context, filtering uses relevant physical facial attributes such as eye color, nose shape, eyebrow position, hairline, and other attributes to compare, select, and narrow results.

Image Analysis—The assessment of an image to determine suitability for comparison, including the ability to discriminate significant features.

Image Evaluation—Ascertaining the value of dissimilarities and similarities between two face images, where an examiner assesses the value of the details observed during the analysis and comparison steps and reaches a conclusion.

Individual Characteristics—Characteristics allowing one to differentiate between individuals having the same class of characteristics (e.g., freckles, moles, and scars).

Investigative Lead—Information which could potentially aid in the successful resolution of an investigation but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

Known Image—The image of an individual associated with a known or claimed identity and recorded electronically or by other medium (also known as exemplars). Known images are enrolled and stored in an image repository.

Law Enforcement (LE) Agency—An organizational unit, or subunit, of a local, state, or federal agency with the principal functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws. LE agencies further investigations of criminal behavior based on prior identification of specific criminal activity with a statutory ability to perform arrest functions.

Law Enforcement Purpose—A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, protection of public or private structures and property, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the P/CRCL of Americans.

Manual Facial Examination—Comparison and evaluations of the probe image and the candidate images by a trained biometric images specialist.

Morphological Comparison—The direct comparison of class and individual face characteristics without explicit measurement. See Comparison and Manual Facial Examination.

Negative Result—A negative result from a facial recognition search is one in which the probe image was not determined to be sufficiently similar to or resemble any of the reference images contained in an image repository.

One-to-Many Face Image Comparison—The process whereby a probe image from one subject is compared with the features of reference images contained in an image repository, generally resulting in a list of most likely candidate images.

One-to-One Face Image Comparison—The process whereby a probe image from one subject is compared with a most likely candidate image that is also from one subject.

Peer Review—An additional layer of verification of facial recognition search results. Examiners submit facial recognition search results to other authorized and trained examiners, or peers, for an independent review of the probe and most likely candidate images.

Personally Identifiable Information (PII)—Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual.

Pose—Orientation of the face with respect to the camera, consisting of pitch, roll, and yaw. Common poses are frontal and profile.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of PII. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); and to avoid being seen or overheard in particular contexts.

Probe Image—Any face image which is lawfully obtained pursuant to an authorized criminal investigation and used by facial recognition software for comparison with the face images contained within a face image repository.

Public—Includes any individual and any for-profit or nonprofit entity, organization, or association; any governmental entity for which there is no existing specific law authorizing access to the entity's information; media organizations; and entities that seek, receive, or disseminate information for whatever reason. Public does not include any employees of CALID or participating agencies; people or entities, private or governmental, who assist CALID in the operation of the justice information system; and public entities whose authority to access information collected or received and retained by CALID is specified by law.

Purge—A term that is commonly used to describe methods that render data unrecoverable in a storage space or destroy data in a manner that it cannot be reconstituted.

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Repository—A location where a group of images of known individuals and biometric templates are stored and managed. An image repository is searched during a facial recognition search process whereby a probe image is used by facial recognition software for comparison with the images (or features within images) contained in the image repository.

Request—A request received by CALID to utilize facial recognition in support of a criminal investigation. Submissions will not contain original evidence. Images received in a request or submission will not be stored as enrolled images within the facial recognition system.

Requester— An employee or an individual representing a participating agency who is authorized to access and/or receive results from CALID's facial recognition system and reports from CALID examiners/users for lawful purposes.

Search—For the purposes of facial recognition, the act of comparing a probe image against an image repository.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Security safeguarding of information is a Fair Information Practice Principle (FIPP).

User—An employee or an individual representing CALID or a participating agency who is authorized and trained to access, use, and receive results from, CALID's facial recognition system for lawful purposes and who is trained to complete morphological comparisons. Also often referred to as face Examiners.

S. Appendices

Cal-ID/Facial Comparison Unit *"Manual Search Report"* forms