an on-duty supervisor must be notified immediately following the emergency. Violations of this directive will result in the personal equipment being confiscated as evidence.

5-117 Response to Emergency Call Out

All personnel, unless physically incapable, will respond to duty when called, regardless of off-duty status.

5-118 Automated License Plate Readers

The purpose of Automated License Plate Readers (ALPRs) is to help identify stolen vehicles, stolen license plates, or locate vehicles that have been entered into the hot list databases described below. ALPRs will be used in accordance with state and federal laws, and in a manner consistent with departmental written directives and appropriate privacy concerns. The data captured will be used exclusively for official law enforcement purposes.

Definitions:

Automated License Plate Reader (ALPR) – Equipment consisting of cameras and other computer hardware/software used to automatically recognize and interpret the characters on vehicle license plates. This data is then compared to a hot list of license plates.

Confirmation – A hit must be verified through the active database in which the license plate was entered. Example, a hit on a stolen license plate that was originally entered into NCIC, must be verified through NCIC as per departmental written directives. A hit on the hot list alone is not confirmation.

Data Download - Automatic updating of the hot list.

Hit – Visual and/or audio notification of a match between a scanned license plate and a license plate on the hot list.

Hot List - A database populated with specific license plates related to a law enforcement concern. The databases include, but are not limited to NCIC, OLETS, municipal court, or local data entered by CIU.

Manual/Local Entry – License plate information that is manually entered into the hot list by CIU personnel.

System Administrator- Manages the technical aspects of the server (maintenance and connections) and establishes access accounts for ALPR users.

General Statements

Only officers who have successfully completed the department's training program on ALPRs shall operate the ALPR. ALPR equipped vehicles will only be assigned to divisions authorized by the Chief of Police. Officers should remember that a license plate number does not identify a specific person; rather it simply identifies a specific license plate.

Equipment

When assigned to a vehicle equipped with an ALPR system, the officer shall ensure that the equipment is turned on and functioning properly during their entire tour of duty. Any ALPR equipment malfunction or damage will be immediately reported to a supervisor. The supervisor will notify the system administrator via e-mail of the malfunction/damage. All maintenance or repairs to ALPR equipment will be performed by radio shop personnel.

ALPR Hit

When a hit is obtained by the ALPR, the officer will visually verify the license plate scanned and confirm the status of the license plate/vehicle prior to taking any enforcement action. Officers will not rely on the hit alone to take enforcement action.

Officers will use appropriate techniques and tactics to deal with a license plate/vehicle where a hit has been confirmed. This may include contacting a supervisor, requesting additional officers, conducting a felony stop or dealing with an unoccupied vehicle.

Data Entry and Update

The hot list is automatically updated twice per 24 hour period (2 a.m. and 2 p.m.), except for manual entries. CIU personnel will add or remove manual/local entries as needed.

Data Retention and Sharing

Data will be purged from the system once the maximum retention period of sixty (60) days has been reached, unless the information has become evidence in a specific criminal investigation. In those cases the applicable data shall be downloaded from the server and maintained in accordance with appropriate evidence and chain of custody procedures.

ALPR data will not be shared as part of a law enforcement information database. However, other law enforcement agencies may request ALPR information related to specific criminal investigations in their jurisdiction.

Data Access

ALPR data will be used only by members of the Oklahoma City Police Department who have been properly trained in the use of ALPR for a legitimate law enforcement purpose.

All data gathered by Oklahoma City Police Department ALPRs will be maintained securely according to current CJIS standards. Requests for searches/inquiries may be made by any commissioned Oklahoma City Police Department member subject to the provisions of this directive.

5-119 Facial Comparison Program

It is the purpose of this directive to provide Oklahoma City police personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a facial comparison program. This directive will ensure that all facial comparison uses are consistent with authorized purposes while not violating privacy, civil rights, and the civil liberties of individuals. Furthermore, this directive will delineate the manner in which requests for facial comparison are received, processed, catalogued, and distributed.

Individuals shall not be arrested based solely on the results of the facial comparison system.

