Atlanta Police Department – Standard Operating Procedure			
	APD.SOP.4045 – Unmanned Aircraft Systems (Drones) **Effective Date: August 11th, 2026**		
Chief Darin Schierbaum	**Signature by: DS**	**Date Signed:8/11/2026**	**Expires: 2027**

SIGNIFICANT CHANGES

APD Staff,

The Policy and Standards Section is dedicated to providing the department, and its employees, with accurate, understandable and transparent policies. In order to publish policies that reflect the most up-to-date standards, the Policy and Standard Section regularly reviews all policies to ensure that they are reflective of the current mission and objectives of the Atlanta Police Department.

Significant changes were made during the review and renewal of APD.SOP.4045 - Unmanned Aircraft Systems. We encourage you to read the policy below in its entirety to better understand how the Unmanned Aircrafts are:

- Regulated
- Used in a variety of circumstances out in the field
- Effective to support officer safety and Atlanta's Mission

Thank you and stay informed!

Policy and Standards Section
Planning, Research, and Accreditation Unit

Table of Contents

Policy Update ***1***
1. PURPOSE 3
2. POLICY 3
3. RESPONSIBILITIES 3
3.1 Authorization 3
3.2 Objectives 3
4. ACTION 4
4.1 UAS Program Personnel, Qualifications & requirements 4
4.2 UAS - Use and Deployment Procedures 5
4.3 Flight & Operating Guidelines 6
4.4 Aircraft Maintenance 7
4.5 Prohibited Acts 7
4.6 Emergency Procedures 8
4.7 Investigation of incidents: Civil and Public UAS 8
4.8 Evidence Collection & Retention 9
5. Implementation of the C-UAS per 6 CFR / 28 CFR § 124.6(a) 10
5.1 Responsibilities 10
5.2 Training and Certification 12
5.3 Authorized Technologies 12
5.4 Credible Threat Determination and Proportionality 13
5.5 C-UAS Operations Plan 13
5.6 Advance Coordination and Notification 14
5.7 Interagency and Lead-Agency Coordination 15
5.8 Real-Time Air Traffic Control Notification 15
5.9 Standing Tactical Procedures 15
5.10 Detection and Warning Operations 17
5.11 Confiscation and Forfeiture 17
5.12 Privacy, Civil Liberties, and Data Handling 18
5.13 Public Notification 20
5.14 Protection of Sensitive Operational Information 20
5.15 Post-Operation Reporting 20
5.16 Testing, Training, and Pre-Operational Validation 21
5.17 Compliance, Audit, and Enforcement 21
6. DEFINITIONS 22
7. CANCELLATIONS 24
8. REFERENCES 24
9. ADOPTION, LEGAL REVIEW, AND ATTESTATION ***25***

1. PURPOSE

The purpose of this policy is to establish guidelines and procedures for operations and investigating incidents utilizing Unmanned Aircraft Systems (UAS), commonly referred to as drones.

2. POLICY

It is the policy of the department that trained and authorized personnel may deploy and operate a UAS, C-UAS, and Drone First Responder when such use is appropriate in the performance of their official duties.

3. RESPONSIBILITIES

3.1 AUTHORIZATION

The UAS Unit will operate under the Special Events Division and must be specifically authorized by the Division Commander, or their designee, to deploy. The Atlanta Police Department has adopted the use of a UAS to provide an aerial visual perspective of the department's public safety mission.

3.2 OBJECTIVES

The departmental objectives within the UAS program are:

1. Situational Awareness – to assist the department in understanding the nature, scale, and scope of an incident and for the planning and coordination of an effective response.

2. Tactical Deployment – to support the tactical deployment of officers and equipment in emergency incidents.

    a. Hostage(s) incidents
    b. Barricaded suspects
    c. Reconnaissance for large scale tactical operations
    d. Perimeter security incidents
    e. Counter-Unmanned Aircraft Systems Tactics

3. Search and Rescue – to assist in:
    a. Missing person's investigations
    b. AMBER Alerts
    c. Mattie's Calls
    d. Other search and rescue operations

4. Visual Perspective – to provide an aerial reconnaissance to assist officers in providing direction for:
    a. Crowd control
    b. Traffic incident management
    c. Special circumstances
    d. Temporary perimeter security

5. Scene Documentation – to document:
    a. Crime scenes
    b. Serious injury and fatal vehicle collision scenes
    c. Natural and man-made Disasters
    d. Incident Command System (ICS) responses
    e. Large scale forensic scene investigations

4. ACTION

4.1 UAS PROGRAM PERSONNEL, QUALIFICATIONS & REQUIREMENTS

4.1.1 Personnel in the UAS program are expected to obtain and maintain the appropriate pilot rating and medical certification, as set forth by the FAA Certificate of Authorization.

4.1.2 All UAS personnel will be trained by approved instructors. The UAS pilots will meet all conditions of the FAA Certificate of Authorization.

4.1.3 A UAS Program Manager is responsible for the administrative and operational management of the UAS program and must hold the rank of Sergeant or above, have a minimum of 75 documented flight hours, and have completed tactical and specialized UAS training.

4.1.4 The UAS Program Manager, or designee, is responsible for, but not limited to, the following:

1. Liaise with the Federal Aviation Administration (FAA) as necessary and any relevant entities supporting the usage of UAS technology (e.g. educational, commercial interests, associations, etc.).
2. Maintain Certificate of Authorization applications and renewal applications according to appropriate FAA timelines.
3. Ensure that the UAS is maintained and flight ready according to the manufacturer's recommendations and related industry standards.
4. Complete timely registration for new aircrafts.
5. Identify and select personnel for UAS Program.
6. Authorize the launch of UAS upon valid request.
7. Ensure all personnel have met FAA part 107 requirements.
8. Develop and maintain a training calendar, which will include, at a minimum, monthly mandatory training.
9. Ensure all flight and flight logs are logged and up to date.
10. Develop and maintain appropriate UAS checklists.
11. Serve as Pilot in Command or Observer on UAS flights when needed.

4.1.5 A Pilot in Command will serve as a UAS primary pilot when designated by the Program Manager and must:

1. Maintain an FAA Remote Pilot Part 107 License before flying.
2. Have three (3) documented UAS take-offs and landings in the preceding 30 days

3. Not have two consecutive unexcused trainings absences.
4. Successfully complete the "Figure 8" course and National Institute of Standards and Technology (N.I.S.T.) course for outdoor missions

4.1.6 Pilots in Command will have the following, but not limited to, responsibilities:

1. Ensure UAS batteries are charged and installed properly according to the UAS checklist.
2. Evaluate all deployment characteristics to determine "go/no-go" for UAS flights (e.g. weather, airspace, surrounding area).
3. Ensure all checklists are followed during all flight phases.
4. Maintain sterile cockpit procedures during all UAS flights.
5. Notify UAS Program Manager in a timely manner of any mechanical/mishaps issues affecting the UAS aircraft or flight.
6. Document all flights and/or mechanical issues in the appropriate flight log.

4.1.7 Observers are individuals trained to maintain the line-of-sight and 360-degree hazard awareness around the UAS at all times. They will participate in deployments when requested, and have the following, but not limited to, responsibilities:

1. Assist the Pilot in Command with flight checklists.
2. Verify UAS batteries are charged and installed properly according to the UAS checklist, after the Pilot in Command inspects/installs flight battery.
3. Observe flight area and report to Pilot in Command anything that could affect the UAS flight.
4. Maintain sterile cockpit procedures during all UAS flights.
5. Monitor UAS flight time, and report regularly to the Pilot in Command.
6. Assume Pilot in Command duties if the initial Pilot in Command is unable to continue the UAS flight.

4.1.8 All tactical indoor pilots MUST show proficiency with manual drones to be considered for indoor drone operations and successfully complete the N.E.S.T (Navigation, Evaluation, in-Structural, and Tight spaces.

4.1.9 Failure to maintain proficiency, proper certifications and training can result in inability to operate/observe missions and possible removal from the UAS program.

4.2 UAS - USE AND DEPLOYMENT PROCEDURES

4.2.1 The department must obtain applicable authorizations, permits, and/ or certificates required by the FAA prior to the use/ deployment of UAS and DFR (Drone First Responder). This includes but is not limited to the receipt of a FAA Certificate of Authorization.

