ARJIS TACIDS Policy

PREFACE

The ARJIS TACIDS policy is intended to provide ARJIS member law enforcement agencies uniform guidance regarding their appropriate use of facial recognition field identification tools. ARJIS staff participated in the Nlets sponsored preparation of its *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field* to better describe the privacy issues surrounding law enforcement agencies' utilization of facial recognition technologies in the field. These policies were generated in response to the discussions contained in that report and are supplemented by ARJIS specific guidelines.

The intent of this policy is to address the privacy issues raised by the use of facial recognition systems to identify individuals in public.

Part A: PURPOSES FOR COLLECTING FACIAL RECOGNITION INFORMATION

101 Law enforcement agencies collect, compare, and disseminate facial images to aid in the visual identification of:
a) Individuals who come into direct contact with criminal justice practitioners;
b) Individuals who are reasonably suspected of having committed a crime; and
c) Individuals who a law enforcement officer reasonably suspect is about to commit a crime.

102 Law enforcement agencies may request facial recognition comparison information from the ARJIS TACIDS (Tactical Identification System):
a) To assist an officer in assessing the situation and evaluating any threats to his own safety;
b) To conduct a criminal investigation;
c) Where appropriate, facial images may be accessed and disseminated to aid in locating a missing person or an individual for whom a warrant has been issued.

Comments
1. Utilizing facial recognition technology assists in accurate and timely identifications, solving crimes and enhancing public safety.
2. Confirming an individual's identity can help an officer ascertain whether the suspect is wanted for another offense or has a record of violence or a recorded mental health disorder. Section 102 (a) is intended to cover any situation in which verifying an individual's identity can help officers assess their specific situation and evaluate any threats to their own safety or possible danger to potential victims.

Part B: COLLECTION OF FACIAL IMAGES BY LAW ENFORCEMENT AGENCIES

201 Individuals in personal contact with law enforcement officers. Law enforcement officers may collect facial images of individuals with whom they are in personal contact for the purpose of submitting those images to a facial recognition field identification tool in the following circumstances:
a) With the individual's consent;
b) When identifying the individual will assist the officer in assessing the situation and evaluating any threats to his own safety;
c) When state law requires individuals to identify themselves to police officers;
d) When the individual is lawfully detained and when the suspect's identity is related to the investigation of the suspicion that originally justified the detention; and
e) When the individual is lawfully detained and using the facial recognition field identification tool does not prolong the detention beyond the time reasonably required to complete the investigation of the suspicion that originally justified the detention.

202 Individuals not in personal contact with law enforcement officers. Law enforcement officers may capture facial images for the purpose of submitting those images to a facial recognition field identification tool in the following circumstances:
a) As part of the investigation of a crime; and
b) As part of an intelligence-gathering effort that:

i) Is conducted in compliance with the U.S. Department of Justice's rules and policies governing criminal intelligence systems at 28 C.F.R. Part 23; and

ii) Limits the collection of facial images from areas that reasonably relate to an individual's political, religious or social views, associations, or activities to instances directly related to criminal conduct or activity.

203 No individual shall be physically detained, nor the individual's movement otherwise hindered, for the exclusive purpose of collecting their facial image for submission to a facial recognition field identification tool.

Comments
1. Law enforcement officers should adhere to their agency's existing policies regarding the detention of individuals. A facial recognition field identification tool does not expand an officer's legal authority to detain persons.
2. Section 201 is intended to govern those situations when an individual is in the officer's presence. The wording of Section 201 was deliberately broad; it contemplates, but is not limited to, the use of facial recognition comparison to identify: individuals driving without a license; individuals in possession of a forged or altered driver license or identification card; individuals lawfully detained as part of a *Terry* stop; deceased individuals found without identification; and missing persons who are unable to identify themselves.

3. Section 202 is intended to govern situations when the individual being photographed is not in the officer's presence. These situations could include the capturing of facial images from a distance as part of surveillance operations. These situations may also include the use of surveillance camera footage, artist sketches, or publicly available photographs such as those contained on social networking Web sites to identify suspects or subjects of a criminal intelligence file.