Facial comparison technology uses biometric algorithms within a software application to analyze and compare distinguishing facial features. This process is supplemented by physical image comparisons conducted by trained personnel.

This technology is a valuable tool for:

A. Detecting and preventing criminal activity;
B. Addressing imminent threats to health or safety;
C. Identifying unknown victims;
D. Locating and identifying missing persons; and
E. Assisting individuals unable to identify themselves.

The Oklahoma City Police Department has implemented procedures for the use of facial comparison technology to support the investigative efforts of its employees.

5-119.1 Definitions

Candidate Images - Images identified by the facial comparison system as potential matches to a probe image. These candidate images are accompanied by basic biographical data.

Facial Comparison - The automated searching for a reference image against a probe image utilizing facial features.

Facial Comparison Program - The Oklahoma City Police Department's facial comparison initiative that includes the management of human components (supervisors, analysts, authorized users), ownership and management of the facial comparison systems, and the establishment and enforcement of department-wide processes and directives.

Facial Comparison System - The technical components of a facial comparison program, such as hardware, software, interfaces, image repositories, biometric templates, autogenerated candidate lists, etc.

Enhancement - The procedure of improving the quality and information content of the candidate image for facial comparison by applying filters. Enhancements may include but are not limited to the following:

A. Contrast - The variance between the light and dark parts of the image. Adding contrast makes darks darker and brights brighter.
B. Crop - Removal of unwanted outer peripheral areas from an image to accentuate or isolate the subject matter from background details.
C. Exposure - Overall brightness or darkness of the image. Highlights control the brighter parts of the image. Shadows control the darker parts of the image. Whites set the brightest point in the image. Blacks set the darkest point in the image.
D. Filter - The technique of altering or adjusting various characteristics of an image, such as size, exposure, or contrast without altering or adjusting the physical features of the individual in the image.
E. Flip - Reversing the image across an axis to create a horizontal or vertical mirror image.
F. Opacity - The transparency of an image, typically utilized when overlaying an image for direct comparison.
G. Overlay - A layered candidate image on top of the probe image to make feature comparisons between images by adjusting the opacity.
H. Rotate - Changing the orientation of an image by turning it on an axis in a clockwise or counterclockwise direction.
I. Sharpen - The contrast on an image is increased anywhere a light area meets a dark area to make the image more clear and crisp.

Image Repository - A collection of images of known individuals whose basic biographical data has been previously obtained (e.g., booking photographs).

Probe Images - An image of an unknown individual submitted to the facial comparison program in an attempt to identify that individual.

Unsolved Image File - Images of unknown individuals that have been submitted to the facial comparison system as probe images which did not yield a verified, positive candidate image.

5-119.2 Guidelines for the Use of the Facial Comparison System

Facial comparison technology shall be used for official use only and shall be considered law enforcement sensitive. Use of facial comparison technology may be approved:

A. When an employee has reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in planning criminal conduct or activity that presents a threat to any individual, the community, or the country, and that the potential information obtained from the facial comparison system is relevant to the investigation of the criminal conduct or activity;
B. To generate a lead on a potential suspect of an active or ongoing criminal investigation who is involved in criminal activity, when reasonable suspicion exists the suspect is indeed committing a crime;

C. To assist in identifying a person who is unable to identify themselves due to conditions such as:
   1. Neurocognitive disorders or other medical conditions;
   2. Unconsciousness resulting from criminal activity, drug, or alcohol effects;
   3. An endangered minor separated from parents/guardians, or;
   4. Death.
D. To identify the victims of crimes when there is reasonable suspicion to believe the unknown individual is the victim of a crime. Examples include but are not limited to:
   1. Human trafficking;
   2. Child sexual abuse material;
   3. Domestic violence; and
   4. Any other crime where the individual may or may not be aware of their victimization.
E. To identify and/or locate missing individuals including but not limited to:
   1. Missing and/or endangered children; and
   2. Missing and/or endangered adults.

Information provided from the facial comparison system shall be treated as an investigative lead only and will not rise to the level of probable cause for an arrest. All investigative leads must be corroborated through additional investigative methods and probable cause developed through those additional methods. Results from the facial comparison system shall not be treated as a positive identification of any suspect.

