2-110   FACIAL RECOGNITION MANAGEMENT SYSTEM

Related SOP(s), Form(s), Other Resource(s), and Rescinded Special Order(s):

A. Related SOP(s)

   2-16   Reports

B. Form(s)

   None

C. Other Resource(s)

   None

D. Rescinded Special Order(s)

   None

2-110-1   Purpose

The purpose of this policy is to provide guidelines for Department personnel when using the Facial Recognition Management System in order to describe the procedures, requirements, and expectations surrounding the use of the system.

2-110-2   Policy

It is the policy of the Albuquerque Police Department's (Department) Investigation Bureau units to use facial recognition software when investigating criminal activity or identifying a person who may be in danger. Furthermore, when the facial recognition software identifies an individual, that information will only be treated as an investigative lead, and further investigation will need to be done to verify an individual's identity.

N/A ### 2-110-3   Definitions

A. Authorized Personnel

   Investigations Bureau personnel that have completed the facial recognition software training, and been approved by the Investigations Services Division (ISD) Commander or designee.

B. Candidate Image

   The possible results of a facial recognition search. When facial recognition software compares the submitted (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.

C. Criminal Activity

A behavior, action, or omission that is punishable by law.

D. Facial Recognition Software

Third-party software that uses specific proprietary algorithms to compare facial features from one or more specific images or probe images. These images are stored in an image repository to determine the most likely match of a candidate for further investigation.

E. Investigative Lead

Information that could aid in the successful resolution of an investigation but does not imply positive identification of an individual who is suspected of a criminal act. An investigative lead does not establish probable cause to obtain an arrest warrant without further investigation.

F. Need to Know

Authorized access to sensitive, confidential information but only in order to conduct one's official job duties.

G. Probe Image:

1. An image used by facial recognition software for comparison of images or features contained within the repository; and

2. Lawfully obtained front-facing image of an individual; including, but not limited to, facial images captured by closed circuit cameras, automatic teller machines (ATM), fraudulent bank cards, or photo identification provided by a victim or witness which is used by facial recognition software for comparison with the images contained within a repository.

H. Repository

A database of images and biometric templates which are searched, stored, and managed.

4 | **2-110-4   Rules and Procedures**

A. Facial Recognition Software shall only be used:

1. By authorized Department personnel who have been trained on its proper use;

2. For legitimate law enforcement purposes where criminal activity is being investigated;

3. To identify a subject who lacks capacity due to a medical issue or is otherwise unable to identify themselves and may be a danger to themselves or others; or

4. For persons who are deceased and not otherwise identified.

B. The Investigative Service Division Commander, or their designee, shall oversee the Facial Recognition Program.

C. The Special Investigations Section Lieutenant shall review and authorize any information Department personnel share with entities outside of the Department prior to the information being released.

D. Department personnel who do not have access to the facial recognition software may contact the on-call Strategic Criminal Intelligence Unit Detective if they have a need to run an image through the facial recognition software.

E. Authorized Department personnel who use the facial recognition software shall:

1. Input the image of the person or individual they are investigating into the facial recognition software;

2. Cross-reference the probe image against the images in the repository to identify possible candidate images that warrant further analysis;

3. Treat a candidate's image as an investigative lead;

4. Verify a candidate's identity using other police resources and databases;

5. Diligently establish additional probable cause to substantiate the case;

    a. Charges cannot be solely predicated on a photo array if the lead on the subject originates solely from facial recognition.

7

6. Document the use of facial recognition for incident(s) that lead to an arrest or search warrant in a Uniform Incident Report and upload the search results into the Department's records management system; and

    a. When the search is performed at the request of an officer who does not have access to the facial recognition software, the officer who conducted the search shall complete a supplemental report as outlined in SOP Reports.

7. Only share images and investigative leads with Department personnel who have a need to know, and approved by the lead investigator on the incident.

8. Not use the software for any internal administrative investigations.

E. Department personnel who fail to adhere to any of these procedures shall lose access to the use of the Department-approved facial recognition software.

2-110   FACIAL RECOGNITION MANAGEMENT SYSTEM

Related SOP(s), Form(s), Other Resource(s), and Rescinded Special Order(s):

A. Related SOP(s)

   2-16   Reports~~None~~

B. Form(s)

   None

C. Other Resource(s)

   None

D. Rescinded Special Order(s)

   None

2-110-1   Purpose

The purpose of this policy is to provide guidelines for Department personnel when using the Facial Recognition Management System in order to describe the procedures, requirements, and expectations surrounding the use of the system.

