Unmanned Aerial System

613.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of an unmanned aerial system (UAS) and for the storage, retrieval, and dissemination of images and data captured by the UAS.

613.1.1 DEFINITIONS

Definitions related to this policy include:

Unmanned aerial system (UAS) - An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached systems designed for gathering information through imaging, recording, or any other means.

613.2 POLICY

A UAS may be utilized to enhance the office's mission of protecting lives and property when other means and resources are not available or are less effective. Any use of a UAS will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations.

613.3 PRIVACY

The use of the UAS potentially involves privacy considerations. Absent a warrant or exigent circumstances, operators and observers shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure). Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy. Reasonable precautions can include, for example, deactivating or turning imaging devices away from such areas or persons during UAS operations.

613.4 PROGRAM COORDINATOR

The Sheriff will appoint a program coordinator who will be responsible for the management of the UAS program. The program coordinator will ensure that policies and procedures conform to current laws, regulations, and best practices and will have the following additional responsibilities:

- Coordinating the FAA Certificate of Waiver or Authorization (COA) application process and ensuring that the COA is current, and/or coordinating compliance with FAA Part 107 Remote Pilot Certificate, as appropriate for office operations.
- Ensuring that all authorized operators and required observers have completed all required FAA and office-approved training in the operation, applicable laws, policies, and procedures regarding use of the UAS.
- Developing uniform protocols for submission and evaluation of requests to deploy a UAS, including urgent requests made during ongoing or emerging incidents.

Deployment of a UAS shall require authorization of the Sheriff or the authorized designee, depending on the type of mission.

- Coordinating the completion of the FAA Emergency Operation Request Form in emergency situations, as applicable (e.g., natural disasters, search and rescue, emergency situations to safeguard human life).
- Developing protocols for conducting criminal investigations involving a UAS, including documentation of time spent monitoring a subject.
- Implementing a system for public notification of UAS deployment.
- Developing operational protocols governing the deployment and operation of a UAS including but not limited to safety oversight, use of visual observers, establishment of lost link procedures, and secure communication with air traffic control facilities.
- Developing a protocol for fully documenting all missions.
- Developing a UAS inspection, maintenance, and record-keeping protocol to ensure continuing airworthiness of a UAS, up to and including its overhaul or life limits.
- Developing protocols to ensure that all data intended to be used as evidence are accessed, maintained, stored, and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, authenticity certificates, and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.
- Developing protocols that ensure retention and purge periods are maintained in accordance with established records retention schedules.
- Facilitating law enforcement access to images and data captured by the UAS.
- Recommending program enhancements, especially regarding safety and information security.
- Ensuring that established protocols are followed by monitoring and providing periodic reports on the program to the Sheriff.
- Maintaining familiarity with FAA regulatory standards, state laws and regulations, and local ordinances regarding the operations of a UAS.
- Developing procedures for the use of facial recognition software to evaluate information gathered by a UAS, as permitted by 725 ILCS 167/17.
- Ensuring that the office's current UAS policy is posted on the office's website (725 ILCS 167/35).

613.5 USE OF UAS

Only authorized operators who have completed the required training shall be permitted to operate the UAS.

Use of vision enhancement technology (e.g., thermal and other imaging equipment not generally available to the public) is permissible in viewing areas only where there is no protectable privacy

interest or when in compliance with a search warrant or court order. In all other instances, legal counsel should be consulted.

UAS operations should only be conducted consistent with FAA regulations.

The Office may not use the UAS to gather information except (725 ILCS 167/15):

(a) To counter a high risk of a terrorist attack by a specific individual or organization if the United States Secretary of Homeland Security determines that credible intelligence indicates there is a risk.

(b) Pursuant to a search warrant based on probable cause. The warrant must be limited to a period of 45 days, renewable by a judge upon showing good cause for subsequent periods of 45 days.