4. The use of the word "area" in the limiting language of Section 202(b)(ii) is not limited to physical locations, such as churches or political rallies, but also includes electronic forums where speakers or participants' photos may be displayed.

Part C: ACCESS TO FACIAL RECOGNITION FIELD IDENTIFICATION RESULTS

301 Law enforcement officers should not request facial recognition field identification results when an individual presents a valid driver license or state identification card unless:
a) The officer reasonably suspects the driver license or identification card is forged, altered, or otherwise fraudulent; or
b) The officer reasonably suspects the individual is presenting, as his or her own, a driver license or identification card issued by a DMV to another person.

302 Where practical, and where it will not negatively impact officer safety, law enforcement officers should first request verification of an individual's identity through a query of their name, date of birth, and other self-reported identifiers. When verification is not possible, or if the officer reasonably suspects the self-reported information is false, officers may request facial recognition field identification results.

303 Where practical, law enforcement officers should submit publicly observable demographic information related to the facial image when requesting facial recognition field identification results.

304 Law enforcement officers shall only access the personally identifying or biographical information of individuals whose facial image is contained in the results of a facial recognition field identification query:

a) After determining that the individual's mugshot or other ARJIS stored image reasonably matches the facial image submitted for comparison; or
b) When the personally identifying or biographical information would reasonably assist the officer in verifying the identity of the person.

Part D: DISSEMINATION OF FACIAL RECOGNITION INFORMATION

401 Where it will further a legitimate criminal justice function, the facial images obtained through the use of a facial recognition field identification tool may be shared with other criminal justice agency personnel.

402 No personally identifying information, including but not limited to facial images, obtained through the use of a facial recognition field identification tool shall be disseminated to members of the general public or news media. This prohibition is subject only to the following specific exceptions:

a) Public safety exception – Where the head law enforcement official or the elected prosecutor of a jurisdiction reasonably determines that an individual poses a threat of substantial harm to the public, facial images and relevant personally identifying information may be released to the public.

i) Documentation of determination – A determination that the public safety exception at Section 402(a) applies must be documented in writing and retained in the same manner as a secondary dissemination log.

ii) Limited release of information – The release of facial images and personally identifying information must be limited to information that could reasonably protect the public from harm.

b) Photo line-up exception – A suspect's facial images may be used in a photo line-up to further the particular investigation for which the suspect's image was requested.

c) Warrant exception – Where a warrant has been issued for a known suspect, and where the suspect's facial image has been verified by an independent witness, the suspect's facial image can be publicly disclosed for the purposes of locating the suspect or protecting the public.

d) Missing person exception – Upon its verification by an independent third-party, the facial image of an individual reported missing can be publicly disclosed to help authorities locate the missing person.

403 Dissemination of facial images obtained through the use of a facial recognition field identification tool, other than as set forth in Sections 401 and 402, is prohibited.

1. In addition to conducting law enforcement investigations, the phrase "legitimate criminal justice function" includes, but is not limited to, aiding in the identification of individuals appearing before a court and gathering criminal intelligence data. Officers authorized to use a facial recognition field identification tool will be trained regarding the legitimate criminal justice purposes for which facial images and facial recognition comparison results may be used.
2. Section 402(c) provides for the release of facial images and personally identifying information where an arrest warrant has been issued for the offender. The independent witness verification is added to help ensure that the photograph to be released is accurately attributed to the wanted individual.
3. State freedom of information laws and court orders operate outside the scope of these policies and procedures. This part intentionally does not address these types of disseminations.

Part E: RETENTION OF FACIAL RECOGNITION INFORMATION

601 Retention of captured facial images.

a) Law enforcement agencies may retain facial images captured as part of their investigation records.

b) Law enforcement agencies must retain facial images captured in accordance with the review and purge provisions of the U.S. Department of Justice's rules and policies governing criminal intelligence systems at 28 C.F.R. Part 23.20(h).