4.2.2 The use and deployment of the UAS will be monitored and regulated as follows:

1. Personnel Authorized – only personnel (pilots and crew members) who have been trained and certified (obtained FAA Remote Pilot Part 107 License) in the use/ deployment of the UAS are authorized to use/ deploy the device, to include all DFR operations and deployments.

2. Inspection – authorized/ certified personnel will inspect and test the UAS prior to each use/ deployment to verify the proper functioning of all components of the UAS and the airworthiness of the device.

3. Responsibility – UAS equipment is the direct responsibility of individual assigned officers. All UAS equipment will be used with reasonable care to ensure proper functionality. Equipment malfunctions will be brought to the attention of the UAS Team Leader as soon as possible so that appropriate repairs can be made, or a replacement unit can be procured.

4. Property of the Department – the unmanned aircraft, associated equipment, and all Distance Measuring Equipment associated with the UAS is the sole property of the Atlanta Police Department.

5. Use/ Deployment Records – All uses and deployments of the UAS will be accurately recorded on Drone Sense.

6. Public Notification – the Chief of Police may direct public notification of the use and deployment of the UAS on a case-by-case basis.

4.3 FLIGHT & OPERATING GUIDELINES

4.3.1 All flights will be conducted at less than 400 feet Above Ground Level (AGL), unless otherwise noted in the FAA Certificate of Authorization or approved directly by the FAA. All flights will be conducted under Visual Flight Rules (VFR).

4.3.2 The Pilot in Command is responsible for obtaining current weather reports from a standard Meteorological Terminal Aviation Routine report (METAR) and Terminal Aerodrome Forecast (TAF). The operational guidelines for these conditions are based upon visibility and operator safety at the local site, therefore the Pilot in Command and Observer must adhere to the line-of-sight Visual Flight Rules (VFR) and the minimum weather requirements as follows:

1. The operational guidelines for heat are less than 110 degrees Fahrenheit at ground level. Operation in temperatures over 110 degrees Fahrenheit should be noted with the air density as obtained from the pre-flight weather report. The battery and length of flight should be adjusted accordingly based upon high humidity and temperature with air density. These local conditions may warrant the Pilot in Command opting to not fly based upon these flight conditions.

2. The operational guidelines for cold are greater than 0 degrees Fahrenheit at ground level. Operation in temperatures under 0 degrees Fahrenheit should be noted with the air density as obtained from the pre-flight weather report. The battery and length of flight should be adjusted accordingly. Also, if the moisture level is high, conditions should be noted for icing on wings and flight surfaces. These conditions may warrant the Pilot in Command opting to not fly based up these flight conditions.

3. The UAS will not be operated in sustained winds greater than 22 knots (25 mph). Wind velocity can be obtained from a hand-held anemometer used at the training location or mission site. Wind information can also be obtained from the Meteorological Terminal Aviation Routine (METAR) and/or Terminal Aerodrome Forecast (TAF).

4.3.3 The Pilot in Command may, at their discretion, opt not to fly, despite being requested to fly, for operational conditions that exceed the limitations of the FAA Certificate of Authorization, manufacturer guidelines, or any other safety consideration deemed relevant by the Pilot in Command. The decision to not fly may not be overridden by a member of the department with more rank or authority over that of the Pilot in Command.

4.3.4 The Pilot in Command will have the following documents on their person during all UAS operations:

1. FAA Unmanned Aircraft License
2. Photo ID (Driver's License, Passport, etc.)
3. The UAS's FAA registration
4. FAA Certificate of Authorization
5. FAA Waivers to the Certificate of Authorization

4.4 AIRCRAFT MAINTENANCE

4.4.1 Maintenance

1. The UAS Program Manager is responsible for the maintenance of the UAS and will be specifically trained in the maintenance of the UAS based on the recommendations by the manufacturer.
2. The Pilot in Command and/or Observer will conduct and document a pre and post-flight inspection of the UAS after major changes in the hardware or software.
3. Any equipment issues will be immediately reported to the UAS Program Manager. It will be the responsibility of the UAS Program Manager to determine whether the reported information or issues need to be corrected prior to the next flight, which will then be documented in the aircraft's log.

4.4.2 Storage Transport - The UAS should be stored in the assigned aircraft case in a secure manner to limit possible damage to the unit while in transit. Batteries must be transported in an appropriate container to prevent possible damage to the batteries and should not be dropped or punctured.

4.4.3 Battery Charge - Any components necessitating a charged battery will be charged in accordance with manufacturer's recommendations. To the extent permissible by manufacturer's recommendations, the UAS will be fully charged when not in use. The Lithium-ion Polymer (LiPO) batteries should be charged and stored in a cool and dry location. Because of the fire hazard risk, batteries should not be left unattended when charging at full or rapid charge (vs. trickle charging) and should be charged at the recommended amperage and not exceeded. If the LiPO batteries begin smoking or expanding (puffing) they should immediately be isolated for risk of explosion or fire. Never completely discharge LiPO batteries or they will become un-useable (i.e. unable to hold a charge).

4.4.4 All aircraft changes will be documented in the aircraft's log by persons authorized to conduct UAS maintenance. All previously proven systems, to include payloads, may be installed or removed as required for missions and documented in the appropriate aircraft log.

4.5 PROHIBITED ACTS

4.5.1 The UAS will not be flown for any mission wherein the UAS Program Manager or the Pilot in Command determines the risk of flying the UAS outweighs the benefit to the mission. Risks may include hazards to individuals or property on the ground, possible collision hazard with other aircraft, loss of control of the UAS. The Pilot in Command has sole accountability for UAS flight determination. In addition, UAS Flights will:

1. Not be used for routine patrol duties.
2. Not be flown in conditions that exceed the manufacturer's recommended limitations, including range, ceiling, wind strength, and battery charge.

3. Not conduct random surveillance activities prohibited by state or federal law.
4. Not target a person or group based solely on individual characteristics, such as, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation
5. Not be operated in an unsafe manner or in violation of FAA rules or departmental policy
6. Not harass, intimidate, or discriminate against any individual or group.
7. Not spray or drop anything from the aircraft nor is it permitted to carry hazardous materials.
8. Not be weaponized.

4.5.2 UAS flights will comply with current federal laws, the issued FAA Certificate of Authorization, and FAA regulations regarding Class B, C, D, E, and G airspaces.

4.5.3 Unless authorized by the FAA only one UAS will be operated in a defined incident perimeter, by a single point of control, and by one pilot at a time.

4.5.4 Unless authorized by the FAA, daisy-chaining Observers to extend line-of-sight is prohibited.

4.5.5 Any unauthorized use of UAS or C-UAS technology may result in administrative discipline or potential violations of federal law.

4.6 EMERGENCY PROCEDURES

4.6.1 Forced Landing/Crash procedures (Reports, notifications, photos)

1. Pilot in Command will secure the scene and immediately notify the Aviation Unit Commander.
2. Crime Scene Investigation (CSI) Unit will process the scene, take photos and document the entire scene.
3. All members of the UAS Program at the scene that are involved will also notify the UAS Program Manager and make sure all information is available to complete the mandatory FAA online notification report, within the time allotted per Certificate of Authorization requirements.

4.6.2 The UAS Team is to perform Simulated Emergency Operations (Table-top Exercises) annually

1. Compass error/loss of GPS maneuvers, and
2. Loss of flight application information (tablet crash)

4.7 INVESTIGATION OF INCIDENTS: CIVIL AND PUBLIC UAS

4.7.1 Determine whether the UAS operations are in violation of state laws and/or federal regulations. If the UAS operations were involved in a more serious crime, include the appropriate law as additional information.

4.7.2 All reports involving UAS operations will ultimately be forwarded to the FAA; therefore, additional information outside the normal scope of Departmental report writing may be helpful to the FAA investigation and should be included in the report.