(c) Upon reasonable suspicion that under particular circumstances, swift action is needed to prevent imminent harm to life, forestall the imminent escape of a suspect, or prevent the destruction of evidence. The use of a UAS under this paragraph is limited to a period of 48 hours. Within 24 hours of UAS initiation under this paragraph, the Sheriff must report its use, in writing, to the State's Attorney.

(d) To locate a missing person, engage in search and rescue operations, or aid a person who cannot otherwise be safely reached while not also undertaking a criminal investigation.

(e) To obtain crime scene and traffic crash scene photography in a geographically confined and time-limited manner. The use of the UAS under this paragraph on private property requires either a search warrant or lawful consent to search.

(f) To obtain information necessary for the determination of whether a disaster or public health emergency should be declared, to manage a disaster by monitoring weather or emergency conditions, to survey damage, or to coordinate response and recovery efforts.

(g) To conduct an inspection of the infrastructure of a designated building or structure when requested by a local government agency.

(h) To locate victims, assist with victims' immediate health or safety needs, or coordinate the response of emergency vehicles and personnel, when dispatched to an emergency.

(i) In advance of or during a routed event or special event, as defined in 725 ILCS 167/5, for those uses allowed under 725 ILCS 167/15.

    1. The notice for UAS use in these instances should be posted at a time, place, and manner as required by 725 ILCS 167/15.

613.5.1 PRIVATE UAS OWNERS

This policy and its restrictions apply to the department's directed use of a UAS owned by a private third party and information gathered by a UAS voluntarily submitted to the Office by a private third party (725 ILCS 167/40).

613.5.2 FACIAL RECOGNITION WITH UAS

Facial recognition software onboard a UAS shall not be used during a flight (725 ILCS 167/17). Use of facial recognition software to evaluate information gathered by a UAS is permissible only under those circumstances described in 725 ILCS 167/17.

613.6 PROHIBITED USE

The UAS video surveillance equipment shall not be used:

- To conduct random surveillance activities.
- To target a person based solely on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.
- To harass, intimidate, or discriminate against any individual or group.
- To conduct personal business of any type.

The UAS shall not be weaponized (725 ILCS 167/18).

613.7 RETENTION OF UAS INFORMATION

The Records Section supervisor shall destroy all information gathered by the UAS within the timeframe specified by law (725 ILCS 167/20).

Information may be retained by a office supervisor when (725 ILCS 167/20):

(a) There is reasonable suspicion that the information contains evidence of criminal activity.

(b) The information is relevant to an ongoing investigation or pending criminal trial.

(c) The information will be used exclusively for training purposes and all personally identifiable information has been removed from it.

(d) The information contains only flight path data, metadata, or telemetry information of the UAS.

613.8 REPORTING

The Records Section supervisor shall report annually, by April 1, to the Illinois Criminal Justice Information Authority the number of UASs owned by the Office and any other required information to be reported under 725 ILCS 167/35.

The report shall contain a copy of the office's current UAS policy (725 ILCS 167/35).

613.9 COMPLIANCE WITH THE FREEDOM FROM DRONE SURVEILLANCE ACT

If a determination is made that a member has violated the Act, the Office shall take prompt and appropriate action (e.g., training, discipline) (725 ILCS 167/45). If a determination is made that a UAS pilot has willfully violated the Act, the Office shall promptly remove the pilot from its UAS program and take other appropriate action (see the Personnel Complaints Policy) (725 ILCS 167/45).

613.10 DISCLOSURE OF UAS INFORMATION

Information gathered during an inspection of the infrastructure of a designated building or structure shall be given, as soon as practicable, to the requesting local government agency before it is destroyed (725 ILCS 167/20).

The disclosure of information gathered by the UAS is prohibited except (725 ILCS 167/25):

(a) To another government agency when there is reasonable suspicion that the information contains evidence of criminal activity or the information is relevant to an ongoing investigation or pending criminal trial.

(b) Pursuant to a court order or subpoena in connection with a criminal proceeding.

(c) In regard to a completed traffic crash investigation.