602 Retention of facial recognition field identification results.

a) Law enforcement agencies may retain candidate galleries and facial images provided by ARJIS in response to a query via a facial recognition field identification tool where there is an evidentiary or investigative need.
b) When a law enforcement agency uses a facial recognition field identification tool for intelligence gathering purposes, candidate galleries and facial images provided by ARJIS must be retained in accordance with the review and purge provisions of the U.S. Department of Justice's rules and policies governing criminal intelligence systems at 28 C.F.R. Part 23.20(h).

603 Retention of audit and dissemination logs.
a) ARJIS shall retain its log of all transactions made via the facial recognition field identification tool. Automated audit logs of facial recognition field identification tool transactions will be maintained for the same length of time as other ARJIS transaction logs.
b) ARJIS may retain a copy of the query response, including any facial images of potential candidate matches, as part of the facial recognition field identification tool's audit logging capabilities.

Comments
1. When a law enforcement officer submits a facial image for identification, ARJIS will respond with a candidate gallery of individuals whose biometric template resembles that of the submitted photograph. Officers in the field will then make a determination as to whether the individual whose identity they seek is one of the candidates provided by the ARJIS.
2. Facial images collected in the field may become important if an officer takes investigative steps in reliance upon the ARJIS information obtained due to the image's submission. As such, law enforcement officers may retain the facial image and candidate images obtained via a facial recognition field identification tool as part of their investigation records. Law enforcement agencies should follow their local retention policies concerning investigation records.
3. ARJIS facial images and personally identifying information would be made available over the ARJISnet network to assist law enforcement offers in the visual identification of individuals, not to compile a separate database of ARJIS information. Audit logs are not designed to be easily searchable and cannot be searched based upon the characteristics of a facial image itself. Audit logs are searched only in limited circumstances, such as during an investigation of system misuse and when ordered by a court. Access to the audit logs is restricted to only personnel authorized to perform audits.

Part F: DATA QUALITY

601 Operational guidelines to ensure quality of facial recognition field identification results.
a) ARJIS may limit its response to a law enforcement officer's request for facial recognition comparison to those facial images in its database that resemble the submitted image within a certain level or degree of similarity.
b) ARJIS may limit the facial images provided to a requesting law enforcement officer in response to a request for facial recognition comparison to those taken within a certain period of time.

c) ARJIS may rank or otherwise sort the facial images provided to a requesting law enforcement officer in response to a request for facial recognition comparison.

602 Individual right to review or challenge facial recognition field identification information.
a) An individual has a right to access, review, or challenge facial images captured by a law enforcement agency only as permitted under the statutes and rules of the jurisdiction and provided for by agency policies.

Comments
1. Section 601 includes several steps ARJIS can take to help ensure that the facial images they provide in response to a facial recognition inquiry are of the best quality available.
2. Sections 601(a) and 601(c) include a distinction between ranking and similarity scoring. Ranking, as provided in 601(c), means sorting the facial images by their resemblance to the submitted image regardless of how similar the facial images/templates may be. Ranking is essentially a "top 10 list" of similar images available from the ARJIS.
3. Section 601(b) would operate by limiting responses to those facial images that resemble the submitted image within a certain threshold. For instance, ARJIS may choose to only provide images that score a 50% similarity or above.
4. Because better quality facial images produce better facial recognition results, officers will be trained to take and submit the best quality photographs possible.
5. Officer training also plays a substantial role in addressing any issues surrounding the reliability of facial recognition software. Officers will be trained as to why facial recognition software cannot be 100% accurate and that individuals who have a mugshot image might not be recognized by the system every time a picture of the person is submitted. Officers, not automated facial recognition software, will make decisions as to whether an ARJIS facial image matches an individual encountered in the field.

Part G: ACCOUNTABILITY FOR FACIAL RECOGNITION INFORMATION

701 Audit logs. Queries and responses transmitted via a facial recognition field identification tool must be logged by ARJIS. Transaction audit logs must contain the following information:
a) The identity of the agency requesting facial recognition;
b) The purpose code for the facial recognition query;
c) The date and time the transaction occurred;
d) Header information, including the identity of the agency that responded to the inquiry; and
e) An ARJIS-assigned number and date of image capture that uniquely identifies the facial images transmitted in response to the facial recognition query or a notation that no facial images were available.

