

EMERALD ISLE POLICE DEPARTMENT UAS PROPOSAL



DJI MATRICE 4T

Rapid Deployment • Search & Rescue • Scene Documentation • Major-event Overwatch

Prepared by Sgt. Michael Lewis

Why EIPD Needs an Unmanned Aircraft System

A rapidly deployable aerial perspective improves safety, response, documentation, and situational awareness.

OFFICER SAFETY

Observe hazardous, inaccessible, or uncertain areas before committing personnel.

FASTER RESPONSE / SEARCHES

Cover beaches, the Intracoastal Waterway (ICW), Bogue Sound, neighborhoods, wooded areas, and other large search areas efficiently.

SITUATIONAL AWARENESS

Give supervisors a real-time overhead view during developing incidents and major events.

BETTER DOCUMENTATION

Capture repeatable aerial imagery for serious crashes, crime scenes, and post-event review.

A UAS would be a department-wide tool supporting patrol, investigations, supervision, emergency response, and mutual aid.

DJI Matrice 4t: The Right Fit for EIPD

Enterprise public-safety capability in a compact platform that can live in a patrol vehicle.

≈ 2 MIN

realistic case-to-sky deployment

2.7 LB

takeoff weight

UP TO 49 MIN

no-wind flight time

640 × 512

thermal sensor

MULTI-SENSOR PAYLOAD

- 48 MP wide-angle camera
- 48 MP medium telephoto camera
- Thermal imaging
- Laser rangefinder up to 1,800 m*
- Near-infrared auxiliary light

COMPACT • PATROL-READY • MULTI-MISSION



Highest-Value Uses for EIPD

Three mission sets would provide immediate operational value.

SEARCH & RESCUE

- Missing or endangered persons
- Beach / shoreline / ICW / Sound searches
- Wooded or low-visibility areas
- Nighttime thermal searches
- Water-rescue reconnaissance
- Expandable SAR capabilities
 - Payload/drop systems
 - High-intensity spotlights
 - Loudspeakers / PA systems

SCENE MAPPING & DOCUMENTATION

- Serious traffic crashes
- Large outdoor crime scenes
- Evidence / vehicle positioning
- 2D / 3D model data collection

MAJOR-EVENT OVERWATCH

- Large public events
- Developing critical incidents
- Crowd / traffic awareness
- Command-level resource deployment

