POLICE DEPARTMENT

Detroit Public Safety Headquarters
1301 Third Street, Suite 7S-751
Detroit, Michigan 48226

Phone 313•596•1800
Fax 313•596•6818

April 3, 2024

Mr. QuanTez Pressley, Chairperson
Board of Police Commissioners
Detroit Public Safety Headquarters
1301 Third Street, Suite 7S-767
Detroit, Michigan 48226

Re: **POLICIES FOR REVIEW**

Dear Chairperson Pressley:

I am pleased to present to you the attached Facial Recognition Policy, new templates for Facial Recognition, and Eyewitness Identification and Lineups Policy that was collaboratively worked on and agreed upon with Philip Mayor, Ramis Wadood, Dan Korobkin, and Nate Wessler of the American Civil Liberties Union (ACLU), Michael Steinberg of the University of Michigan Law School, and the assistance of the United States District Court – Eastern Michigan District.

Should you have any questions, please feel free to contact 2nd Deputy Chief Grant Ha, Legal Advisor to the Chief of Police, Monday through Friday, 8:00 a.m. until 4:00 pm at 313-596-1803.

Sincerely,

JAMES E. WHITE
Chief of Police

JEW/gh

Attachment:

1. Facial Recognition Policy
2. Facial Recognition Templates
3. Eyewitness Identification and Lineups Policy

FSeries 200 Operations	Effective Date	Review Date *Two Years*	Directive Number **203.11**
Chapter 203 – Criminal Investigations			
Reviewing Office *Investigative Operations*			☐ New ☐ Directive ☒ Revised Revisions in *italics*
References			

EYEWITNESS IDENTIFICATION AND LINEUPS

203.11 - 1 PURPOSE

The purpose of this directive is to establish the guidelines for eyewitness identification *procedures involving showups, photo arrays, and live lineups. Erroneous eyewitness identifications have been cited as the factor most frequently associated with wrongful convictions. Therefore, in addition to eyewitness identification, all appropriate investigative steps and methods should be employed to uncover evidence that either supports or eliminates the suspect identification.*

203.11 - 2 POLICY

Members shall strictly adhere to this directive in order to maximize the reliability of identifications, minimize *erroneous identifications, and gather evidence that conforms to established legal procedures.*

203.11 - 3 Definitions

203.11 - 3.1 *Administrator*

The law enforcement official conducting the identification procedure.

203.11 - 3.2 *Double-Blind Presentation*

The administrator conducting the identification procedure does not know the suspect's identity.

203.11 - 3.3 *Filler*

A live person, or a photograph of a person, included in an identification procedure who is not considered a suspect.

203.11 - 3.4 *Live Lineup*

The process of presenting live individuals to an eyewitness for the purpose of identifying or eliminating suspects.

203.11 - 3.5 *Photo Array*
A means of presenting photographs to an eyewitness for the purpose of identifying or eliminating suspects.

203.11 - 3.6 *Sequential*
Presentation of a series of photographs or individuals to a witness and or a victim one at a time.

203.11 - 3.7 *Showup*
The presentation of a suspect to an eyewitness within a short time frame following the commission of a crime to eliminate them as a possible perpetrator. Showups, sometimes referred to as field identifications, are conducted in a contemporaneous time frame and proximity to the crime.

203.11 - 3.8 *Simultaneous*
Presentation of a series of photographs or individuals to a witness and or a victim all at once.

203.11 – 3.9 *Victim*
For purposes of this directive, an individual who is allegedly the victim of a crime and who also meets the definition of Witness under this policy.

203.11 – 3.10 *Witness*
For purposes of this directive, an eyewitness, meaning an individual who saw the suspect in person.

203.11 - 4 Procedures

203.11 - 4.1 *Showups*
The use of showups should be avoided whenever possible in preference to the use of a live lineup or photo array procedure. However, when circumstances require the prompt presentation of a suspect to a witness and or a victim, the following guidelines shall be followed to minimize potential suggestiveness and increase reliability:

a. *Document the witness's and or a victim's description of the perpetrator prior to conducting the showup. This description should be clearly noted as the witness and or victims' description and separate from the description noted by the member;*
b. *Conduct a showup only when the suspect is detained within a reasonable time frame after the commission of the offense and within a close physical proximity to the location of the crime;*
c. *Members shall obtain supervisory approval before conducting a showup;*