Available records of drone usage (e.g., flight path data, metadata, telemetry information of specific flights) may be disclosed subject to the Freedom of Information Act, 5 ILCS 140/1 et seq., and rules adopted under it (725 ILCS 167/25).

FACIAL RECOGNITION POLICY

614.1 PURPOSE

The purpose of this policy is to establish procedures for the acceptable use of the images (probe and candidate), information and tools within the facial recognition system. Facial Recognition shall only be used when there is reasonable suspicion that such use will provide information relevant to an active investigation, imminent threat to health or safety ("at-risk"), or to help in the identification of deceased persons, persons unable to identify themselves, or persons unwilling to identify themselves. This policy applies to all law enforcement personnel who are granted direct access to the face recognition system as well as personnel who are permitted to request face recognition searches. Any outside agency, or personnel from an outside agency, requesting face recognition assistance with an investigation must also adhere to this policy.

614.2 DEFINITIONS & TERMS AS IDENTIFIED BY LACRIS

Digital Mugshot System (DMS) – DMS is the repository of all criminal booking photos (mugshots) and includes a Facial Recognition application.

Facial Recognition (FR) – The automated searching of a facial image (probe) against a known database(s) resulting in a list of candidates ranked by computer-evaluated similarity score. This is commonly referred to as a one-to-many comparison.

Facial Recognition (Mobile FR) - is the process of conducting an automated FR search in a mobile environment.

Personally identifiable Information (PII) - is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

User - is an individual who is authorized to access the facial recognition application and is approved by the Agency to utilize the facial recognition application.

614.3 POLICY

This policy of the Madison County Sheriff's Office is to solely utilize face recognition technology as an investigative tool during investigations, while recognizing the established privacy rights of the public. Potential matches returned by the facial recognition system are to be considered investigative leads only and should not be the sole basis for an arrest or identification.

614.4 USE OF FACIAL RECOGNITION SOFTWARE

The Madison County Sheriff's Office will only use FR software for the following reasons:

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

(b) An active or ongoing criminal or homeland security investigation.

(c) To assist in the identification of a person who lacks capacity or is otherwise unable to identify him or herself (such as an incapacitated, deceased, or otherwise at-risk person).

(d) To assist in the identification of a person who is unwilling to identify themselves.

(e) To investigate and/or corroborate tips and leads.

(f) To assist in the identification of potential witnesses and/or victims of violent crime.

614.5 USE OF MOBILE FACIAL RECOGNITION

Any use of Mobile FR by the Madison County Sheriff's Office shall be in accordance with the FBI CJIS Cybersecurity Policy and Illinois State Law. Mobile FR shall only be used during the course of a User's lawful duties and one of the following circumstances exists:

Mobile FR may be used with the consent of an individual. The individual may withdraw consent at any time. If consent is withdrawn, and the use of FR is solely based upon consent, use of Mobile FR is not authorized, and its' use must stop immediately.

Mobile FR may be used without consent of an individual if one of the following circumstances exists:

(a) The User has probable cause to believe the individual has committed a crime for which the collection of biometric data is allowable under applicable state law in the State of Illinois.

(b) The individual is unable to provide reliable identification due to physical incapacitation or defect, mental incapacitation or defect, or death, and immediate identification is needed to assist the User in performance of his or her lawful duties.

(c) Pursuant to a valid court order.

614.6 PROHIBITED SEARCHES

In accordance with Illinois State Law, users shall not use drone based onboard Facial Recognition software during flight, unless there is a high risk of a terrorist attack, or swift action is needed to prevent imminent harm to life, or to forestall the imminent escape of a suspect, or the destruction of evidence.

614.7 AUDITING

All FR use is subject to audit. In the event of an audit, the User will be required to provide appropriate justification for the use of FR. Appropriate justification may include a case/complaint number and file class/ crime type, if available, or a situation description and purpose for the search. For searches conducted on behalf of another individual, the name and rank/job title of other individual requesting the search shall also be included.