4.7.3 The following investigative considerations should be included where possible:

1. Identify the operator of the UAS and anyone assisting and/or witnessing the operation.

2. Obtain the operator's unmanned aircraft pilot license, when appropriate.

3. Document critical information, such as, but not limited to:

   a. The make, model, and series of unmanned aircraft and its payload.

   b. The FAA Registration number.

   c. The type of unmanned aircraft operator (hobby/recreational, commercial, or public)

   d. The flight path of the unmanned aircraft, including the location of the unmanned aircraft's take-off and landing and Document the time of all operations.

   e. Statements the operator may have made to other individuals in the area regarding the purpose of the flight.

   f. The weather conditions at the time of the UAS flight.

4. Determine:
   a. If the UAS was flown within five miles of an airport or Helipad (such as hospital helicopter pad). If so, document if the operator contacted the associated tower or controlling agency ahead of time for permission to do so.

   b. If the operation occurred in airspace associated with Hartsfield-Jackson Atlanta International Airport or other controlled airspace based on the UAS position on the ground and altitude. Contact FAA for assistance in determining if the operation occurred in controlled airspace.

   c. If operations occurred within an excluded area such as a Temporary Flight Restrictions (TFR). FAA can provide this information.

   d. The proximity of the UAS was flown in relation to people or property including estimated the altitude of the UAS. Use references such as "twice as high as the three-story building on the northwest corner at the location" (i.e., do not simply state "above 400 feet altitude").

   e. Determine if the UAS was flown in a careless or reckless manner (describe specific violations of Federal Aviation Regulations).

   f. What level of law enforcement action is required (Report Only/FIF/Arrest).

4.8 EVIDENCE COLLECTION & RETENTION

4.8.1 State and/or Federal UAS violation(s) may require that the aircraft, and its components, be seized as evidence.

4.8.2 The UAS is not required to activate the onboard video recorder during training missions, or any mission designated by the UAS Program Manager where recorded video is not integral to the mission of the UAS.

4.8.3 Photographic Evidence Procedures

1. Any video evidence obtained during flight will be stored in accordance with evidence collection policies and procedures.

2. Any video deemed non-evidentiary will be deleted with approval of the UAS Program Manager.

3. The Pilot in Command is responsible for downloading the in-flight video onto the designated platform, and notifying the lead investigator for the mission that in-flight video evidence is available for their case.

4. The lead investigator will facilitate recovery of the in-flight video and submission as evidence within their case.

4.8.4 In-flight video recordings will be considered subject to open records requests and will be retained in accordance to APD retention policies.

5. IMPLEMENTATION OF THE C-UAS PER 6 CFR / 28 CFR § 124.6(A)

This policy applies only to operations that require the authority of, or relief from certain laws under, 6 U.S.C. 124n. Detection and warning activity conducted with systems that do not require that authority, such as electro-optical, infrared, acoustic sensors, and radar that do not implicate the surveillance laws, may be governed by the agency's other policies and is not necessarily subject to this policy. (§ 124.2, definition of detection and warning operations.)

5.1 RESPONSIBILITIES

5.1.1 **City of Atlanta Police Department** designates Commander over the SRU, or his or her designee, as the Agency Approving Official. The Agency Approving Official approves C-UAS operations on behalf of the agency and signs each C-UAS Operations Plan. (§§ 124.2, 124.6(a)(1).) This personal may not serve as the mitigation operator for an operation that official approved. (§ 124.2.)

5.1.2 Only agency personnel whose assigned duties include the security or protection of people, facilities, or assets, and who hold the certification required for the authority exercised, may conduct operations under this policy. Atlanta Police will maintain a roster of certified personnel drawn from the NCUTC certification database and verifies the certification status of every person assigned to a C-UAS operation. (§§ 124.4, 124.5(c).) Contractors do not conduct operations or make operational determinations under this policy; contractor support is limited to technical support, maintenance, and training assistance, and to detection services that do not require the authority of 6 U.S.C. 124n. The agency does not enter into any arrangement under which a non-accredited agency, contractor, or vendor exercises de facto operational control of systems requiring that authority; where C-UAS support is provided or received through mutual aid or another written arrangement, certified personnel of the accredited agency operate the systems and make all operational determinations. (§ 124.4(b), (c), (d).)

Atlanta Police will establish the following recurrent training requirements for authorized personnel:

- Quarterly documented training. (§ 124.6(a)(2).)

5.1.3 For operations involving multiple personnel, Atlanta police will define the roles and responsibilities of each position, identifies which positions require Mitigation Certification and which require only Detection and Warning Certification, and establishes the communication and concurrence procedures between the mitigation operator and other personnel. (§ 124.3(e)(3).) The positions and their certification requirements are:

- C-UAS Command Post Supervisor – Overall authority for the operation; oversees detection, intercept, and mitigation actions. Coordinates with external agencies. Supervises tactical operations and ensures communication between operational positions, directing resources and coordinating response. No certification requirements are required unless assuming a role with requirements.

- Airspace Awareness Officer – Responsible for maintaining real-time awareness of known authorized aviation and for communicating that information to personnel authorized to initiate mitigation before any mitigation is executed. This role is often referred to as an "air boss" and serves as a centralized point of contact for team members involved in the C-UAS mission. Relays information and documents events in real-time. No certification requirements are required unless assuming a role with requirements.

- Evidence Lead – Preserves recovered UAS, payloads, flight logs, and electronic evidence. Compiles recovered information with pilot and incident documentation into case files. No certification requirements are required unless assuming a role with requirements.

- Mitigation Operator – Operates authorized mitigation systems, detection and warning systems, and executes approved mitigation actions. Maintains situational awareness of all aircraft operations, restricted airspace, temporary flight restrictions, and deconfliction issues. Must hold a current NCUTC Mitigation Certification covering the technology category employed, an NCUTC Detection and Warning Certification, a valid 14 CFR part 107 remote pilot certificate, and must be the individual who directly executes the mitigation command. Supervision of an uncertified person by a certified operator does not satisfy this requirement.

- Detection Operator – Operates authorized detection and warning systems. Maintains situational awareness of all aircraft operations, restricted airspace, temporary flight restrictions, and deconfliction issues. Must hold an NCUTC Detection and Warning Certification, a valid 14 CFR part 107 remote pilot certificate, and must be the individual who directly operates the authorized systems requiring 6 U.S.C. 124n authority. Supervision of an uncertified person by a certified operator does not satisfy this requirement.

- Ground Intercept Team (GIT) Member – Locates, secures, and recovers landed or disabled UAS and associated evidence. Contacts pilots of unauthorized UAS within the C-UAS operation for interview and conducts enforcement as appropriate. Requirements for GIT Members will be internal training on pilot contacts and safe evidence preservation practices.

- UAS Pilot – Operates authorized UAS to aid GIT Members in the location, identification, and tracking of suspects related to unauthorized UAS within the C-UAS operation. Required to hold a valid 14 CFR part 107 remote pilot certificate.

- Support Members – Mission dictated positions may be added at the discretion of the C-UAS Command Post Supervisor. Additional positions may include personnel from other agencies with specific interest to the C-UAS mission such as: FAA or Federal Liaison, Intelligence Analyst, Explosive Ordinance or Hazardous Device Technician, Legal Advisors, Critical Infrastructure Liaison, Visual Observer, etc. Such additional positions may require their own certification requirements outside of this policy.

The person who takes a mitigation action must hold a current Mitigation Certification covering the technology category employed and a valid 14 CFR part 107 remote pilot certificate, and must be the individual who directly executes the mitigation command. Supervision of an uncertified person by a certified operator does not satisfy this requirement. Support functions that do not initiate mitigation do not require Mitigation Certification but must be performed by personnel trained under this policy and, where the function operates systems requiring 6 U.S.C. 124n authority, by personnel holding a current Detection and Warning Certification. (§ 124.3(e)(1), (2).)

5.1.4 The certified mitigation operator retains independent professional judgment on whether to initiate a mitigation action. A supervisor, commander, or other official, regardless of rank, may direct the operator to withhold or cease mitigation and may provide operational direction, tactical context, and coordination guidance. No official, regardless of rank, may direct a certified operator to initiate a mitigation action when the operator has determined that the credible threat standard or the

proportionality requirement is not met. Non-certified personnel, regardless of rank, may not direct mitigation actions that override the certified operator's professional judgment on whether the conditions for mitigation are present. An operator who declines to mitigate based on a good-faith professional determination that the conditions are not met may not be subjected to adverse employment action for that decision. (§ 124.3(f).)