Information from the facial comparison system shall not be provided to outside law enforcement agencies, or any other entity, unless that agency is part of a joint criminal investigation with the Oklahoma City Police Department and has received the approval from the Special Operations Division commander. If the facial comparison program is utilized to assist another law enforcement agency, all aspects of this directive shall be adhered to.

Facial comparison technology will be used only after an incident has occurred, the probe image is obtained, and the request process completed, reviewed, and approved.

Facial comparison technology will only be used in compliance with 28 CFR Part 23 requirements:

A. Information collected and maintained for criminal intelligence purposes shall be premised on circumstances that provide reasonable suspicion as defined in the U.S. Department of Justice 28 CFR, Part 23 for Criminal Intelligence Operating Systems.
B. Personnel shall not collect or retain any information 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 race, ethnicity, citizenship, origin, age, disability, gender, or sexual orientation.

Only software owned and operated in the United States of America may be used. Additionally, any software must be independently tested by the National Institute of Standards and Technology (NIST) to ensure accuracy across all racial demographics and genders.

Facial comparison technology shall not be used under the following circumstances:

A. Facial Recognition in Live Video Feeds
   1. This directive does not authorize the use of Live Facial Recognition (LFR), which relies on live video feeds to provide real-time identification of individuals. Unlike facial comparison, LFR does not require physical comparison after using facial recognition technology. This directive only permits the use of facial comparison technology after an incident has occurred, a probe image has been obtained, and the review and approval process outlined above has been completed.
B. Monitoring Daily Activities of Individuals or Groups
   1. Facial comparison technology is not used to track the geolocation, timeframe, or daily activities of any person or group. Its use is strictly limited to incident-based evaluations of probe images.
C. Identifying individuals known or believed to be under the age of sixteen (16), with the exception of the following circumstances:
   1. Investigation on a matter related to public safety or the person's safety;

2. Victim identification, when the person's welfare is at risk;
3. Conduct or investigations of violent felonies;
4. Conduct or activity that may violate federal or state laws; or
5. To help protect against the spread of Child Sexual Abuse Material.

5-119.3 Requests for the Use of the Facial Comparison System

Requests for facial comparison must be made in the following manner:

A. Police employees shall submit requests for facial comparisons to their supervisor. The supervisor will review the request and if appropriate, forward the request to an on-duty or on-call Criminal Intelligence Group supervisor on the authorized form;
B. All requests shall include an incident number (if applicable), the name, and commission/employee ID number of the employee requesting the information, the purpose for the request, and the name of the supervisor. The purpose will, at a minimum, demonstrate reasonable suspicion of criminal activity or the incapacity of a person preventing identification such as death or mental impairment; and
C. All requests shall include a probe image from the investigation.

A Criminal Intelligence Group supervisor must review each request and ensure it complies with this directive. If the request is in compliance with this directive, the supervisor shall approve the facial comparison request and send the request to a member of the Criminal Intelligence Group with access to the facial comparison system.

A copy of all original probe images shall be saved without any alteration to preserve the integrity of the investigation. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made such as improving picture contrast and size.

Initial searches shall not be enhanced. Subsequent automated searches of the probe image may be enhanced using filters if needed. In some cases, enhancements may be considered for subsequent searches. Enhancements will not alter the image itself but will only improve the ability to identify distinguishing features. Enhancements include image cropping, tilting, repositioning of the face, and image exposure.

The resulting candidate images, if any, shall be physically compared with the probe image(s) and examined by an authorized examiner as defined in Section 5-119.5. Examiners shall conduct the physical comparison of images in accordance with their training, identify any candidate images which are incompatible with the probe image, and remove them from the candidate image list.

Should the initial examiner reasonably believe the probe image and candidate images are the same person, the examiner shall submit the results to another authorized examiner for peer review. Multiple peer reviews may be completed but only one is required. The Criminal Intelligence Group supervisor is permitted to be the examiner conducting the peer review if they are so trained.

