

Unmanned Aerial System

5-106.01 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.

DEFINITIONS

Definitions related to this policy include:

Information - any evidence, images, sounds, data, or other information gathered by a drone.

Parade - a march, procession, or other similar activity consisting of persons, animals, vehicles, or things, or any combination thereof, upon a public street, sidewalk, alley, or other public place, which requires a street closing or otherwise requires stopping or rerouting vehicular traffic because the parade will not or cannot comply with normal and usual traffic regulations or controls. "Parade" does not include a political protest, march, demonstration, or other assembly protected by the First Amendment.

Routed Event - a parade, walk, or race that:

- a) is hosted by the State of Illinois or a county, municipality, township, or park district;
- b) is outdoors and open to the public; and
- c) has an estimated attendance of more than 50 people.

Special Event - a concert or food festival that:

- a) is hosted by the State of Illinois or a county, municipality, township, or park district;
- b) is outdoors and open to the public; and
- c) has an estimated attendance of:
 - 1. 150 or more people in a unit of local government with a population that is less than 50,000;
 - 2. 250 or more people in a unit of local government with a population that is greater than or equal to 50,000 but less than 100,000;
 - 3. 350 or more people in a unit of local government with a population that is greater than or equal to 100,000 but less than 500,000; or
 - 4. 500 or more people in a unit of local government with a population that is 500,000 or more.

"Routed event" and "Special event" does not include any political protest, march, demonstration, or other assembly protected by the First Amendment.

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 a drone), and all of the supporting or attached systems designed for gathering information through imaging, recording, or any other means.

5-106.02 POLICY

A UAS may be utilized to enhance the Department'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.

5-106.03 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.

5-106.04 PROGRAM COORDINATOR

The Chief of Police 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 compliance with FAA Part 107 Remote Pilot Certificate, as appropriate for Department operations.
- Ensuring that all authorized operators and required observers have completed all required FAA and Department-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 Chief of Police 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 Chief of Police.
- 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 Department's current UAS policy is posted on the Department's website (725 ILCS 167/35).

5-106.05 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 Department 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 Chief of Police 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 demonstrate the capabilities and functionality of a police drone for public relations purposes, provided that no information is collected or recorded by the drone during such demonstration.
- i) 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.

- j) In advance of or during a routed event or special event, as long as:
1. notice is posted at the event location for at least 24 hours before the event and clearly communicates that drones may be used at the upcoming event for the purpose of real-time monitoring of participant safety;
 2. notice is posted, if practical, at major entry points to the event clearly informing the attendees that a drone may be used for the purpose of real-time monitoring of participant safety; and
 3. the drone is flown in accordance with Federal Aviation Administration safety regulations.

Under this section (j) a UAS may be used

1. In advance of an event, before event participants have begun to assemble, for the sole purpose of creating maps and determining appropriate access routes, staging areas, and traffic routes, provided that no personal identifying information is recorded and provided further that not recorded information is used in any criminal prosecutions.
2. during the event to proactively support public safety personnel by monitoring the event footprint in real time:
 - i. to detect a breach of event space, including a breach by an unauthorized vehicle, an interruption of a parade route, or a breach of an event barricade or fencing;
 - ii. to evaluate crowd size and density;
 - iii. to identify activity that could present a public safety issue for the crowd as a whole, including crowd movement;
 - iv. to assist in the response of public safety personnel to a real-time public safety incident at the event; and
 - v. to assess the traffic and pedestrian flow around the event in real time.

5-106.06 PRIVATE UAS OWNERS

Except as provided in Section 5-106.05 above, the Belvidere Police Department may not acquire information from or direct the acquisition of information through the use of a drone owned by a private third party. In the event that law enforcement acquires

information from or directs the acquisition of information through the use of a privately owned drone under Section 5-106.05 above, any information so acquired is subject to the information retention and information disclosure restrictions listed in Sections 725 ILCS 167/20 & 25.

Nothing prohibits private third parties from voluntarily submitting information acquired by a privately owned drone to law enforcement. In the event that law enforcement acquires information from the voluntary submission of that information, whether under a request or on a private drone owner's initiative, the information is subject to the information retention and information disclosure restrictions listed in Sections 725 ILCS 167/20 & 25.

5-106.07 AUDIO RECORDING OR MONITORING

The use of any device to record or listen to a conversation is permissible only under those circumstances described in 720 ILCS 5/14-3 and 725 ILCS 5/108A-1 & 108A-6.

- a) with prior notification to the State's Attorney the use of any device to record or listen to any conversation where a law enforcement officer or any other person has consented when necessary to protect the officer or other party during the investigation of enumerated offenses (720 ILCS 5/14-3(g))
- b) the use of a device during an ongoing hostage or barricade is allowable when necessary to protect the safety of the general public, hostages, or law enforcement
- c) with approval of the State's Attorney the use of a device to record or monitor a conversation where a law enforcement officer has consented during the investigation of any felony under Illinois law

5-106.08 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:

- a) the law enforcement agency is using a drone to counter a high risk of a terrorist attack by a specific individual or organization and the United States Secretary of Homeland Security has determined that credible intelligence indicates that there is such a risk; or
- b) the law enforcement agency possesses reasonable suspicion that, under particular circumstances, swift action is needed to prevent imminent harm to life or to forestall the imminent escape of a suspect or the destruction of evidence.

5-106.09 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).

5-106.10 RETENTION OF UAS INFORMATION

The Department shall destroy all information gathered by the UAS within the timeframe specified by law (725 ILCS 167/20):

- a) All information gathered pursuant to paragraphs (a), (b), (c), (d), (e), (f), or (i) of Section 5-106.05 above shall be destroyed within 30 days after being gathered.
- b) All information gathered pursuant to paragraph (j) of Section 5-106.05 above shall be destroyed within 24 hours after being gathered.
 1. All information gathered pursuant to paragraph (g) of Section 5-106.05 above shall be turned over to the requesting local government agency as soon as practicable, and all gathered information shall be destroyed immediately after the information has been turned over.

A Department supervisor may retain Information 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.

5-106.11 REPORTING

The Chief of Police or Department designee shall report annually, by April 1, to the Illinois Criminal Justice Information Authority the number of UASs owned by the Department and any other required information to be reported under 725 ILCS 167/35.

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

The deployment of a drone does not necessarily require a written case report, unless the call for service requires one; however, for every deployment, the pilot must complete a Drone Deployment Report Form as soon as practicable, but no later than the ending of the pilot's tour of duty.

5-106.12 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).

5-106.13 COMPLIANCE WITH THE FREEDOM FROM DRONE SURVEILLANCE ACT

If a determination is made that a member has violated the Act, the Department 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 Department shall promptly remove the pilot from its UAS program and take other appropriate action (725 ILCS 167/45).



BELVIDERE
POLICE

DRONE DEPLOYMENT REPORT

Pilot:

Case#:

Date of report:

Date of Use:

Time of Use:

Duration of Use:

Reason for Use:

Summary of Flight:

Pilot's signature: _____

Supervisor's signature: _____

Does the reviewing supervisor recommend drone videos/photos be retained Yes _____ No _____

If yes, reason:

Shane Woody, Chief of Police

Approval Date