5.1.5 For operations where known authorized manned or unmanned aviation is operating or anticipated in or near the area of operations, Atlanta Police designates a person or position responsible for maintaining real-time awareness of known authorized aviation and for communicating that information to personnel authorized to initiate mitigation before any mitigation is executed. This role is often referred to as an "air boss." The designated person must be able to communicate directly with the mitigation operator. No mitigation action may be initiated without reasonable efforts to confirm that the target is not a known authorized aircraft. The scope and formality of this role must be commensurate with the complexity of the aviation environment. (§ 124.3(g).)

5.1.6 This policy is reviewed and concurred in by Atlanta Police Department's legal counsel before adoption and on each annual renewal. The review specifically addresses the privacy and civil liberties requirements of part 124, including data retention, minimization, and dissemination, and the interplay of the agency's C-UAS operations and this policy with applicable state, local, Tribal, or territorial law. If the agency has a designated official responsible for privacy and civil liberties compliance, that official also reviews this policy. (§ 124.6(b).)

5.2 Training and Certification

5.2.1 All personnel who operate systems requiring the authority of 6 U.S.C. 124n, or who make operational determinations, under this policy hold a current Detection and Warning Certification issued by the NCUTC. Detection and warning training or certification from any other source does not satisfy this requirement. The certification is the system of record in the NCUTC certification database. (§ 124.5(c).) Certification requirements for each operational position, including support functions that do not require certification, are stated below. (§ 124.3(e)(2).)

5.2.2 Personnel who take mitigation actions hold a current Mitigation Certification issued by the NCUTC covering each technology category they employ, and a valid 14 CFR part 107 remote pilot certificate. A current Detection and Warning Certification is a prerequisite for obtaining and maintaining a Mitigation Certification. Personnel who will operate only at correctional facilities may hold the abbreviated Correctional Mitigation Certification, which is limited to correctional-facility operations. The NCUTC is the sole certifying authority for mitigation operators. (§ 124.5(a), (d), (e).)

5.2.3 When a new technology category is added to the Authorized Technologies List, mitigation-certified personnel who completed the mitigation course before that addition complete the additional NCUTC training on the new category before using any system in that category. (§ 124.7(d).)

If the unit has personnel who held an NCUTC Mitigation Certification before the rule's effective date, they must complete the detection and warning curriculum by September 29, 2026, as § 124.5(n) provides; the Mitigation Certification remains valid and the detection and warning prerequisite is deemed satisfied during that period. Track and document completion.

5.2.4 Vendor-specific and system-level operator training is the agency's responsibility through its own training procedures and is provided before any person operates a specific system. (§ 124.5(c).)

5.3 Authorized Technologies

5.3.1 The City of Atlanta Police Department deploys only systems within technology categories on the Authorized Technologies List. Where the Authorized Systems List is populated for a category, the agency deploys only specific systems listed for that category. For categories on the Authorized Technologies List for which the Authorized Systems List is not yet populated, the agency may

deploy a specific system within the category only if the operator holds the certification covering that category and has completed manufacturer or vendor training on the specific system. (§ 124.7(b).)

5.3.2 APD employs mitigation systems only in technology categories covered by the NCUTC mitigation courses its certified personnel have completed. (§ 124.7(d).)

5.3.3 On receipt of an emergency suspension notice issued through the interagency process, Atlanta Police will immediately ceases deployment of the affected system or technology category and does not resume until the suspension is lifted or the system or category is restored, subject to any attached conditions. (§ 124.7(g).)

5.4 Credible Threat Determination and Proportionality

5.4.1 Before taking any mitigation action, personnel reasonably determine, under the totality of the circumstances, that a credible threat exists. The determination is made in real time by the certified and trained personnel closest to the operational situation and is documented in the post-operation report. For mitigation, the determination must be supported by a contemporaneous indicator that the specific UAS at issue poses a current, articulable risk if unabated. A contemporaneous indicator need not independently establish a threat; considered with the totality of the circumstances, it must provide a present-tense basis for concluding that the specific aircraft poses a current risk. Activity protected by the First Amendment may not be considered. (§§ 124.2, 124.3(b).)

5.4.2 A credible threat may be based on, among other things, specific intelligence; behavioral indicators such as flight in restricted airspace, approach toward a protected interest, failure to respond to warnings, or evasive maneuvering; payload or configuration indicators; unauthorized surveillance of a protected interest; indications of unauthorized access to protected information; and pattern-based indicators. A single indicator may establish a credible threat where it is sufficiently probative. (§ 124.2.)

5.4.3 Mitigation actions must be proportionate to the credible threat. Personnel employ the least disruptive effective means available under the totality of the circumstances. If equipment is available and time permits, a warning to the remote pilot in command should precede any mitigation action. Every warning delivered is documented, including who delivered the warning, when, by what means, and the operator's response. Before any action that may disable, damage, or destroy a UAS, personnel consider whether the threat outweighs the risk of collateral harm to public safety, including falling debris, harm to persons or property on the ground, disruption to communications, and risks to aviation safety. A mitigation action that creates a greater risk to public safety than the threat it addresses is not proportionate and must not be taken. (§ 124.3(c).)

5.5 C-UAS Operations Plan

5.5.1 Each mitigation operation, and each detection and warning operation that uses systems requiring 6 U.S.C. 124n authority, is authorized by a C-UAS Operations Plan signed by the Agency Approving Official before operations begin. The signed plan certifies that the operation is consistent with this policy, that the operators hold the required certification, and that the risk-based assessment factors have been addressed. APD does not commence mitigation operations until both the advance coordination process and the signed plan are complete. (§ 124.8(a).) The plan is submitted through the designated federal C-UAS coordination portal as a supplement to the advance notification not fewer than 7 calendar days before operations commence, or as early as practicable when the notification timeline does not permit 7 days, and material updates are resubmitted promptly. (§ 124.8(f).) For a detection and warning operation not subject to advance notification, the plan is submitted through the portal before operations commence, for situational awareness and recordkeeping, not as a supplement to an advance notification. (§§ 124.8(f), 124.12(c).)

5.5.2 The plan is prepared on the standardized form set by the Attorney General. It uses short-answer and selection fields and map or diagram attachments and does not repeat standing procedures in this policy. For a detection and warning operation, fields specific to mitigation do not apply. The

plan references this policy by title and version rather than repeating standing procedures. (§ 124.8(c), (g).)

5.5.3 The plan addresses, to the extent applicable: operation identification and points of contact; systems and airspace, including ATL category or ASL system and RF parameters; coordination confirmation, including operator certification status, compliance with this policy, legal counsel certification, and privacy compliance; and operational planning elements. (§ 124.8(b), (d).)

5.5.4 The plan addresses the risk-based assessment factors in § 124.8(e), including potential impacts to aviation safety and the use of the airspace, technical and siting limitations, options for mitigating identified impacts, the ability to provide advance notice to aircraft operators, the setting and character of the protected interest, and the potential consequences to public safety if a UAS threat is not addressed. (§ 124.8(e).)

5.5.5 A single plan may authorize operations for up to 30 consecutive calendar days. For fixed-site persistent-protection operations, including correctional facilities, critical infrastructure sites, and recurring venues, the Agency Approving Official may authorize a standing operational window of up to 365 calendar days, renewable on submission of a renewal plan. No plan may authorize an indefinite or open-ended window. Material changes require an update. (§ 124.8(h).)

5.6 Advance Coordination and Notification

5.6.1 Before any mitigation operation, C-UAS Lead, will submit an advance notification through the designated federal C-UAS coordination portal not fewer than 30 calendar days before the operational period. When 30 days is not feasible, the agency submits as early as circumstances permit, with enough lead time for federal review, and includes a brief explanation. The advance notification is a coordination document, not a request for approval; the absence of a federal response does not affect the agency's authority to proceed. (§ 124.9(a).)