d. *Do not use a showup procedure if probable cause to arrest the suspect has already been established;*
e. *Transport the witness and or the victim to the location of the suspect whenever possible. Members shall not transport the suspect to the witness and or victim;*
f. *If possible, avoid conducting a showup when the suspect is in a patrol vehicle, handcuffed, or physically restrained by Department members, unless safety concerns make this impractical;*
g. *Do not take a suspect to the witness's and or victim's residence unless it is the scene of the crime and without the consent of both the suspect and the witness or victim;*
h. *Caution the witness and or victim that the person they are about to see may or may not be the perpetrator – and it is equally important to clear an innocent person. The witness and or victim should also be advised that the investigation will continue regardless of the outcome of the showup;*
i. *Do not conduct the showup with more than one witness and or victim present at a time;*
j. *Separate witnesses and or victims and do not allow communication between them before or after conducting a showup;*
k. *If one witness and or victim identifies the suspect, use a live lineup or photo array for remaining witnesses;*
l. *Do not present the same suspect to the same witness and or victim more than once;*
m. *Do not require showup suspects to put on clothing worn by, speak words uttered by, or perform other actions of the perpetrator;*
n. *Members should avoid words or conduct of any type that may suggest to the witness and or victim that the individual is or may be the perpetrator;*
o. *Remind the witness and or victim not to talk about the showup to other witnesses and or victims until police or prosecutors deem it permissible;*
p. *Videotape the identification process using an in-car or body-worn camera;*
q. *Members shall not use a cellular phone or other mobile communication device for a showup; and*
r. *Members shall document the time and location of the showup, the members present, the result of the procedure, and any other relevant information on their officer's daily report.*

203.11 - 4.2 *Basic Procedures for Conducting a Live Lineup or Photo Array*

1. *A live lineup or photo array may only be administered to a witness and or victim as defined in this policy.*
2. *Prior to conducting a live lineup or photo array, members shall have the witness and or victim provide a recap of the incident to provide clarity that the witness and or victim has actual recollection of the incident and the suspect.*
3. *Prior to conducting a photographic line-up, a supervisor shall ensure that there is an independent basis supported by reliable evidence that the suspect, who will be presented in the line-up, committed the crime. An investigative lead generated by a search using facial recognition technology does not alone constitute an independent basis that the person selected as the lead committed the crime.*
4. *The photographic lineup shall not contain an image derived from facial recognition.*
5. *All photo lineups will be conducted using the sequential, double-blind presentation technique to ensure effective eye-witness identification. This means that an investigator, other than the lead investigator, who does not know who the suspect is, will present the line-up to the witness and or victim. It also means that photographs will be presented one-by-one to the witness and or victim.*
6. *The live lineup or photo array should consist of a minimum of six (6) individuals or photographs. Use a minimum of five (5) fillers and only one suspect.*
7. *Fillers should be reasonably similar in age, height, weight, and general appearance and be of the same sex and race, in accordance with the witness's and or victim's description of the offender.*
8. *Avoid the use of fillers who so closely resemble the suspect that a person familiar with the suspect might find it difficult to distinguish the suspect from the fillers (i.e., twins, look-alikes, facial recognition derived images, etc.).*
9. *Create a consistent appearance between the suspect and the fillers with respect to any unique or unusual features (e.g. scars, tattoos, facial hair) used to describe the perpetrator by artificially adding or concealing that feature on the fillers.*
10. *If there is more than one suspect, include only one in each live lineup or photo array.*
11. *During a double-blind presentation, no one who is aware of the suspect's identity should be present during the administration of the photo array. However, during a live lineup, the witnessing attorney should be present.*
12. *Place suspects in different positions in each live lineup or photo array.*
13. *Neither witnesses nor victims should be permitted to see or be shown any photos or images of the suspect prior to or during the live lineup or photo array other than the photo of the suspect included in the photo array at the time it is administered.*
14. *The live lineup or photo array should be shown to only one witness and or victim at a time; in order to prevent participating witnesses and or victims from being aware of the responses of other witnesses and or victims, members should separate witnesses and or victims and warn them not to communicate with each other about the lineup or images involved in the lineup until all witnesses and or victims have completed the live lineup or photo array.*