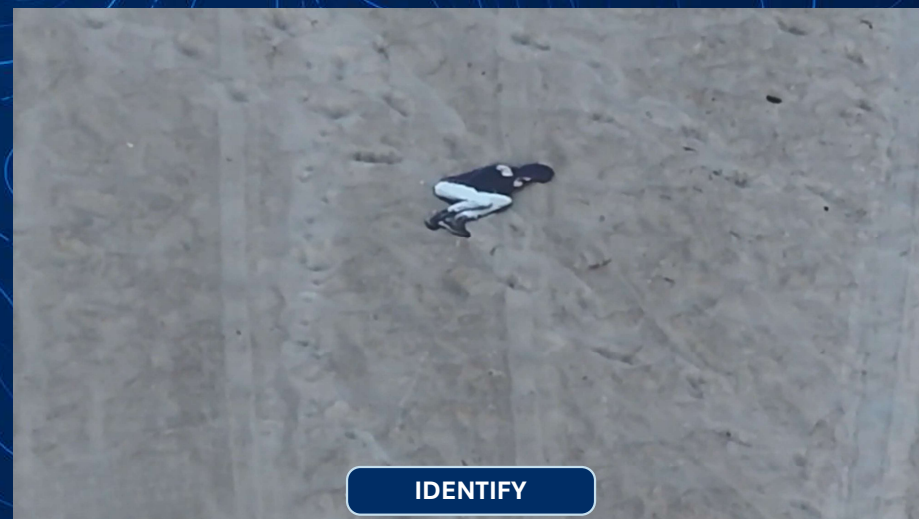
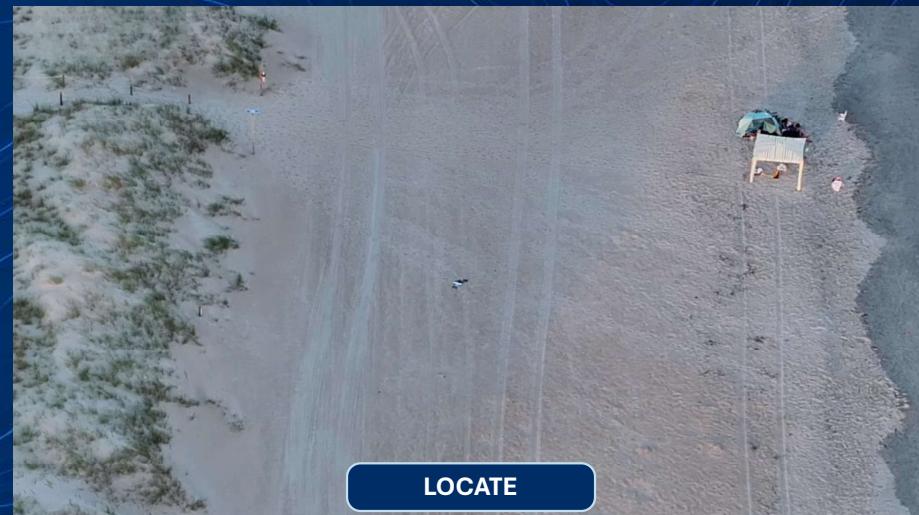
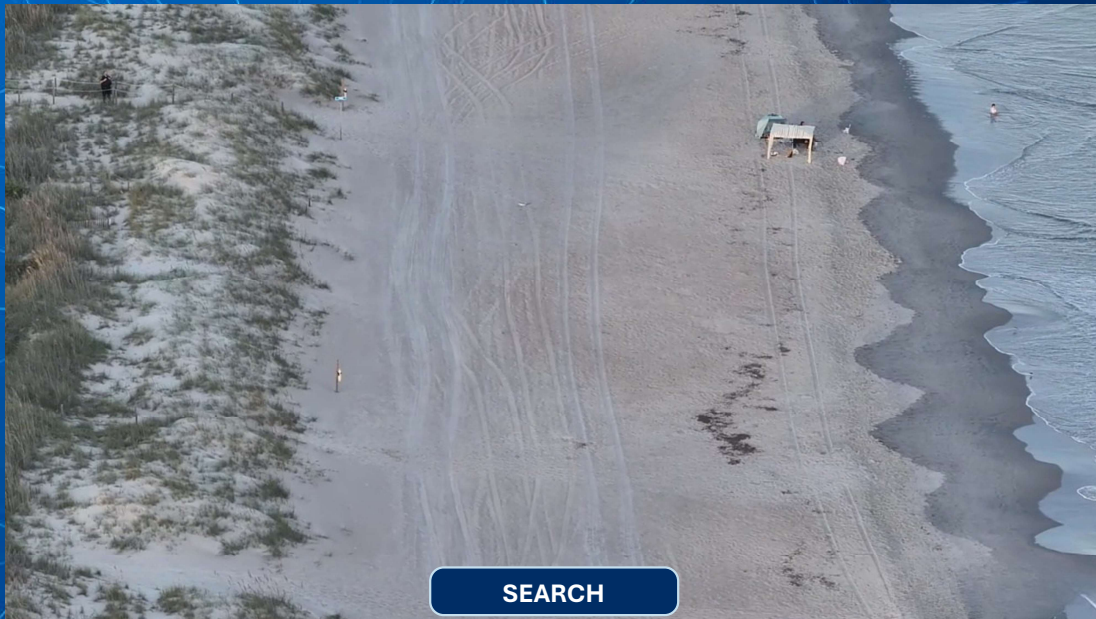
EXPANDABLE PLATFORM

Additional third-party accessories can expand the aircraft's SAR capabilities: payload-release systems, spotlights, and loudspeakers for communicating instructions to missing or distressed persons.

The same platform can also support storm damage assessment and mutual aid to another agency if needed.

From Aerial Search to Identification

Actual imagery captured during the EIPD Matrice 4T demonstration.



ONE AIRCRAFT • WIDE-AREA SEARCH • DETAILED IDENTIFICATION

Accountability & Responsible Use

Every EIPS UAS deployment will operate under established legal, training, documentation, and supervisory safeguards.

TRAINED & QUALIFIED

- Part 107 Certified
- 60-day flight
- Quarterly training
- Annual evaluation



AUTHORIZED & LAWFUL

- Authorized purpose
- FAA / NC Law
- EIPD policy
- Constitutional & privacy protections



DOCUMENTED

- CFS every deployment
- OCA when applicable
- Flight records
- Evidence procedures



Oversight

- Supervisor oversight
- UAS Coordinator
- Annual program review
- RPIC final authority



GREATER CAPABILITY WITH TRAINING, OVERSIGHT, DOCUMENTATION, AND ACCOUNTABILITY BUILT INTO EVERY DEPLOYMENT.

Mapping, Flight History, & Accountability

The UAS provides more than live video. It can create location-based data and a documented record of each deployment.

MAPPING & DOCUMENTATION

- Create detailed overhead maps
- Build 2D and 3D views of scenes
- Document crashes and crime scenes
- Measure distances and locations
- Document storm and property damage

GIS-compatible data can also be used with the Town's existing mapping systems.