5.6.2 Before any mitigation operation, the Atlanta Police Department will coordinate with the Department of Transportation and the Federal Aviation Administration through the FAA-designated coordination mechanism, providing the systems to be deployed, the coordinates of each deployment and enforcement location, the expected duration, and a characterization of the airspace. The agency operates within any flight restriction the Administrator establishes. The agency also submits a comparable advance notification to the State if state law or policy requires it. (§ 124.9(b), (d).)

5.6.3 Before deploying any C-UAS system that emits radio waves, whether for detection, warning, or mitigation, the C-UAS Lead will obtain authorization consistent with Title III of the Communications Act of 1934 and complies with Federal Communications Commission requirements, submitting its request through the advance notification process and as the Commission directs. (§ 124.9(f).)

5.6.4 When a credible threat poses an imminent risk to human life and advance coordination is not practicable, APD may take mitigation action and then complete the required notifications as soon as practicable, and in any event within two hours. If the action uses an RF-emitting system, the agency also complies with the real-time air traffic control notification requirement. Each invocation is documented in the post-operation report with a specific explanation of why advance coordination was not feasible. This exception is not a routine alternative to advance coordination, and a pattern of invocations may result in compliance review and penalties. (§ 124.9(g).)

5.6.5 Before conducting any operation within a security or protection mission overseen by a federal entity, or within an area over which a federal entity exercises a security or protection responsibility (such as a coastal waterway, airport, military facility, etc.), the APD will coordinate with that entity through the advance coordination process. (§ 124.9(h).)

5.7 Interagency and Lead-Agency Coordination

5.7.1 For operations supporting National Special Security Events, events rated Special Event Assessment Rating 1 through 3, or other events where federal C-UAS operations are anticipated, APD will notify the local Federal Bureau of Investigation field office of its intent to provide C-UAS coverage as early as practicable, and may use the notice-of-intent function in the federal portal. A notice of intent is informational only. (§ 124.10(a).)

5.7.2 Where a lead C-UAS agency has been designated for an event or location, APD will operate under the tactical coordination of the lead agency for the duration of the event and conform its C-UAS Operations Plan to the lead agency's operational framework. Whenever federal, state, and local law enforcement operations occur at the same event or overlap in area and time, the federal agency is the lead C-UAS agency. An agency that does not accept tactical coordination by the designated lead agency may not conduct operations, including detection and warning operations using systems requiring 6 U.S.C. 124n authority, within the covered area and time. (§ 124.10(c), (d).)

5.7.3 When the Federal Bureau of Investigation and the Department of Homeland Security notify the Atlanta Police Department of overlapping state and local law enforcement operations, the affected agencies will designate a lead C-UAS agency or establish a joint coordination arrangement, documented and provided to the FBI and DHS, before any agency commences mitigation operations in the overlapping area. (§ 124.10(e).)

5.8 Real-Time Air Traffic Control Notification

Any time APD activates a C-UAS system for mitigation purposes, personnel provide verbal or electronic notification, within five minutes of activation or as soon as operationally practicable, to the notification point the Federal Aviation Administration designates for real-time C-UAS coordination, using the jointly established procedures. The notification identifies the type of C-UAS action, the time of activation, and the location. On termination of the mitigation action, personnel provide a follow-up notification confirming the time of termination. (§ 124.11(a), (b), (c).)

5.9 Standing Tactical Procedures

This section states the standing tactical procedures required by § 124.6(a)(6). These procedures govern the execution of C-UAS operations. The C-UAS Operations Plan references this section rather than repeating it.

5.9.1 **Engagement protocols:** Before any engagement, personnel account for the risk to persons and property on the surface and in the air. No mitigation is initiated without reasonable efforts to confirm the target is not a known authorized aircraft and a contemporaneous determination that the credible threat and proportionality standards are met. When the totality of circumstances allow, aircraft identifying information will be searched in applicable databases to determine if the flight is authorized. An attempt to visually surveil the aircraft whether by ground intercept team or aerial overwatch to collect credible information will be attempted. Nothing in this text shall prevent immediate mitigation if the operator reasonably believes there is a threat to public safety. (§§ 124.3©, (g), 124.6(a)(6).)

5.9.2 **Escalation procedures:** Personnel use the least disruptive effective means first and escalate only as the threat and the totality of the circumstances require. A reasonable attempt to locate and warn the pilot by a ground intercept team should be initiated upon discovery of the aircraft. If the attempt to locate or warn the pilot is unsuccessful mitigation should be attempted by the least disruptive means available to agency personnel at that time. If the first attempt is unsuccessful, members are authorized to utilize additional means for the purposes of public safety. Nothing in this text should prevent a member from taking immediate disruptive action if the totality of circumstances indicates a reasonable threat to public safety. This may be only one factor, such as but not limited to, the unlawful intrusion into restricted air space.

5.9.3 **Use-of-force considerations:** A mitigation action that is likely to disable, damage, or destroy a UAS is taken only after personnel weigh the threat against the risk of collateral harm to public safety and that member reasonably believes that not taking action would result in an injury to themselves or third party.

5.9.4 **Ground intercept team procedures:** Ground Intercept Team (GIT) will be comprised of a minimum of two personnel, one of which will be a certified Part 107 UAS pilot, when possible. ATAK (Android Team Awareness Kit) or similar should be utilized to expedite GIT response whenever technological resources support the system employment. A communication plan, as well as a GIT operational directive plan, should be established by the C-UAS Command Post Supervisor, or his designee.

A GIT should be dispatched as soon as it is reasonably believed a detected UAS may pose a threat to a protected asset or public safety. Upon locating the downed aircraft, members should follow the established operational directive for handling and the request of supportive resources. The operational directive is likely to change each operation due to available resources and environmental circumstances. To ensure overall team effectiveness, the approved directive will be briefed to the GIT members.

5.9.5 **Render safe procedures:** A downed or recovered UAS may present a hazard, including an explosive or hazardous payload. If obvious signs of an improvised explosive payload are present, or information collected indicates the potential of an improvised explosive, hazardous, and/or chemical payload would be present, a safe perimeter around the aircraft should be established. Additional and/or Specialty resources should be requested. Personnel do not approach or handle a suspected hazardous device except as the agency's procedures allow.

5.9.6 **Evidence collection and chain of custody:** A UAS seized or confiscated, and any recovered components or media, are collected, documented, and preserved consistent with APD evidence and chain-of-custody procedures. A physical seizure or confiscation under 6 U.S.C. 124n(b)(1)(E) is documented through normal evidence-handling procedures outlined in APD Policy 12.01. Confiscation authority under 6 U.S.C. 124n(b)(1)(E) is outlined within this policy.

5.9.7 **Communications procedures:** The C-UAS Command Post Supervisor, or his designee, shall develop a clear communication plan for every operation. If the operation involves multiple agencies, the communication plan will be approved by the Lead CUAS agency. All members will be briefed on the communication plan. When possible, the air space coordinator will be in close proximity to the member conducting mitigation operations or, at minimum, in direct communication.

5.9.8 **System operating procedures:** Personnel operate each system within its authorized configuration and within any operating restriction stated on the Authorized Systems List. When a system permits adjustment of the scope of interception, operators use the narrowest configuration consistent with operational effectiveness. (§ 124.14(c)(2).)

5.9.9 **Data handling and purge procedures:** Personnel handle, retain, and purge data as directed by this policy, including the 180-day limit on records of communications and the purge of incidental material. Operations follow the data handling and purge procedures, and each operation concludes with verification that data subject to purge has been deleted. (§§ 124.6(a)(6), 124.14.)

5.9.10 **Operation plan requirements:** No operation may begin without a C-UAS Operations Plan signed by the Agency Approving Official. (§§ 124.6(a)(6), 124.8.)

5.9.11 **Post-operation procedures:** After each operation, personnel complete demobilization, post-operation reporting as instructed within this policy, and data purge verification, and record the verification in the audit trail. (§§ 124.6(a)(6), 124.13, 124.14(g).)

5.10 Detection and Warning Operations

5.10.1 The APD Drone unit will conduct detection and warning operations under this policy when all personnel hold a current Detection and Warning Certification, the agency deploys only systems within ATL categories and, where populated, ASL systems, the operation is authorized by a C-UAS Operations Plan, and the agency complies with the privacy, data handling, and retention requirements of this policy. Detection and warning operations that do not emit radio frequency energy and do not affect aviation safety do not require per-operation advance notification, FAA coordination, or FCC coordination. For RF-emitting detection or warning systems, the advance coordination requirements apply. (§ 124.12(b), (c).)