702 Secondary dissemination logs. Law enforcement agencies that disseminate ARJIS facial images or personally identifying information obtained through the use of a facial recognition field identification tool shall maintain a secondary dissemination log.
a) A secondary dissemination log must contain the following information:
i) A copy or description of the facial image record disseminated;

ii) The date and time the information was disseminated;
iii) The identity of the individual to whom the information was released, including their agency and contact information; and
iv) The purpose for which the facial image will subsequently be used.
b) Law enforcement agencies make their secondary dissemination logs available to ARJIS upon request.

703 Monitoring system use and conducting audits.
a) The use of a facial recognition field identification tool over the ARJISnet network will be monitored and audited in accordance with ARJIS policies to guard against inappropriate or unauthorized use.
b) Law enforcement agencies utilizing a facial recognition field identification tool must:

i) Have an internal policy regarding the appropriate use of the facial recognition field identification tool;

ii) Certify that each officer using the facial recognition field identification tool has been trained in accordance with Section 801 of this policy; and

iii) Limit the use of the facial recognition field identification tool to only those officers who have been trained in its use.

Comments
1. ARJIS currently maintains a log of all transactions conducted over its network.
2. ARJIS may need to keep copies of the actual images to provide a complete audit trail for a particular transaction because it is not possible to recreate an exact duplicate candidate gallery by simply re-submitting a facial image through the facial recognition system at a later date. Audit information retained by ARJIS is only available to authorized personnel and logs are only searched in limited circumstances, such as during an investigation of system misuse and when ordered by a court.

Part H: POLICY AWARENESS AND TRAINING

801 User training. Law enforcement agencies must train each officer utilizing a facial recognition field identification tool in the following areas:
a) The proper collection of facial images for facial recognition purposes;
b) How to take high quality facial images in the field;
c) How to interpret the facial recognition comparison results obtained via a facial recognition field identification tool and not base decisions entirely upon the comparison results;
d) The appropriate use and sharing of information obtained from a facial recognition field identification tool; and
e) How facial recognition field identification tool policies will be enforced, including any penalties for committing violations of the policy provisions.