15. *Multiple identification procedures should not be conducted in which the same witness and or victim views the same suspect more than once.*
16. *Members shall not use statements, cues, casual comments, or provide unnecessary or irrelevant information that in any manner may influence the witnesses' and or victim's decision-making process or perception. In investigations where facial recognition technology was used prior to the lineup, members shall not inform the witness or victim that facial recognition technology was used or that it generated information contributing to the inclusion of an individual in the lineup.*
17. *The proceeding must be conducted in a fair manner, so as not to be unduly suggestive of the suspect. This is important because any remarks could later be interpreted as an attempt to influence the identification.*
18. *The administrator shall ask the witness and or victim to complete and sign a live lineup or photo array form at the time of the lineup. As part of the form, the witness and or victim shall record their degree of confidence in their identification.*
19. *Live lineup and photo array procedures shall be video and audio recorded, unless doing so is not possible. If a procedure is not recorded, a written record shall be created and the reason for not recording shall be documented. In the case of live lineups that cannot be recorded, members shall take and preserve a still photograph of each individual in the lineup.*
20. *The administrator shall document all parties present during the live lineup.*

203.11 - 4.3 *Photographic Arrays*

Prior to conducting a photographic lineup, a supervisor shall ensure that there is an independent basis supported by reliable evidence that the suspect, whose picture is to be presented in the course of the photo lineup, committed the crime. An investigative lead generated by a search using facial recognition technology does not alone constitute an independent basis.

1. *When creating a photo array, members shall follow the below guidelines:*
   a. *Do not use a facial recognition derived image;*
   b. *Use photos contemporary to when the crime occurred;*
   c. *Use black and white photos only if there are no color photos available;*
   d. *Do not mix color and black and white photos;*
   e. *Use photos of the same size and basic composition;*
   f. *Never mix mug shots with other photos;*
   g. *Do not include more than one photo of the same suspect; and*
   h. *Cover any portions of mug shots or other photos that provide identifying information on the subject – and similarly cover other photos used in the array.*
   i. *Do not use images of people who so closely resemble the suspect that a person familiar with the suspect might find it difficult to distinguish the suspect from the fillers (i.e., twins, look-alikes, facial recognition derived images, etc.).*

2. *The sequential procedure process should be preserved as part of the case file.*
3. A *witnessing* attorney *must* be present if a witness and or victim views photographs when the suspect is in custody. *Members shall obtain the attorney's information including their name, phone number, address, and state bar number.*
4. The attorney shall initial photocopies of all photographs used in the *photo array*. The officer in charge of the case shall ensure that attorneys witnessing the photo *array* are provided with a document outlining the attorney's role at the photo show up.
5. Where a witness and or victim identifies the suspect through the use of photographs, the "totality of the circumstances" test is used to determine whether the photographs utilized are not unnecessarily suggestive of any particular suspect.

203.11 - 4.4 *Live Lineups*

1. *When conducting the live lineup, members shall follow the below guidelines:*

   a. *The administrator of a live lineup must be a blind administrator who does not know the identity of the suspect;*
   b. *Ensure that all persons in the live lineup are numbered consecutively and are referred to only by number; and*
   c. *Document all parties present at the live lineup.*

2. *The officer in charge of the case is responsible for the following:*

   a. *Scheduling the live lineup on a date and at a time that is convenient for all concerned parties, to include the witnessing attorney and any witnesses and or victims;*
   b. *Ensuring compliance with any legal requirements for transfer of the subject to the live lineup location if they are incarcerated at a detention center; and*
   c. *Making arrangements to have persons act as fillers.*

3. A written record, the *Lineup* and Photo Identification Record (DPD355), should include:
   a. Names, *age,* and addresses of all persons whose photographs are to be used in the *live lineup or photo array*;
   b. Physical description of all persons whose photographs are to be used in the *live lineup or photo array*;
   c. Names and addresses of all persons present at the *live lineup or photo array*;
   d. Statements of identifying witnesses and or victims while making the identification; and
   e. *The witness's and or victim's degree of confidence in their identification, as specified above in 203.11 – 4.2(18).*

4. A *live* lineup cannot be avoided by having a witness and or victim view photographs when a formal *live* lineup is *reasonably* possible. *A photo array shall* not *be* conducted if the suspect is in custody, unless:
   a. It is not possible to arrange a proper lineup;
   b. There are an insufficient number of persons available with the defendant's physical characteristics;
   c. The nature of the case requires immediate identification;
   d. The witnesses and or victims are *physically unable to attend a lineup*; or
   e. The subject refuses to participate in a lineup and by this action would seek to destroy the value of the identification.