2-110-2   Policy

It is the policy of the Albuquerque Police Department's (Department) Investigation Bureau units to use facial recognition software when investigating criminal activity or identifying a person who may be in danger. Furthermore, when the facial recognition software identifies an individual, that information will only be treated as an investigative lead, and further investigation will need to be done to verify an individual's identity.

N/A ### 2-110-3   Definitions

A. Authorized Personnel

   Investigations Bureau personnel that have completed the facial recognition software training, and been approved by the Investigations Services Division (ISD) Commander or designee.

B. Candidate Image

   The possible results of a facial recognition search. When facial recognition software compares the submitted (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. ~~e results of a facial recognition search.~~

C. Criminal Activity

A behavior, action, or omission that is punishable by law.

D. Facial Recognition Software

Third-party software that uses specific proprietary algorithms to compare facial features from one or more specific images or probe images. These images are stored in an image repository to determine the most likely match of a candidate for further investigation.

E. Investigative Lead

Information that could aid in the successful resolution of an investigation but does not imply positive identification of an individual who is suspected of a criminal act. An investigative lead does not establish probable cause to obtain an arrest warrant without further investigation.

F. Need to Know

Authorized access to sensitive, confidential information but only in order to conduct one's official job duties.

G. Probe Image:

1. An image used by facial recognition software for comparison of images or features contained within the repository; and

2. Lawfully obtained front-facing image of an individual; including, but not limited to, facial images captured by closed circuit cameras, automatic teller machines (ATM), fraudulent bank cards, or photo identification provided by a victim or witness which is used by facial recognition software for comparison with the images contained within a repository.

H. Repository

A database of images and biometric templates which are searched, stored, and managed.

4 2-110-4   Rules and Procedures

A. Facial Recognition Software shall only be used:

1. By authorized Department personnel who have been trained on its proper use;

2. For legitimate law enforcement purposes where criminal activity is being investigated; ~~or~~

3. To identify a subject <u>who lacks capacity due to a medical issue or is otherwise unable to identify themselves</u>~~who forgot their identity~~ and may be ~~in~~ <u>a</u> danger <u>to themselves or others</u> ~~due to a medical issue~~; <u>or</u>~~, such as a subject who has dementia and is lost; or~~.

4. <u>For persons who are deceased and not otherwise identified</u>~~To identify a decedent when no immediate alternative exists~~.

~~4.   .~~

B. The Investigative Service Division Commander, or their designee, shall oversee the Facial Recognition Program.

<u>C.</u> The Special Investigations Section Lieutenant shall review and authorize any information Department personnel share with entities outside of the Department prior to the information being released.

~~C.~~<u>D.</u>   <u>Department personnel who do not have access to the facial recognition software may contact the on-call Strategic Criminal Intelligence Unit Detective if they have a need to run an image through the facial recognition software.</u>

~~D.~~<u>E.</u>   Authorized Department personnel who use the facial recognition software shall:

~~1. Contact the on-call Strategic Criminal Intelligence Unit Detective, if applicable, to run a candidate image through facial recognition software to identify a subject.~~

~~2.~~<u>1.</u>   Input the image of the person or individual they are investigating into the facial recognition software;

~~3.~~<u>2.</u>   Cross-reference the probe image against the images in the repository to identify possible candidate images that warrant further analysis;

~~4.~~<u>3.</u>   Treat a candidate<u>'s</u> image as an investigative lead;

<u>4.</u> Verify a candidate's identity using other police resources and databases; ~~and~~

<u>5. Diligently establish additional probable cause to substantiate the case;</u>

<u>a. Charges cannot be solely predicated on a photo array if the lead on the subject originates solely from facial recognition.</u>

6. Document the use of ~~the~~ facial recognition for ~~all~~ incident(s) that ~~leads~~lead to an arrest or search warrant in a Uniform Incident Report and upload the search results into the Department's records management system~~Mark43 on a case that leads to an arrest or search warrant~~; and~~.~~

    ~~5.~~a. When the search is performed at the request of an officer who does not have access to the facial recognition software, the officer who conducted the search shall complete a supplemental report as outlined in SOP Reports.

7. Only share images and investigative leads with Department personnel who have a need to know, and approved by the lead investigator on the incident.

~~6.~~8. Not use the software for any internal administrative investigations.

E. Department personnel who fail to adhere to any of these procedures shall lose access to the use of the Department-approved facial recognition software.