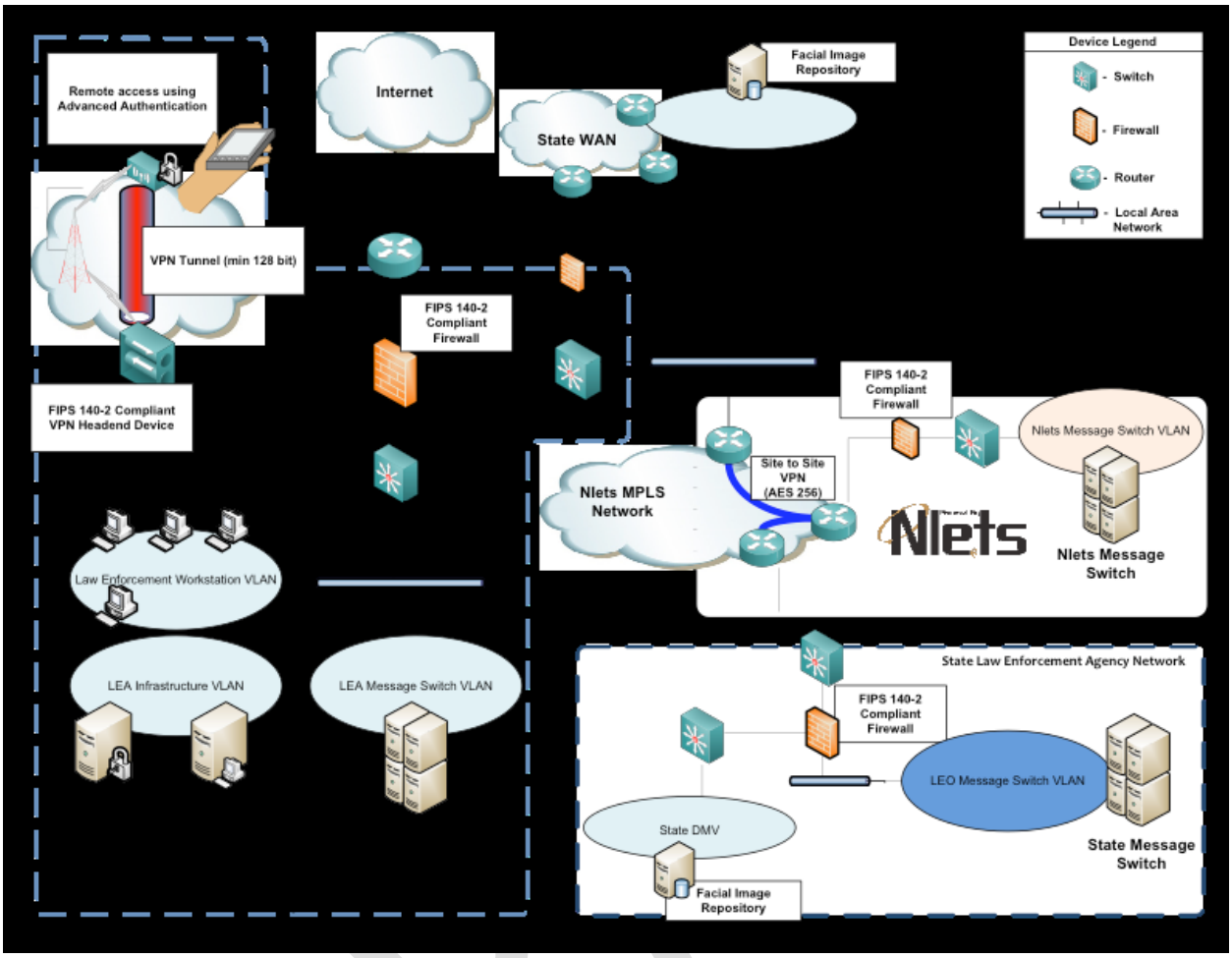
902 Policy awareness and policy updates.

a) Participating law enforcement agencies will be provided access to, and acknowledge a thorough understanding of, any policies and procedures governing the use of a facial recognition field identification tool via the ARJIS network.
b) Participating law enforcement agencies shall regularly review and update their policies and practices concerning the sharing of facial recognition field identification information to comport with any changes in relevant laws and regulations governing biometric data systems and data sharing.

Comments
1. Section 801(a) requires officers to be trained as to when they can and cannot capture a facial image for submission to ARJIS for comparison with mugshot records.
2. Because a camera's age, calibration, and compensation for ambient light factors can impact facial recognition results, Section 801(b) requires officers to be trained how to take the highest quality photos possible given the conditions officers are likely to encounter in the field. Officers should also be trained on their agency's policies regarding the removal of dark sunglasses or other facial coverings.
3. Additional information concerning some aspects of capturing quality facial images can be found in ISO/IEC TR 29794-5, *Information technology — Biometric sample quality — Part 5: Face image data*.
4. Section 801(c) ensures that officers have an understanding of the limitations of facial recognition systems. This understanding is necessary to evaluate the ARJIS facial recognition results, in addition to any other available identifying information, to make the best determination possible as to a subject's identity.
5. Educating users on the proper use of facial recognition systems and ARJIS facial images is a continual process that must be regularly updated as laws and regulations governing biometric data systems and ARJIS data systems change. Thus, Section 802 requires participating agencies to stay informed of any changes in relevant law and to update their policies accordingly.

Part I: SECURITY SAFEGUARDS

901 Network Connection Diagram
a) The diagram below is a graphical representation of the various connectivity paths that may be used to share facial images. The diagram identifies critical policy enforcement points typical within the criminal justice community that are required to share criminal justice information. The diagram does not attempt to depict all possible connectivity options, rather, it is a general overview of the interconnection of law enforcement and criminal justice agencies that may participate in the exchange of facial images.