5.10.2 City of Atlanta may plan and conduct an operation as a detection and warning operation even though it maintains mitigation capability and mitigation-certified personnel. An operation in which no mitigation system is deployed, and no mitigation capability is enabled is a detection and warning operation; a system with both detection and mitigation capability is a detection system for an operation in which its mitigation capability is not enabled. Mitigation-certified personnel may conduct detection and warning operations under this section; the current Detection and Warning Certification their Mitigation Certification presupposes satisfies the certification requirement. (§§ 124.2, 124.5(a).)

5.10.3 A detection and warning operation is not subject to the mitigation-specific requirements of this policy: the advance notification and coordination outlined within this policy, except for RF-emitting systems; the real-time air traffic control notification; and per-event post-operation reporting. It is authorized by a C-UAS Operations Plan, in which the mitigation-specific fields do not apply, and detection activity is reported in the semiannual operational summary. (§§ 124.9(i), 124.11, 124.12(c), (d).)

5.10.4 If a detection operation identifies a credible threat requiring mitigation, the agency responds through mitigation-certified personnel under this policy. (§ 124.12(e).)

5.11 Confiscation and Forfeiture

5.11.1 Personnel holding a current Detection and Warning Certification may seize or otherwise confiscate an unmanned aircraft that is no longer active in flight, or any other UAS component, such as a ground control station, under 6 U.S.C. 124n(b)(1)(E). The authority is contingent on a credible threat, assessed by the guidelines outlined within this policy, and the basis for the determination is documented in the operational record. Confiscation under this section does not require Mitigation Certification, systems on the Authorized Technologies List or Authorized Systems List, or advance coordination. (§ 124.17(a)(1), (2).)

5.11.2 Any action that affects an unmanned aircraft in flight, including catching or netting an aircraft by hand or with a non-electronic physical device, implicates 6 U.S.C. 124n(b)(1)(D), (E), or (F), requires Mitigation Certification, and is conducted only under required guidelines explained within this policy. The erection of physical barriers that a UAS operator has an obligation to avoid, such as netting affixed to a structure, is not mitigation. A seizure under traditional law enforcement authority, including of an abandoned or crashed aircraft, incident to arrest, or pursuant to a warrant or a recognized exception, is independent of 6 U.S.C. 124n, requires no certification, and is not governed by this policy. (§ 124.17(a)(3), (5), (7).)

5.11.3 A confiscated unmanned aircraft and any recovered components or media are handled under the evidence collection, chain-of-custody, and render safe procedures, including preservation of digital evidence stored on the aircraft and its flight controller; personnel do not power on, reset, pair with, or interrogate a device except under the agency's digital-forensics procedures. Once the aircraft is on the ground and confiscated, subsequent actions, including threat assessment, render safe

procedures, evidence collection, and search warrant execution, are governed by traditional legal authorities, including the Fourth Amendment. (§ 124.17(a)(4), (5).)

5.11.4 When an operation involves a known or suspected unmanned aircraft being used as a delivery mechanism for a hazardous device, the response to the hazardous device is conducted by a public safety bomb squad accredited through the Federal Bureau of Investigation's Hazardous Devices School. A seized UAS or unmanned aircraft is subject to forfeiture under the laws of the Atlanta Police Department's jurisdiction.

5.12 PRIVACY, CIVIL LIBERTIES, AND DATA HANDLING

5.12.1 In exercising authority under this policy, The Atlanta Police Department and its personnel comply with 6 U.S.C. 124n(e) and implement privacy protections for the interception, acquisition, access, maintenance, use, and dissemination of communications, consistent with the First and Fourth Amendments and applicable federal law. Individual searches and seizures during operations remain subject to the Fourth Amendment reasonableness requirement and the agency's search-and-seizure policies. (§ 124.14(a).)

5.12.2 **First Amendment:** No C-UAS authority is used solely to seize, monitor, deter, interfere with, or disrupt individuals exercising First Amendment rights. Where operations occur at events or locations where individuals are exercising First Amendment rights, personnel take affirmative steps to minimize the collection, retention, and dissemination of information about those individuals and do not use C-UAS-derived information to identify, track, or build records on individuals based on protected activity. (§ 124.14(b).)

5.12.3 **Scope of interception and minimization:** Communications are intercepted or acquired only to the extent necessary to support an authorized action. Material that is not control communications is incidental capture. The Atlanta Police Department configures systems to minimize incidental capture. Incidentally captured material that is not relevant to a C-UAS, law enforcement, or national security purpose is not reviewed, retained, or disseminated and is purged as soon as practicable. If it becomes apparent that a captured video, audio, or other data stream is not control communications, the interception of that stream is discontinued, and the incidental capture is documented in the post-operation report. Where identifying a threat requires processing the control signaling of all unmanned aircraft in range, the control communications of an aircraft determined not to pose a threat are not retained or used beyond what is needed to make the threat determination and are purged on the same schedule as other incidental material. (§ 124.14(c)(2), (4).) During an operation, personnel view incidentally captured material only as necessary for C-UAS purposes. For standing detection deployments exceeding 30 days, the agency conducts a review at least quarterly to confirm that the scope of interception remains proportionate and that minimization and purge procedures are on schedule. (§ 124.14(c).)

5.12.4 **Records of communications and retention:** Control communications captured or maintained by the agency's systems are records of communications under 6 U.S.C. 124n(e)(3) and are maintained only as long as necessary, and in no event more than 180 days, unless the Agency Approving Official or the agency's chief legal officer determines that retention is necessary to investigate or prosecute a violation of law, to directly support an ongoing security operation, for litigation, or as required by law. Data retained under the ongoing security operation exception is reviewed at 90-day intervals and purged when the operation concludes. When records will be retained beyond 180 days, the agency notifies the Federal Bureau of Investigation through the portal within 30 days of the determination, and documents the specific basis for retention unless an open investigative or prosecutorial case file already documents the data as evidence. Pattern data extracted and recorded independently is not a record of communications and is not subject to the 180-day limit. (§ 124.14(d).)

5.12.5 **Anonymization standards for pattern data:** The Atlanta Police Department qualifies a data product as pattern data only when it meets the following written anonymization standards: An aggregation threshold of less than 5 observations or events before a product may be released,

Suppression of the following identifiers (For example UAS serial or device ID, operator or take-off location, precise timestamps), and a re-identification risk assessment performed by a C-UAS Command Post Supervisor before release. (§§ 124.6(a)(3), 124.2.)

5.12.6 **Dissemination:** Control communications acquired under this policy are disclosed outside the Atlanta Police Department only as 6 U.S.C. 124n(e)(4) allows: when necessary to investigate or prosecute a violation of law; to support the Department of War, a federal law enforcement agency, or a federal regulatory agency's enforcement activity in connection with an action described in 6 U.S.C. 124n(b)(1); or as otherwise required by law. Because the agency's authority is limited to protecting against a credible threat, control communications are disseminated only for law enforcement action arising from the UAS activity that prompted the operation, or for aviation safety, unless the communications are independently obtainable through lawful means not dependent on 6 U.S.C. 124n. At dissemination, the agency communicates the protective purpose and records, in the audit trail, the legal basis, the category of recipient, whether the handling caveat was conveyed, and whether control communications were included. (§ 124.14(e), (f).)

5.12.7 **Handling caveat:** Data acquired under 6 U.S.C. 124n is marked with a handling caveat at dissemination. Unless The City of Atlanta adopts different wording, the caveat reads: “LAW ENFORCEMENT SENSITIVE // 6 U.S.C. 124n C-UAS DATA — Use limited to the stated protective purpose (§ 124.14(f)). No further dissemination without the originating agency’s consent. Contains records of communications: delete within 180 days of acquisition unless a documented § 124.14(d) exception applies. POC: Open Records Unit. The rule prescribes no caveat wording; this marking implements the sensitivity-designation requirement and supports the audit-trail record of whether the caveat was conveyed. (§§ 124.14(e)(3), (f), 124.15(c).)

5.12.8 Pattern data containing no control communications may be disseminated consistent with the agency's standard data handling and information sharing policies and applicable law. Before disseminating pattern data beyond the agency, the agency verifies anonymization and screens the product for operationally sensitive information. Public release of pattern data products requires approval by the Open Records unit. (§ 124.14(e)(5).)

5.12.9 **Audit trail:** Atlanta Police will maintain an audit trail sufficient to document each instance in which C-UAS authority was exercised, the basis for the action, the disposition of any data acquired, and any dissemination. The audit trail is searchable, accessible to compliance auditors, protected against unauthorized modification or deletion, and retained for at least six years. The format and system of records for the audit trail is controlled by the digital preservation on the departments Microsoft Onedrive cloud-based server storage. (§ 124.14(g).)

5.12.10 **Third-party sources and vendor data: The Atlanta Police Department** does not request, purchase, subscribe to, or operationally rely on intercepted UAS control communications acquired by any actor lacking lawful authority and relief for the underlying interception. When the agency acquires UAS intelligence from a third-party source, it documents the source's lawful authority and applies the retention and dissemination requirements of this policy to that data. The agency may provide operational raw sensor data to system vendors for diagnostics, troubleshooting, and performance validation only after removing any communications content and only for the stated purpose of the services requested of the vendor. (§ 124.14(i), (j).)

5.12.11 **State and local retention conflicts:** If a state, local, Tribal, or territorial records retention requirement applicable to the agency's records encompasses C-UAS communications data and the agency cannot comply with both the 180-day limit and that requirement, APD retains the data for the period the applicable law requires and applies the handling restrictions of this policy, including the prohibition on use for unrelated law enforcement purposes and the dissemination restrictions, for the full duration of retention. (§ 124.14(h).)

5.13 PUBLIC NOTIFICATION

The City of Atlanta Police Department will provide public notification regarding the potential use of C-UAS authority within its jurisdiction by publishing a public version of this policy on the Department website. Public notification shall describe the existence and general purpose of the program without revealing operational specifics, capabilities, or coverage patterns. (§ 124.6(a)(4).)

5.14 PROTECTION OF SENSITIVE OPERATIONAL INFORMATION

5.14.1 Information that links the specific capabilities, vulnerabilities, operating parameters, or countermeasure effectiveness of C-UAS systems to planned or completed operations, including deployment locations, operating frequencies, tactical methods, and threat-specific approaches, is treated as law enforcement sensitive and protected from public disclosure to the extent applicable law permits. Where such information reveals a capability gap of national security concern, it is evaluated for classification. Other operational coordination information, such as the existence, general timing, or general coverage area of a deployment, is handled as Controlled Unclassified Information. General technical specifications not tied to a specific operation are not subject to these handling requirements. (§ 124.15(a).)

5.14.2 The Atlanta Police Department takes the steps available under applicable state, local, Tribal, or territorial law to protect operationally sensitive information from disclosure through public records requests or civil discovery, and coordinates with the prosecuting authority in any criminal prosecution to limit testimony and pleadings to the information necessary to establish the elements of the offense. Advance notifications, C-UAS Operations Plans, post-operation reports, and audit records are marked with appropriate sensitivity designations. Nothing in this section requires action inconsistent with applicable public records law. (§ 124.15(b), (c).)

5.15 POST-OPERATION REPORTING

5.15.1 The City of Atlanta Police Department will submit a post-operation report through the designated federal C-UAS coordination portal within 48 hours of whichever occurs first: taking any mitigation action; any confiscation of a UAS under 6 U.S.C. 124n(b)(1)(E), including a standalone confiscation under § 124.17(a), other than a confiscation resulting from a detection and warning operation; or the conclusion of an operation for which notification was provided. Submission through the portal satisfies notification to both the Attorney General and the Secretary of Homeland Security. (§ 124.13(a), (d).) A confiscation under 6 U.S.C. 124n(b)(1)(E) that results from a detection and warning operation under this policy is documented through APD's normal evidence-handling procedures and is not separately reported; detection and warning operations do not require per-event reporting. (§ 124.12(d).) A standalone confiscation is reported even though no operation surrounds it: it relies on federal authority for the taking itself and occurs without advance coordination or an operations plan, so the report is the only federal oversight record of that exercise. A seizure under traditional law enforcement authority is independent of 6 U.S.C. 124n and is not reported under this part. (§ 124.17(a)(5).)

5.15.2 The report contains the content required by § 124.13(c): whether the operation occurred as notified; the date, time, and location of the reportable action; a brief description of the credible threat; the type of capability employed by reference to the ASL and ATL category and, in all cases, the make, model, hardware version, firmware revision, and software version of each system as deployed; any known operational effects, including any effect on other aviation systems, spectrum users, or persons and property, any aviation accident, and any temporary flight restriction granted or denied; any anomalies or deviations; and summary operational statistics. The credible threat determination is documented as part of this report. (§§ 124.3(b), 124.13(c).)

5.15.3 If any detection, warning, or mitigation action results in unintended consequences, including interference with manned aviation or lawfully operating UAS, property damage, injury, or a malfunction affecting third parties, the supervisor of the Unit will immediately notify the Federal

Bureau of Investigation and the Department of Homeland Security by the most expedient means available, in addition to the 48-hour report. Where multiple reportable events occur within a 48-hour period, the agency may submit a single consolidated report. For recurring venue operations under a standing operational window, each discrete event is reported separately. (§ 124.13(e), (f), (g).)

5.15.4 **Semiannual operational summary:** The C-UAS Lead, or their designee, will submit a semiannual operational summary through the portal, covering total operations, mitigation actions, detection activity (counted in good faith as confirmed detections attributable to a distinct unmanned aircraft, with reasonable deduplication, § 124.13(c)(7)), instances of retention of records of communications beyond 180 days, instances in which control communications were disclosed outside the agency organized by legal basis, compliance issues, and lessons learned. The summary also reports requests the agency received for C-UAS protection from critical infrastructure or airport owners or operators that are not SLTT law enforcement or correctional agencies, the number it supported, and the number it could not support with reasons. (§ 124.13(h).)

5.16 TESTING, TRAINING, AND PRE-OPERATIONAL VALIDATION

The Atlanta's UAS Unit may conduct operational acceptance testing of acquired or candidate systems, on-the-job proficiency training, and interoperability exercises to maintain readiness. Testing and training do not involve the mitigation of a credible threat and are not conducted under 6 U.S.C. 124n(a)(2). RF-emitting systems are operated during testing and training only under applicable Federal Communications Commission authorization and Federal Aviation Administration coordination, and only against controlled test targets owned or operated by, or operated with the consent of, the agency. The agency uses only approved technologies and verifies that all necessary FAA authorizations or relief for operating any unmanned aircraft, including a UAS forming part of a C-UAS system, have been obtained before any testing or exercise. Any communications incidentally collected from non-participating third parties during testing, training, or exercises are purged at the conclusion of the activity, or as soon as practicable thereafter, and the purge is verified in the audit trail. (§ 124.18(e).) Compliance with this section is a condition of maintaining certification and accreditation. (§ 124.18.)

5.17 COMPLIANCE, AUDIT, AND ENFORCEMENT

5.17.1 Atlanta Police will retain this policy and make it available to the Attorney General or the Secretary of Homeland Security, or their designee, on request, including during compliance audits. The agency cooperates with periodic federal compliance audits, which include review of post-operation reports, advance notification records, and this policy. (§§ 124.6(e), 124.16(a).)

5.17.2 The agency understands that knowingly taking mitigation actions without the required federal coordination, real-time air traffic control notification, or post-action notification may subject the agency or its personnel to a civil fine of up to $100,000 per violation or suspension of C-UAS authority, and that violations of other requirements of part 124 are addressed through the compliance audit program and certification or accreditation suspension. (§ 124.16(b), (d).)

5.17.3 Before conducting operations, the agency head or designee certifies compliance through the federal C-UAS coordination portal by attesting that APD has adopted this policy addressing each required element. The attestation is renewed annually. Conducting operations without current attestation is a violation of part 124. (§ 124.6(d), (f).) Until the designated federal C-UAS coordination portal is fully established, the agency completes attestations and other required submissions through the interim channel designated by the Federal Bureau of Investigation and the Department of Homeland Security, including the standardized interim filing forms. (§ 124.9(c).)