5. All live lineups shall be photographed.
   a. The name, rank, and assignment of the *member* taking the photograph shall be entered on the *Lineup* and Photo Identification Record (DPD355), in the box designated "OTHERS PRESENT." The photograph shall then be attached to the *Lineup* and Photo Identification Record and become a permanent part of the court file.
   b. The officer in charge of the case shall be responsible for the photographing of lineups conducted at all other locations.

203.11 - 4.5 Refusal of Detainee to Stand in a Lineup

1. If a detainee refuses to stand in a lineup, the following procedures shall be followed:
   a. A determination shall be made as to the availability of a photograph of the detainee suitable for use in photograph identification; and
   b. Photograph identification can be used in lieu of a lineup if the subject refuses to participate in a lineup and, by the subject's action, would seek to destroy the value of the identification.

2. Regardless *of* whether a photograph is available or not, between the hours of 8:30 a.m. to 4:30 p.m. on weekdays and from 8:30 a.m. to 1:00 p.m., on Saturdays, Sundays, and holidays, the Wayne County Prosecutor's Office shall be contacted. *At any other time*, the Control Desk shall be contacted for the number of the on-duty assistant prosecuting attorney.
3. The prosecuting attorney contacted shall be informed if a photograph of the detainee is available or not and shall be informed that the detainee refuses to participate in a lineup. Department members and detention personnel shall be guided by the advice of the prosecuting attorney. Although the Michigan Supreme Court has ruled that forced participation in a lineup does not constitute unreasonable search and seizure, no force shall be exerted to force participation of a detainee in a lineup unless the prosecuting attorney contacted gives direction for such action.

203.11 - 4.6 *Limited Use of Video for Identification Purposes*

Members shall only utilize video to confirm the identity of a subject should the witness and or victim be a close associate or family member of the subject (e.g. mother / father or close friend).

203.11 - 5 Witnessing Attorney

1. *A witnessing attorney shall be present for all live lineups and photo arrays when the suspect is in custody.*
2. *Should the suspect be criminally charged and have obtained a lawyer, then the suspect's defense attorney shall act as a witnessing attorney. In all other cases, the officer in charge of the case shall call Notification and Control who shall identify the witnessing attorney.*
3. The purpose *of the witnessing attorney*'s presence is not to interfere with the conduct of the *live* lineup or *photo array* but to observe the procedures used by the law enforcement officers, so that in any subsequent court proceeding the accused will have a lawyer as a witness to any unfair suggestive procedures that may have been employed during the lineup or *photo array*.
4. Under no circumstances may a lawyer interfere with the conduct of the *live* lineup. While counsel may advise a client not to make incriminating statements, counsel may not advise a client to refuse to participate in the *live* lineup or any requested physical demonstrations *including a voice test, a handwriting sample, to wear certain clothing to assume a stance, to walk or to gesture*. If any lawyer should so advise a client, the Prosecuting Attorney's Office should be notified so that appropriate action may be considered.
5. *The OIC's responsibility is to document any objections, procedural violations, or other concerns voiced by the witnessing attorney during the live lineup or photo array.*

Series 300 Support Services	Effective Date	Review Date Annually	Directive Number 307.5
Chapter 307 – Information System			
Reviewing Office Crime Intelligence			☐ New Directive ☐ Revised
References:			

FACIAL RECOGNITION

307.5 - 1 PURPOSE

The purpose of this policy is to establish acceptable use *of Facial Recognition technology by* the Detroit Police Department (DPD). Facial Recognition shall only be used when there is reasonable suspicion that such use will provide information relevant to an active or ongoing *investigation of a* Part 1 Violent Crime or a first-degree Home Invasion. If *an investigative lead* is *developed* through DPD's *F*acial *R*ecognition *program*, it shall be considered *only* an investigative lead *that shall not be the sole ground for arrest or to apply for an arrest warrant.*

307.5 - 2 Definitions

307.5 - 2.1 Biometric Data

Data derived from one or more intrinsic physical or behavioral traits of humans, to include fingerprints, palm prints, iris scans, and *F*acial *R*ecognition data.

307.5 - 2.2 Examiner

An individual who has received advanced training in the *F*acial *R*ecognition *program* and its features. Examiners have at least a working knowledge of the limitations of *F*acial *R*ecognition. *Examiners are* qualified to assess image quality and appropriateness for *F*acial *R*ecognition searches and to perform one-to-many and one-to-one facial image comparisons.

307.5 - 2.3 Facial Recognition (FR)

The automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity. All Facial Recognition searches must be corroborated by at least two examiners and one supervisor.

307.5 - 2.4 ***First-degree Home Invasion***
A person who breaks and enters a dwelling with intent to commit a felony, larceny, or assault in the dwelling, a person who enters a dwelling without permission with intent to commit a felony, larceny, or assault in the dwelling, or a person who breaks and enters a dwelling or enters a dwelling without permission and, at any time while he or she is entering, present in, or exiting the dwelling, commits a felony, larceny, or assault is guilty of home invasion in the first degree if at any time while the person is entering, present in, or exiting the dwelling either of the following circumstances exists:
(a) The person is armed with a dangerous weapon.
(b) Another person is lawfully present in the dwelling. (MCL 750.110a(2)).

307.5 - 2.5 Part 1 Violent Crimes
For the purposes of this directive, Part 1 Violent Crimes are defined as robbery, sexual assault, aggravated assault, or homicide.

307.5 - 2.6 ***Predictive Analysis***
The process of using data to forecast future outcomes.

307.5 - 2.7 Reasonable Suspicion
The specific facts and reasonable inferences drawn from those facts to convince an ordinarily prudent person that criminality is at hand.

307.5 - 2.8 Statewide Network of Agency Photos (SNAP)
A computer application managed by the SNAP Unit, deployed through the MiCJIN portal, which serves as an investigative tool and a central repository of images from local, state, and federal agencies.

307.5 - 3 Prohibited Uses

307.5 - 3.1 Surveillance
Members shall not use *F*acial *R*ecognition to surveil the public through any camera or video device.

307.5 - 3.2 Live Streaming or Recorded Videos
Members shall not use *F*acial *R*ecognition on live stream or on recorded videos. This prohibition applies to all videos, whether they originate from DPD itself, from private citizens, or from any other source.

307.5 - 3.3 Mobile Facial Recognition
Members shall not use mobile *F*acial *R*ecognition.

307.5 - 3.4 Predictive Analysis
Members shall not use *F*acial *R*ecognition for predictive analysis.

307.5 - 3.5 First Amendment Events

The Detroit Police Department will not violate First, Fourth, and Fourteenth Amendments and will not perform or request *F*acial *R*ecognition searches about individuals or organizations based solely on the following:

a. Their religious, political, or social views or activities;
b. Their participation in a particular noncriminal organization or lawful event; or
c. Their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

307.5 - 3.6 Facial Recognition Use for Immigration Enforcement

DPD members are strictly prohibited from using *F*acial *R*ecognition to assess immigration status.

307.5 - 4 Discipline

1. Any violations to this policy shall be deemed major misconduct. Any misuse of the *F*acial *R*ecognition *program* will be investigated and reviewed for criminality. The remedy for this misconduct is dismissal from DPD.

2. If *F*acial *R*ecognition is used contrary to section 307.5 -3.5 First Amendment Events, DPD shall notify the Board of Policy Commissioners, the Mayor of Detroit, City Council President, and City Council President Pro Tem within 24 hours of the violation.

307.5 - 5 Use of Facial Recognition Technology

307.5 - 5.1 Use Limited to Still Images

Facial *R*ecognition *technology* may only be used on a still image of an individual, *including still images captured from video.*

307.5 - 5.2 Criminal Investigation Required

Members shall not use *F*acial *R*ecognition technology unless *there is reasonable suspicion that use of Facial Recognition technology will provide information relevant to* an active or ongoing *investigation of a* Part 1 Violent Crime or a *first-degree* Home Invasion.

307.5 - 5.3 *An Arrest or Arrest Warrant Request Following Use of Facial Recognition Technology Must Be Supported by Additional Independent Reliable Evidence*

Probable cause must be established for an arrest or for an arrest warrant request must be established using legally authorized methods other than Facial Recognition. Examples of other investigative methods may include, but are not limited to cellular data analysis; eyewitness testimony, establishment of a timeline, DNA, etc. A request for an arrest warrant, or an arrest, shall not be made solely on the basis of an investigative lead developed through Facial Recognition technology in combination with a lineup identification. A request for an arrest warrant, or an arrest, must be supported by additional independent reliable evidence.