FLIGHT PATH HISTORY

- Records where and when the drone flew
- Records flight path, altitude, time, and location
- Flight data can be downloaded and retained
- Maintained as a central Departmental record
- Supports after-action review and accountability

DOCUMENTED DEPLOYMENT

- Each deployment will be assigned a CFS
- Multiple flights may be documented under the same CFS
- An OCA will be attached when applicable
- Photos and video with evidentiary value will be preserved in accordance with Department evidence procedures
- Flight records identify the RPIC and mission

LPR PROPOSAL: FLOCK CAMERAS vs. VERKADA LPR's

CORE ARCHITECTURE AND PURPOSE

• FLOCK

- Purpose-built to connect local users to a massive, searchable multi-agency network shared with thousands of law enforcement entities.
- Captured data feeds into a collaborative nationwide hotlist and search ecosystem.

• VERKADA

- Keeps data localized within the deploying organization rather than sharing with a national database.
- License plate and video data remain confined to the specific organization's private command dashboard, giving local administrators tighter control over storage and access boundaries.

KEY TECHNICAL & FUNCTIONAL DIFFERENCES

• FLOCK

- Flock's primary value proposition is its "Talons" network, which automatically shares captured vehicle data with thousands of law enforcement agencies nationwide that are on the network. This is what allows the controversial vehicle tracking over a period of time and space.

• VERKADA

- Verkada operates on a closed siloed architecture where the captured vehicle data is totally isolated. Captured data belongs strictly to the organization that purchased the system. There is no central, interconnected national database, and out-of-jurisdiction police departments cannot log in or search a global Verkada pool to track someone. Data can only be shared if a local administrator manually exports a specific clip after an incident occurs and ONLY for a legitimate law enforcement purpose.

LPR PROPOSAL

LPR technology is an investigative tool, not a stand-alone basis for enforcement.

INVESTIGATIVE TOOL • AUTHORIZED PURPOSES • VERIFIED ALERTS

AUTHORIZED USES

- Used only for authorized law enforcement purposes under NC law.
- LPR data **shall not** be used for enforcement of traffic violations.
- Audits conducted annually

INVESTIGATIVE VALUE

- May assist with stolen vehicles, felony warrants, missing/endangered persons, and criminal investigations.
- LPR information supports investigations—it is not, by itself, enforcement authority.

VERIFY & DOCUMENT

- Officers must verify any LPR alert before taking enforcement action.
- Historical searches require a legitimate purpose and documentation.

DATA & OVERSIGHT

- Captured data is confidential and subject to strict retention limits in accordance with State law.
- Access, searches, sharing, and preservation are subject to audit and supervisory oversight.

MISUSE WILL RESULT IN DISCIPLINARY ACTION AND POSSIBLE CRIMINAL LIABILITY.

SAFEGUARDS

SIX CONTROLS IN PLACE TO PREVENT MISUSE. FIVE ARE BUILT INTO THE SOFTWARE

WRITTEN POLICY

- Adopted policy defines permitted uses, prohibited queries and disciplinary consequences.

CASE NUMBER AND OFFENSE REQUIRED

- Software requires case number and offense type before any query can be run.
- Every search is logged.

ROLE BASED PERMISSIONS & CJIS

- Custom roles/permissions limit search capabilities
- CJIS Viewer required for NCIC alerts

SUPERVISOR AND RANDOM AUDITS

- Supervisors review flagged searches the same business day.
- Audits filter the log by event type.

ALERT RECIPIENTS SCOPED TIGHTLY

- Alerts scoped to certain cameras/sites.
- Alerts scoped to specific users/groups

RETENTION AND TRAINING

- Retention is set by State Law and Department Policy.
- Annual training on authorized uses and bias awareness descriptors.

SURVEILLANCE TECHNOLOGY POLICY & OVERSIGHT

DEPARTMENT POLICY IS BASED ON FOUR CORE PRINCIPLES

**LEGITIMATE
NEED**

**LEGAL
AUTHORITY**

ACCOUNTABILITY

**PRIVACY
PROTECTION**

GOALS

1. To ensure that the technology remains a focused public safety tool that does not allow for unrestricted monitoring.
2. To provide officers with modern tools that can improve public safety while placing clear boundaries around how those tools may be use.
3. To respond more effectively to emergencies while maintaining appropriate safeguards to protect individual constitutional rights and public trust.

Emerald Isle Police Department Policy and Procedures Manual

Chapter 35

Automated License Plate Readers

Original Effective Date:

09/01/2026

Date Revised:

Date Reissued:

By Order of:

Jeffrey D. Waters, Chief of Police

35.01 PURPOSE

To provide guidance for the capture, storage, and use of digital data obtained by Automated License Reader (ALPR) technology in accordance with (N.C.G.S. §20-183.31).