After peer review, and with the approval of the Criminal Intelligence Group supervisor, the "most likely" candidate image result(s) may be released to the requesting employee as a lead only.

All search results provided to the requester other than those returning with no candidate images shall include a cover sheet with the following warning:

> The following facial comparison search results are being provided by the Oklahoma City Police Department only as an investigative lead. These results are not to be considered a positive identification of any subject. The possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources. These results shall not be the sole factor in requesting a probable cause warrant for search or arrest.

Unsolved image file searches shall also be conducted and verified according to this directive.

5-119.4 Use of Image Repositories

The Oklahoma City Police Department can utilize photo repositories from any source where the photographs were legally obtained such as:

A. Booking photographs;
B. Sex offender registry photographs;
C. Driver's license photographs in accordance with Oklahoma Department of Public Safety procedures;
D. Gang file images maintained in accordance with applicable law;
E. Other lawfully maintained governmental entity repositories;
F. Image repositories or sources made available to the general public; and
G. Image repositories legally obtained by private entities through subscription access.

5-119.5 Training

Before access to the facial comparison system is authorized, examiners will be required to participate in training regarding the authorized use of the facial comparison system. Examiners will also have training on the facial comparison program utilized by the department.

All personnel requesting access to the facial comparison system, as well as Criminal Intelligence Group supervisors, will be required to complete the following prior to receiving access or authority to approve requests:

A. Training and certification on 28 CFR Part 23;
B. Complete an approved class on intelligence gathering limitations, constitutional rights to privacy, records retention requirements, and aspects of this directive;
C. All examiners will receive training from the FBI's Facial Identification training course or other recognized equivalent facial identification training.

All police personnel will receive training on the aspects of the facial comparison program, definitions of reasonable suspicion, how to make requests, intelligence gathering limitations, constitutional rights to privacy, use of results, records retention requirements, and aspects of this directive.

Those with access to the facial comparison system shall not share their login information with any other employee, remain logged into the software while away from their computer, or utilize the software in any manner contrary to this directive in compliance with Criminal Justice Information System (CJIS) guidelines. Those with facial comparison system access are required to comply with this directive and ensure all information is protected according to this directive.

5-119.6 Administrative Procedures

Oversight

The primary responsibility for the operation of the facial comparison program, including the receiving, seeking, retention, evaluations, data quality, use, sharing, disclosure, or dissemination of information, is assigned to the Special Operations Division commander or their designee.

The Special Operations Division commander has primary oversight of the department's facial comparison program and shall:

A. Ensure the facial comparison program remains in compliance with applicable laws, regulations, and policies including Criminal Justice Information System guidelines;
B. Ensure any violations of this directive are investigated and appropriate action is taken; and
C. Ensure audits are scheduled and completed.

The Oklahoma City Police Department will contract only with commercial facial comparison companies or subcontractors that verify their methods for collecting, receiving, accessing, disseminating, retaining, and purging facial comparison information and ensure they 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.

Audits

Queries made to the facial comparison system shall be logged into the system identifying the user initiating the query. All user accesses are subject to review and audit.

The Special Operations Division commander, or their designee, shall maintain an audit log of requested, accessed, or searched facial comparison information.

The audit log will be kept for a minimum of three (3) years and will include:

A. The incident number of the investigation (if applicable);
B. The name and commission/employee ID number of the requester;
C. The name and commission/employee ID number of the approving supervisor;
D. The name of the authorized examiner and peer reviewer;
E. The date and time of system access;
F. The image repositories or file types searched;
G. The justification for access;
H. Whether any leads were generated from the program;
I. Whether the leads produced by the program were verified by the examiner;
J. If the lead was sent to the requester, was the lead verified as accurate.

The Special Operations Division commander, or their designee, shall conduct a monthly audit of the facial comparison system to ensure compliance with this directive. The audit will include:

A. Summary of how the audit was completed;
B. Findings of the audit, including any identified violations or necessary proposed revisions to this directive; and
C. Actions taken to address any violations or directive revisions.

The audit will be forwarded through the chain of command to the bureau commander.