902 Site Security

a) Facial images and personally identifying information will be treated as CJI

b) Establish an environment to protect the physical security of computer site and related infrastructure technology supporting Exchange of Facial Images including information system servers, networking equipment, security equipment and monitoring facilities, electronic and printed storage facilities (both online and offline) and personal computing devices. Physical security controls must provide adequate security to protect against unauthorized use.

c) Maintain a physically secure location for the storage of CJI in compliance with CJIS Security Policy Version 5.0 Section 5.9.1.

d) Access to the physically secure location shall be logged. Logging entries must include accurate date and time records capturing the asserted identity of the person granted access. Entry logs must be maintained for 1 year.

e) All visitors to physically secure areas must be accompanied by an authorized user at all times. Names of visitors must be recorded in a visitor log, to include date and time of visit, name of visitor,

purpose of visit, name of accompanying authorized user, and date and time of departure. The visitor logs shall be maintained for 1 year.

f) All devices physically or logically connected to the LEA network with access to CJI must be protected against use or access by unauthorized persons.

903 System Integrity
a) Maintain a level of system integrity commensurate with the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of CJI.

b) Maintain a log of all access and dissemination of CJI including record requests and responses for a period of no less than 1 year.

c) Periodically assess the inquiries of facial recognition systems made through the LEA network and subsequent information dissemination to determine accordance with applicable policies and regulations set forth in the following:
I. U.S. Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Security Policy, version 5.0 (02/2011);
II. 28 C.F.R. Part 20; and
III. 28 C.F.R. Part 23.

d) All dissemination of CJI will be considered "Sensitive but Unclassified, For Official Use Only", bearing the label "FOR OFFICIAL USE ONLY" on any printed pages.

e) All resources including CJI intended for printing such as report output shall bear a header and/or footer with the label "FOR OFFICIAL USE ONLY". All resources including CJI intended for printing such as report output shall bear a header and/or footer with the label "FOR OFFICIAL USE ONLY."

f) Other electronic resources not typically intended for printing that lack this designation will be stamped with the label "FOR OFFICIAL USE ONLY" prominently on the cover page.

904 Personnel Security
a) Maintain a level of system integrity commensurate with the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of CJI.

b) All personnel involved in the handling, maintenance and processing of CJI data must meet the requirements for personnel security as defined in the CJIS Security Policy section 5.12.

905 System Security
a) All systems processing, handling or storing CJI shall be subject to compliance with the Agency's Information Security Policy.

b) Under no circumstances may CJI be stored on systems whose access is governed by policies that vary from the Agency's Information Security Policy.

c) All reasonable measures should be taken to ensure that the ability to identify and account for all activities on a CJI system are preserved, including but not limited to the following: (i) Recording of successful user login and logout;

(ii) Recording of failed user login attempts;
(iii) Recording of the unique identifiers for queries and the corresponding responses with the associated request for facial images;
(iv) All IP addresses associated with the authentication and access of request and response data transferred through the ARJIS network.

d) Unique identification and authentication credentials will be used for all personnel accessing facial imagery. Under no circumstances will authorized personnel share their assigned authentication credentials with other authorized or unauthorized users.

e) Remote access to systems capable of generating requests for facial images will require multi-factor authentication credentials allocated by agency personnel.

f) Auditing controls will be used to identify the changes and attempted changes to system or data resources, including the identity of the user requesting the change.

g) Electronic access control mechanisms will be used on communications devices (routers, firewalls) to limit access to CJI systems. (i) Access to CJI systems should be granted following an explicit grant policy, denying all traffic not explicitly permitted by electronic access control mechanisms.
(ii) Access attempts that are rejected should be logged identifying the source address information for the system requesting access and the requested service that was rejected.

h) Provide a system for ensuring the confidentiality of CJI over public networks such as the Internet.

i) All CJI transmitted across an untrusted network shall, at minimum, be encrypted using AES-128.

j) Devices responsible for encryption shall meet the requirements for FIPS 140-2.