6. DEFINITIONS

Definitions are reproduced here for the reader's convenience; many of which the rule controls.

- **Agency Approving Official:** The senior official designated by the agency, authorized to approve C-UAS operations on the agency's behalf. The official must not be below the rank of a Senior Executive or Senior Official or its equivalent, except that for an agency with no equivalent rank, the agency head or the agency head's designee may serve. The Agency Approving Official may not serve as a mitigation operator for an operation that official has approved.
- **Authorized Technologies List (ATL):** The list of authorized technology categories for SLTT law enforcement and correctional agency C-UAS operations, maintained jointly through the federal interagency process.
- **Authorized Systems List (ASL):** The subset of the ATL that identifies specific systems, by make, model, and version, approved by the interagency body for operational use within one or more ATL categories, with any stated operating restrictions. The ASL is populated on a phased basis.
- **Civil UAS**: An unmanned aircraft or UAS operated for purposes other than strictly hobby or recreation (generally used for commercial, business, or media purposes). The operator must obtain an authority to operate from the FAA. There are two such authorities; one or the other must be present:
- **Components**: The following are considered components of the UAS: the remote-control device which could be in the form of a radio, Bluetooth or Wi-Fi enabled device (to include a smart phone or tablet), the payload, and any Subscriber Identity Module (SIM) cards or multimedia storage devices associated with the unmanned aircraft.
- **Control communications:** Any wire, oral, or electronic communication used to navigate, command, or otherwise control a UAS, including telemetry, command-and-control signals, and any video, audio, or data stream used to navigate the aircraft when other telemetry is unavailable. The operational role of a communication, not its packet type or frequency, determines whether it is a control communication. Control communications also include a UAS unique identifier and the operator or take-off location, location, velocity, and emergency status of the UAS when that information is acquired by intercepting a communication under the relief provided by 6 U.S.C. 124n.
- **C-UAS Operations Plan:** The event-specific or operation-specific document, signed by the Agency Approving Official, that authorizes a given operation and certifies it is consistent with this policy. (§ 124.8.)
- **Credible threat:** A threat that, based on the totality of circumstances known to the operator at the time, would cause a reasonable person in the operator's position, considering training and experience, to conclude that a UAS poses an articulable risk to a protected interest. Activity protected by the First Amendment may not be considered.
- **Data purge verification:** Documented confirmation that records subject to purge have been deleted from all systems on which they were stored, recorded in the audit trail.
- **Defined Incident Perimeter**: The location has a defined perimeter to be determined based on the scope of the operation and a defined operational ceiling at or below 400 feet Above the Ground.
- **Detection and Warning Certification:** Certification, issued only by the NCUTC, that personnel completed the online detection and warning curriculum and passed the post-course assessment. It authorizes the holder to exercise the authorities in 6 U.S.C. 124n(b)(1)(A), (B), and (E).
- **Detection and warning operations:** Operations conducted using systems whose operation requires the authority of, or relief from certain laws under, 6 U.S.C. 124n, involving only detecting,

identifying, monitoring, tracking, and warning. Activity using systems that do not require that authority is not subject to part 124.

- **Detection system:** A system used to detect, identify, monitor, or track a UAS, or to warn its operator, with no capability enabled to disrupt, seize control of, disable, damage, or destroy a UAS.
- **Drone First Responder (DFR):** A program or operational model utilizing Unmanned Aircraft Systems (UAS) as an initial response tool to calls for service, enabling real-time aerial intelligence to support incident assessment, enhance officer and public safety, and inform tactical and operational decision-making.
- **FAA Certificate of Authorization:** An authorization issued by the Air Traffic Organization to a public operator for a specific unmanned aircraft activity. If necessary, provisions or limitations may be imposed as part of the approval to ensure the unmanned aircraft can operate safely with other airspace users. (FAA.gov)
- **Mitigation action:** An action described in 6 U.S.C. 124n(b)(1)(C), (D), or (F): disrupting, disabling, interfering with, seizing control of, or using reasonable force to disable, damage, or destroy a UAS. Detection and warning are not mitigation actions.
- **Mitigation Certification:** Certification issued by the NCUTC authorizing the holder to exercise the mitigation authorities in 6 U.S.C. 124n(b)(1)(C), (D), and (F), within the technology categories the holder's completed courses cover. A current Detection and Warning Certification is a prerequisite.
- **Mitigation operation:** An operation in which a mitigation system is deployed to take a mitigation action, whether or not a mitigation action is actually taken. It may include detection and warning elements.
- **Mitigation system:** A system used or capable of being employed to take a mitigation action. A system with both detection and mitigation capability is a mitigation system while its mitigation capability is enabled.
- **National Counter-UAS Training Center (NCUTC):** The national schoolhouse operated by the Federal Bureau of Investigation, designated as the national training center for purposes of 6 U.S.C. 124n and the sole certifying authority for SLTT C-UAS operators.
- **Observer**: The individual trained to maintain the line-of-sight and 360-degree hazard awareness around the UAS at all times and assist the PIC in carrying out all duties required for the safe operation of the UAS.
- **Pattern data:** A derived data product reflecting aggregated trends, frequencies, or statistical observations of UAS activity across multiple operations that has met the anonymization standards in the agency's policy and contains no information identifying any specific aircraft, operator, or natural person.
- **Personnel:** Officers and employees of the agency with assigned duties that include the security or protection of people, facilities, or assets. The term does not include contractors.
- **Pilot in Command (PIC):** The individual responsible for the overall flight operations of a specific mission. The PIC is the person in control of the UAS during flight.
- **Pre-Flight Briefing**: A discussion led by the PIC prior to aircraft launch which will include but not be limited to:
  - Review of mission goals and methods to achieve goals, including handoff procedures.
  - Review of current and forecasted weather conditions and weather limitations on mission;

- Identification of mission limitations and safety issues such as battery charge, GPS strength, and potential for radio interference;
- Review of proposed flight area, including maximum ceiling and floor;
- Review of emergency/contingency procedures; and
- Review of required video or digital images.

Public UAS: An unmanned aircraft in which operations are limited to federal, state, local agencies.

Raw sensor data: Unprocessed or minimally processed data generated by C-UAS systems, including radio frequency captures, radar returns, optical and infrared imagery, acoustic signatures, full sensor logs, and telemetry.

RF-emitting C-UAS system: Any C-UAS system that, when employed for detection or mitigation, actively transmits radio frequency energy. This includes detection-only systems such as transmitting radars that may require a Federal Communications Commission radiolocation license, and mitigation systems that jam or manipulate control signals.

Unmanned Aircraft: An aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.

Unmanned Aircraft System: An unmanned aircraft and associated elements, including, but not limited to, any communication links and components that control the unmanned aircraft.

UAS Program Manager: The individual responsible for reviewing and approving the use of the UAS in a law enforcement mission. The UAS Program Manager has full oversight responsibility of all logistical and administrative elements of UAS operations

7. CANCELLATIONS

APD.SOP.4045 – Effective May 19, 2020

8. REFERENCES

- OCGA § 6-1-4 Unmanned Aircraft Systems
- 6 U.S.C. 124n (as amended by the SAFER SKIES Act).
- 6 CFR part 124; 28 CFR part 124 (the SAFER SKIES interim final rule).
- 14 CFR part 107 (remote pilot certification).
- Title III of the Communications Act of 1934, as amended.
- Authorized Technologies List and Authorized Systems List (federal interagency).

9. ADOPTION, LEGAL REVIEW, AND ATTESTATION

This policy takes effect on adoption by the City of Atlanta Police Department and remains in effect until superseded. It is reviewed and renewed annually, and the portal attestation is renewed annually. (§ 124.6(b), (d).)

Chief Darin Schierbaum
Agency Head

Date: Signed Electronically on August 11th, 2026

_____
Legal Counsel Concurrence
[Counsel name, title] — reviewed for compliance with part 124, including the privacy and civil liberties, data retention, minimization, and dissemination provisions, and the interplay with applicable state, local, Tribal, or territorial law.

Date: _____