35.02 POLICY

To provide guidelines for the implementation, training, responsibilities, and use of fixed ALPR technology and equipment to scan, detect, and identify vehicles and/or license plate numbers. The ALPR technology shall be restricted to legitimate law enforcement uses for the purpose of furthering law enforcement goals and enhancing public safety.

35.03 PROCEDURE

ALPR ADMINISTRATOR

The Assistant Chief of Police is responsible and will act as the ALPR Administrator. The Administrator will have administrative oversight into the ALPR system deployment and operation.

35.04 OPERATIONS

Use of ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Prior to initiation of a stop based on an ALPR Alert or Hit, the user must: Verify through NC DCIN (N.C.G.S. § 20-183.31).

Use of ALPR during special or covert operations or during highly sensitive criminal investigations must be approved, in writing, by the ALPR Administrator.

35.05 SUPERVISOR RESPONSIBILITIES

Supervisors should appropriately monitor ALPR operators to ensure that use of the ALPR equipment and data is consistent with policy. Any use of the ALPR system that violates the restrictions contained in the policy may/will result in disciplinary action.

35.06 DATA SHARING AND DISSEMINATION

- A. The ALPR systems and associated equipment and databases are authorized for public safety purposes. Use of this equipment, associated databases, or data in a manner outside the scope of this policy may subject the employee to disciplinary action.
- B. ALPR data is not a public record and shall not be disclosed except as provided in N.C.G.S. §20-183.32(e).

35.07 DATA COLLECTION, RETENTION AND PROCEDURES

- A. The ALPR Administrator is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. The ALPR Administrator shall keep a Data Retention Request Log and File and all requests for ALPR data must be logged.
- B. ALPR data shall be purged after 90 days unless one of the following methods of preservation occurs:
 - (a) A federal or state search warrant has been issued for the data; or
 - (b) A preservation request is made under N.C.G.S. §20-183.32 as detailed in (4) of this policy.

35.08 DATA SECURITY AND ACCESS

- A. All ALPR data shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
- B. Periodic ALPR system audits (1x month) are required and will be managed through the ALPR System Administrator and/or System Administrator.

35.09 SYSTEM INTEGRITY

- A. The ALPR system should be updated every 24 hours, or as soon as practical, with any license plate data obtained from the DCI Network or any other databases used in conjunction with the ALPR system.
- B. The ALPR Administrator, or designated System Administrator, shall maintain a schedule and record thereof to regularly perform audits, maintenance checks, calibration and any needed corrections or adjustments to the ALPR system. The audits shall be conducted at least annually and include a report to the Chief of Police of the use and effectiveness of the system. The audit shall also include a report of all data existing on the device for more than 90 days together with a comparison of the Data Retention Request Log to determine if any data has existed on the device for longer than 90 days without being supported by the required retention documentation.

Emerald Isle Police Department Policy and Procedures Manual

Chapter 36

Unmanned Aerial Systems

Original Effective Date: 09/01/2026

Date Revised:

Date Reissued:

By Order of: Jeffrey D. Waters, Chief of Police

36.01 PURPOSE

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.

36.02 DEFINITIONS

Unmanned aerial system (UAS) - An unmanned aircraft of any type that is capable of sustaining directed flight, whether pre-programmed 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.

36.03 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, within the purview of the National Airspace, will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations. All operators and pilots of the UAS systems will be FAA certificated Part 107 - Small Remote Pilots.

36.04 PRIVACY

The use of the UAS potentially involves privacy considerations. Absent a warrant or exigent circumstances, operators and observers shall adhere to Federal Aviation Administration (FAA) altitude regulations and 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 people during UAS operations.

36.05 PROGRAM OVERSIGHT

A. The Chief of Police will appoint a Program Commander who will be responsible for the overall management of the UAS program. The Program Commander will ensure that policies and procedures conform to current laws, regulations, and best practices. Additionally, the Chief of Police will appoint a Chief Pilot / Program Coordinator, that will report to the commander, that will assist the Commander in training, guiding and program operations.

36.06 USE OF UAS

Only authorized operators who have completed the required training shall be permitted to operate the UAS. All operators must be approved by the Chief Pilot prior to operating. Operations will be conducted under FAA Part 107 or FAA Part 91 rules and regulations at all times while in the National Airspace.

36.07 RETENTION OF UAS DATA

Data collected by the UAS shall be retained as provided in the established records retention schedule.

36.08 PROHIBITED USE

The UAS video surveillance equipment shall not be used:

- A. To conduct random surveillance activities.
- B. 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.
- C. To harass, intimidate, or discriminate against any individual or group.
- D. To conduct personal business of any type.

Violation of this policy will constitute disciplinary actions up to and including termination.