Retention

All facial comparison search records and requests shall be retained according to Oklahoma state record retention requirements. Upon receiving the search results, the requesting employee will save the information under the incident number in the department's evidence repository.

Probe images, along with the request forms, will be maintained on a local server for inspection and tracking. The file containing the probe image and request form will also contain the result information sent to the requesting employee.

Adopted 10/25

Section 2: Specific Enforcement Actions

Police officers in a marked police vehicle, on or off duty, are required to take appropriate action when a crime is committed in their presence. This would include the completion of all departmental forms, reports and citations.

5-201 Civil Disputes

7-207.1 Police Athletic League

The Police Athletic League (PAL) puts police officers on school campuses to be effective role models for the students, as well as promote a positive and engaging relationship between students and the police department. Police officers assigned to the Police Athletic League will organize and administer PAL-sponsored sports programs for at-risk youths year-round.

The Oklahoma City Police Athletic League is a charter member of the National Police Athletic/Activities League and is a not-for-profit organization. PAL works with volunteers from the police department and the community to provide these services.

7-207.2 Family Awareness and Community Teamwork

The Family Awareness and Community Teamwork Program (FACT) uses police officers as youth outreach officers to facilitate mentoring programs for troubled and at-risk youth in the community. FACT officers organize various mentoring and leadership programs year-round through partnerships with local churches, non-profit foundations, and private businesses with the focus of lowering juvenile crime, increasing educational opportunities and building lasting relationships with youth. Youth outreach officers are supervised by a FACT Program lieutenant who is also responsible for FACT programming and facilities.

7-207.3 TRIAD

TRIAD is a collaboration between senior citizens and law enforcement with the purpose of working together to reduce criminal victimization of the elderly. The TRIAD coordinator organizes events and services where senior citizens can be educated on crime prevention, services and victim programs for the elderly. The TRIAD coordinator is a full-time professional staff position which is supervised by the PAL lieutenant.

7-208 Small Unmanned Aircraft Systems (sUAS)

The purpose of the sUAS program is to provide aerial support in field operations by collecting forensic digital data utilizing a sUAS. Use of the sUAS will be in strict accordance with constitutional and privacy rights and is governed by Federal Aviation Administration (FAA) regulations.

The Administration Bureau division major will serve as the sUAS program commander. The Police Information Technology Unit Captain will serve as the program manager.

Revised 10/25

7-208.1 Definitions

sUAS - An unmanned aircraft weighing less than 55 lbs, capable of sustaining directed flight, whether preprogrammed or remotely controlled, and includes attached systems designed for gathering information through imaging, recording, or other means.

Visual Observer (VO) – Officer trained to maintain the line-of-sight and 360-degree hazard awareness around the sUAS at all times and assist the pilot in command in carrying out all duties required for the safe operation of the sUAS.

Revised 10/25

7-208.2 Selection Process

Employees must meet selection criteria in order to operate a sUAS. Employees may apply through their chain of command to participate in the sUAS program. Division commanders should forward applications meeting the

criteria to the sUAS commander for consideration. The sUAS commander and program manager will select qualified candidates for available positions.

Employees must meet the following requirements to be a pilot in command (PIC):

1. Be a department employee;
2. Not be on any type of probationary status, unless approved by the sUAS commander;
3. Receive approval from division commander; and,
4. Successfully complete department training curriculum, to include Part 107 FAA certification.

Employees must meet the following requirements to be a visual observer (VO):

1. Be a department employee; and
2. Not be on any type of probationary status, unless approved by the sUAS commander.

In order to be considered for a PIC position, there must be an opening in the employee's designated work area for the desired position. The Major at each division and/or applicable bureau will be responsible for ensuring the equitable distribution of PICs.

Revised 10/25

7-208.3 Deployment

Only authorized operators who have completed the required department training and have successfully obtained the Part 107 certification shall be permitted to deploy the sUAS. Only department-approved sUAS and equipment shall be used to conduct deployments. Use of personal sUAS and equipment is prohibited. No employee shall use a sUAS without having received proper departmental training. All deployments utilizing the sUAS must fall within the specific utilization parameters.