307.5 Facial Recognition

307.5 - 5.4 Process for Requesting Facial Recognition

1. Requests for *F*acial *R*ecognition services shall be submitted to the Crime Intelligence Unit (CIU), with photograph(s) to be reviewed, the incident number, the crime type, and other pertinent information.

   a. *Members requesting Facial Recognition services shall affirm that they have completed investigative Facial Recognition training;*

   b. *Members performing Facial Recognition services shall confirm that the requesting member has made the affirmation above.*

307.5 - 5.5 *Process for Performing Facial Recognition*

1. *Prior to the use of Facial Recognition, a CIU examiner shall complete the Real Time Crime Center – Facial Recognition Vetting form, which shall contain:*
   a. *The requestor's name, rank, and command;*
   b. *Confirmation that the requestor has affirmed that they have completed investigative Facial Recognition training;*
   c. *The crime being investigated (Part 1 Violent Crime or first-degree Home Invasion);*
   d. *The role the individual in the probe image is reasonably suspected to have played in the incident; and*
   e. *A description of the probe image quality.*

2. *CIU shall reject a request for Facial Recognition when:*
   a. *The request fails to identify the requestor's name, rank or command;*
   b. *The requestor fails to affirm that they have completed investigative Facial Recognition training;*
   c. *The crime being investigated is not a Part 1 Violent Crime or first-degree Home Invasion;*
   d. *There is not a reasonable suspicion that the individual in the probe image had a role in the commission of the crime; or*
   e. *The quality of the probe image is unsuitable for Facial Recognition.*

3. CIU shall perform *F*acial *R*ecognition searches utilizing SNAP, which includes criminal mug shot images. In the event additional analysis is needed for confirmation of an investigative lead, a formal request may be made to MSP to search the state's database. Any such request must be approved by a CIU supervisor.

4. If the examiner *develops* an investigative lead, the examiner must corroborate this lead with at least one other examiner and a CIU supervisor. *Both examiners and the CIU supervisor shall sign off on the investigative lead.*

5. Upon final approval, CIU shall complete *an investigative lead* report for the requestor. *This investigative lead report must be attached to any request for a warrant for any person named in the investigative lead report.* The investigative lead report shall include the following language:

- "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any *possible* connection or involvement of any subject to the investigation must be determined through further *independent* investigation and investigative resources."

- *"Facial Recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the probe image's quality, lighting, face angle, and face obstructions, among other factors."*

- *"Facial Recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).*

In addition, the investigative lead or vetting report shall also:

- *Disclose the probe image used to run the Facial Recognition search (in both its original form and with any enhancements), and identify all features of the probe image that may reduce the reliability of the Facial Recognition result (such as low light, low pixel density, angle of face, partial occlusion of face, etc.), and any enhancements or modifications made to the probe image during the course of the search process;*

- *Disclose each of the following: the date the investigative lead image was taken, how many other images of the same individual in the investigative lead image exist in the database that was searched, and, if other images of the same individual exist in the database, the dates when each was taken.*

6. *In any case in which charges are filed and in which Facial Recognition technology was used at any stage of the investigation, the member responsible for that investigation shall provide the following to the Wayne County Prosecutor's Office (WCPO):*

    - *Any investigative lead report and vetting report;*

7. In the event that *an investigative lead* cannot be developed, the requestor will be notified that no *investigative lead was developed*.

307.5- 5.6 Outside Agency Using Facial Recognition

An outside agency, or investigators from an outside agency, may request *Facial Recognition* searches *by DPD* to assist with investigations only if the following requirements are met:

a. Prior to making the request, the outside agency has a formalized agreement (e.g. a memorandum of understanding or an interagency agreement) between *DPD* and the outside agency;
b. The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in this directive and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:

   - "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any *possible* connection or involvement of any subject to the investigation must be determined through further *independent* investigation and investigative resources."

c. If any agency is found not in compliance with this Directive, *DPD* shall immediately suspend all Facial Recognition requests until the requesting agency becomes in compliance with this Directive.

307.5 - 6 Governance and Oversight

307.5 - 6.1 LASO & *CIU* Responsibilities

1. The primary responsibility for the operation of *DPD*'s criminal justice information systems, *F*acial *R*ecognition program and system, operations, and the coordination of personnel, the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Local Agency Security Officer (LASO) who is assigned to Technical Services.

2. The LASO will be responsible for the following:

   a. Overseeing and administering the *F*acial *R*ecognition program to ensure compliance with applicable laws, regulations, standards, and policy;
   b. Acting as the authorizing official for individual access to *F*acial *R*ecognition information;
   c. Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status; and
   d. Ensuring that random evaluations of user compliance with system requirements along with this policy and applicable laws are conducted and documented;

3. The commanding officer of *CIU* will be responsible for the following:

   a. Reviewing *F*acial *R*ecognition search requests, reviewing the results of *F*acial *R*ecognition searches, and returning the most likely candidates – or candidate images – if any, to the requestor.
   b. Ensuring and documenting that personnel (including investigators from external agencies who request *F*acial *R*ecognition searches) meet all prerequisites stated in this policy prior to being authorized to use the *F*acial *R*ecognition system.

4. *Members of investigative entities shall be responsible for the following:*

   a. In the event that the Facial Recognition program develops an investigative lead, prior to making any probable cause arrest, or requesting a warrant from the (WCPO), the member must obtain written approval from their commanding officer and the commanding officer of Investigative Operations.

5. *DPD* is guided by applicable laws, regulations, and standards to ensure that privacy, civil rights, and civil liberties are not violated by this Facial Recognition policy or by the *DPD*'s *F*acial *R*ecognition information collection, receipt, access, use, dissemination, retention, and procedure.

307.5 - 6.2 Weekly Report to the Board of Police Commissioners

DPD shall provide a weekly report to the Board of Police Commissioners with information pertaining to the number of *F*acial *R*ecognition requests that were fulfilled, the crimes that the *F*acial *R*ecognition requests were attempting to solve, the number of leads developed from the *F*acial *R*ecognition *program, and the number of searches that did not produce investigative leads*. During this report, if there are any upgrades to the Facial Recognition software, any planned changes to the contract, and/or any confirmed policy violations, *DPD* shall notify the Board of Police Commissioners.

307.5 – 6.3 Annual Report to the Board of Police Commissioners

DPD shall provide an annual report to the Board of Police Commissioners. This annual report shall include a summary of the weekly reports and an evaluation of the efficacy of the *DPD*'s *F*acial *R*ecognition technology. The evaluation shall include any relevant lawsuits or settlements involving *F*acial *R*ecognition, the number of cases *in which* use of the technology assisted in investigations, and any other relevant factors. This shall be disseminated at the Board of Police Commissioners' meeting, and electronic copy shall be provided to the Board for dissemination to the public.

307.5 - 6.4 All Policy Changes to the Board of Police Commissioners
DPD shall seek the Board of Police Commissioners' approval regarding any and all changes to *this manual directive*.

307.5 - 7 Security and Maintenance

1. *DPD* will comply with generally accepted industry or other applicable standards for security 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 *DPD* activity. *DPD*'s *F*acial *R*ecognition system 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 the *DPD*'s *F*acial *R*ecognition information from outside the facility will be allowed only over secure networks. All results produced by *DPD* as a result of a *F*acial *R*ecognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee. When such non-electronic dissemination is made, the member shall memorialize the dissemination as follows:

   a. To whom it was released;
   b. Date and time it was released; and
   c. Manner in which it was released (i.e. if by phone, include the number; if in person, include name of witness who saw it released).

2. All members with access to *DPD*'s information or information systems will report a suspected or confirmed breach to their immediate supervisor who will ensure that the LASO) is notified as soon as possible without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, *or* electric. Following assessment of the suspected or confirmed breach and as soon as practicable, *DPD* will notify the originating agency from which the entity received *F*acial *R*ecognition information of the nature and scope of a suspected or confirmed breach of such information. *DPD* will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

3. All *F*acial *R*ecognition equipment and *F*acial *R*ecognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

4. *DPD* will store *F*acial *R*ecognition information in a manner that ensures that it cannot be modified, accessed, or purged except by members authorized to take such actions.

5. Authorized access to the *DPD*'s *F*acial *R*ecognition system will be granted only to members whose positions and job duties require such access and who have successfully completed a background check and required training.

6. Usernames and passwords to the *F*acial *R*ecognition system are not transferrable, must not be shared by *DPD* members, and must be kept confidential.

7. The system administrator (LASO) will ensure that all manufacturer- generated default passwords are replaced with secure passwords before web-based interfacial of the system become operational. User passwords must meet the standards outlined in Manual Directive 307.4, Criminal Justice Information Systems (CJIS).

8. Queries made to *DPD*'s *F*acial *R*ecognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.

9. *DPD* will maintain an audit trail of requested, accessed, searched, or disseminated *F*acial *R*ecognition information. An audit trail will be kept for a minimum of one (1) year of requests, access, and searches of *F*acial *R*ecognition information for specific purposes and of what *F*acial *R*ecognition information is disseminated to each individual in response to the request. Audit logs will include:

    a. The name and unit of the law enforcement user;
    b. The date of access;
    c. Case number; and
    d. The authorized law enforcement or public safety justification for access including a relevant case number.

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT.** Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources.

Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors.

Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REAL TIME CRIME CENTER — FACIAL RECOGNITION INVESTIGATIVE LEAD

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT**. Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REQUEST #:	23-00				
REQUEST DATE/TIME:					
REPORT NUMBER:					
CRIME:	☐Homicide ☒Robbery/Carjacking ☐Aggravated Assault/NFS ☐CSC 1/CSC 3 ☐Home Invasion 1				
REQUESTER NAME:		**RANK:**	Choose an item.	**COMMAND:**	
REASON:	☒ Reasonable Suspicion of a Part I Violent Crime or First-Degree Home Invasion ☐ Physical Incapacity/Mental Incapacity/At-Risk Person/Deceased Person (Homicide Only)				
IMAGES:	**ORIGINAL IMAGE**	**INQUIRY IMAGE**	**INVESTIGATIVE LEAD**		
IMAGE SOURCE:	Choose an item.	Choose an item.	SNAP	**Date**	
IMAGE ENHANCEMENTS:	Choose an item.	Choose an item.	None		
# OF IMAGES PRODUCED IN GALLERY:		**# OF LEAD IMAGES IN DATABASE:**		**DATES OF LEAD IMAGES:**	
NAME:					
ALIAS:					
DOB:					
DL/PID #:					
SID #:		**FBI #:**			
ADDRESS:					
SOCIAL MEDIA:					
INCARCERATION STATUS:	Choose an item.	**SOURCE:**	Choose an item.	**DATE:**	
INVESTIGATIVE LEAD PROCESS:	☒ Statewide Network of Agency Photos (SNAP) ☒ DataWorks Plus ☐ Forwarded to Michigan State Police (MSP) for additional assistance				
DATE/TIME FINALIZED:					
CIU PERSONNEL:					
CIU PEER REVIEWER:					
SUPERVISOR:					

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT**. Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

FURTHER INVESTIGATION WAS COMPLETED TO DETERMINE THE NECESSARY PROBABLE CAUSE TO PROCEED WITH AN ARREST OF THE INDIVIDUAL AND/OR SUBMISSION OF A WARRANT:

- ☐ CODIS Match
- ☐ AFIS hit
- ☐ CDR warrant results
- ☐ PEN warrant results
- ☐ Social Media warrant results
- ☐ Witness Statements
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____

INVESTIGATIVE OPERATIONS:

Prior to an arrest of an individual and/or submission of a warrant, the information was reviewed and:

- ☐ APPROVED
- ☐ DENIED

Investigate Operations Captain (print): _____

Signature: _____ **Date:** _____

COMMANDING OFFICER:

Prior to an arrest of an individual and/or submission of a warrant, the information was reviewed and:

- ☐ APPROVED
- ☐ DENIED

Commanding Officer (print): _____

Signature: _____ **Date:** _____

REAL TIME CRIME CENTER — FACIAL RECOGNITION VETTING

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT**. Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REQUEST DATE/TIME:					
REPORT NUMBER:					
CRIME:	☐Homicide ☐Robbery/Carjacking ☐Aggravated Assault/NFS ☒CSC 1/CSC 3 ☐Home Invasion 1				
REQUESTER NAME:		**RANK:**	Choose an item.	**COMMAND:**	
IMAGE SOURCE:			**NUMBER OF IMAGES:**		
REASON:	☒ Reasonable Suspicion of a Part I Violent Crime or First-Degree Home Invasion ☐ Physical Incapacity/Mental Incapacity/At-Risk Person/Deceased Person (Homicide Only)				
PER POLICE REPORT, SUPPLEMENTS, AND DETECTIVE NOTES:					
PROBE ROLE IN CRIME:	Choose an item.				
SUSPECT KNOWN:	Choose an item.				
PHOTO QUALITY:					
FILE SIZE:		**DIMENSIONS:**			
RACE:		**SEX:**			
FACIAL OBSTRUCTIONS:					
FACE ORIENTATION:					
IMAGE BRIGHTNESS:					
TATTOOS/FACIAL PIERCINGS/BIRTH MARKS:					
NUMBER OF USABLE IMAGES:					
STATUS OF REQUEST:	Choose an item.				
IF REJECTED, WHY?					
ANALYST:		**DATE/TIME:**			
REVIEWER:		**DATE/TIME:**			
SUPERVISOR:		**DATE/TIME:**			

Intel Number:	**23-**

Revised: 12/6/2023