Use of the sUAS to conduct a search of an area in which a person has a reasonable expectation of privacy must at all times comply with the 4th Amendment's reasonableness requirement. Absent exigent circumstances or the consent of the property owner, a warrant shall be obtained by the respective investigative unit prior to deployment of the sUAS in an area in which a person has a reasonable expectation of privacy.

The PIC shall be the final authority for determining when the sUAS may be safely utilized or if a deployment must be terminated based on weather, airworthiness, darkness or other hazardous conditions.

The sUAS equipment shall only be operated by qualified employees who can ensure a safe and secure deployment. Reasons for which an employee may be removed from the program include, but are not limited to:

1. Demonstrating an inability to safely or effectively operate the equipment;
2. Poor deployment decisions; or
3. Engaging in unprofessional conduct when using the department's sUAS or equipment.

The program manager and sUAS commander may remove an employee from the program for cause.

Responsibilities and Duties of the Visual Observer (VO)

VOs are responsible for identifying any unsafe conditions at the scene and during deployment. This includes, but is not limited to:

A. During the pre-flight check, the VO will identify:
   1. Any unsafe conditions at the scene to include debris in the takeoff/landing area;
   2. Any trees, bushes, power lines, cell towers or other potential obstructions prior to flight.

B. When an sUAS is deployed, the PIC or VO will notify 911 Communications with the unit number of the sUAS and the unit number of the PIC.
   1. If time permits, the PIC or VO will notify Air Support by phone or radio that an sUAS is being deployed, giving the general location of deployment.
   2. If time does not permit, the PIC or VO will ask 911 Communications to notify Air Support.
   3. When Air One is in flight and requested by another division, sUAS location, division and unit number will be relayed to Air Support.

C. The VO will be positioned in appropriate locations during all sUAS flight operations.
   1. Binoculars, night vision devices, etc., may not be used as the primary means for visual observation duties. Such devices are permitted only for augmentation of the observer's visual capability. Visual observers must use caution to ensure the aircraft remains within normal visual line-of-sight. Vision assisted devices are aids to vision and should not be confused with corrective lenses or contact lenses, which do not alter the field of view or distort vision.

D. All sUAS operations shall be conducted within visual line-of-sight of the PIC or VO to detect and avoid hazards such as aircraft and property unless waived by the FAA.

E. Take-off and landing site: This area should be free of obstructions, items on the ground, and debris that may interfere with the rotors. This includes creation of a flight line, from which other law enforcement officers and civilians must remain clear.

F. Security perimeter: The site must be safeguarded to minimize civilian interference during the operation.

G. Flight area: The PIC and VO should identify potential obstructions and coordinate the pre-flight briefing accordingly.

H. Interference: The PIC and VO should identify sources, which might create interference with the flight equipment. The equipment should be tested on the ground to ensure proper communications and operation before the flight.

I. The PIC and VO shall utilize the current sUAS flight checklist.

J. Serve as sUAS observer when designated.

K. Assist PIC with flight checklists.

L. After the PIC inspects/installs flight battery, verify sUAS batteries are charged and installed properly according to the sUAS checklist.

M. Observe flight area and report to PIC anything that could affect the sUAS flight.

N. Monitor sUAS flight time, and report regularly to the PIC.

Revised 10/25

7-208.4 Incident / Collision Reporting

In all instances where an sUAS was deployed, an incident report will be completed. The officer shall document the use of an sUAS in the first line of the narrative of the report or immediately thereafter.

Revised 10/25

Section 3: Canine Procedures

The department will utilize canine units as a supportive tool to assist with crime deterrence and offender apprehension, and to increase officer safety.

7-301 Police Canine

A canine unit should be assigned to any operational need suited to the unique capabilities of the police canine. Attempts must be made to minimize any and all obstacles the canine encounters. For instance, a scene should not be contaminated prior to calling for a canine. The canine should be used first, followed by human resources. Poor environmental conditions, and the health of the canine, can affect the canine's daily performance.

Types of calls on which a police canine may be assigned include but are not limited to: