UNMANNED AIRCRAFT SYSTEMS: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that UAS does not use artificial intelligence and machine learning.	Public comment highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon UAS capabilities.	Added language regarding how UAS compliment other NYPD technologies.
Expanded upon UAS rules of use.	Added language clarifying UAS rules of use. Added language clarifying UAS use-authorization.
Expanded upon UAS safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to UAS when job duties no longer require access.
Expanded upon UAS data retention.	Added language to reflect NYPD obligations under Federal, State and local record retention laws.
Expanded upon UAS external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Minor grammar changes.	Minor syntax edits were made.

ABSTRACT

Unmanned aircraft systems (UAS), commonly referred to as "drones," are used by the New York City Police Department (NYPD) are used to conduct search and rescue missions, disaster response, documentation of traffic collision and crime scenes, crowd monitoring and provide a bird's eye view in dangerous active shooter and hostage situations. UAS help NYPD personnel gather crucial information as situations unfold without putting officers, civilian bystanders and other involved parties at risk.

The NYPD produced this impact and use policy because NYPD UAS are capable of collecting video, thermal and location information, and sharing that information with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

NYPD UAS are composed of aircraft without a human pilot onboard. The devices are controlled remotely by a NYPD operator through the use of a transmitter. UAS used by the NYPD vary in size. They are weather-resistant, and are equipped with multi-zoom cameras and thermal imaging capabilities.

UAS generally serve as a non-invasive compliment to other law enforcement and security measures employed by the NYPD. At large-scale events, UAS provide an expansive aerial view of a large area and can inform personnel deployments regarding congestion at these sites at a fraction of the cost and resources of other equipment.

UAS assist NYPD personnel conducting search and rescue operations; document collisions and crimes scenes; search for evidence at large or inaccessible scenes and hazardous material incidents; monitor of vehicular traffic and pedestrian congestion at large events; and provide visual assistance at hostage/barricaded suspect situations and at rooftop security situations during shooting incidents.

NYPD UAS do not use video analytics or biometric measuring technologies beyond the processing of thermal data. NYPD UAS do not use facial recognition technologies and cannot conduct facial recognition analysis. However, a still image can be created from the recorded video images and may be used as a probe image for facial recognition analysis.[1]

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

The NYPD's UAS policy seeks to balance the public safety benefits of this technology with individual privacy. UAS must be used in a manner that is consistent with the requirements and protection of the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

NYPD policy directs that UAS may be used for the following purposes: search and rescue operations, documentation of collisions and crimes scenes, evidence searches at large inaccessible scenes, hazardous material incidents, monitoring vehicular traffic and pedestrian congestion at large scale events, visual assistance at hostage/barricaded suspect situations, rooftop security

[1] For additional information on facial recognition, please refer to the facial recognition impact and use policy.

observations at shooting or large scale events, public safety, emergency, and other situations with the approval of the Chief of Department.

UAS cannot be used for routine foot patrol by officers; traffic enforcement or immobilizing a vehicle or suspect.

In situations where deployment of NYPD UAS has not been foreseen or prescribed in policy, the highest uniformed member of the NYPD, the Chief of Department, will decide if deployment is appropriate and lawful. In accordance with the Public Oversight of Surveillance Technology Act, an addendum to this impact and use policy will be prepared as necessary to describe any additional uses of UAS.

When UAS are used to conduct aerial surveillance of areas exposed to public observation, court authorization is not required prior to their use. Absent exigent circumstances, a UAS will not be used in areas where there is a reasonable expectation of privacy without NYPD personnel first obtaining a search warrant that explicitly authorizes the use of a UAS. After a search warrant is issued, a UAS may be used for a pre-warrant execution safety survey. The warrant will be obtained with the assistance of the prosecutor with jurisdiction over the matter.

NYPD investigations involving political activity are conducted by the Intelligence Bureau, which is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the *Handschu* Consent Decree.

No person will be the subject of police action solely because of actual or perceived race, color, religion or creed, age, national origin, alienage, citizenship status, gender (including gender identity), sexual orientation, disability, marital status, partnership status, military status, or political affiliation or beliefs.

The misuse of UAS will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

NYPD UAS may only be used and operated by members assigned to the Technical Assistance Response Unit (TARU). Operation of UAS must follow the guidelines of Title 14 of the Code of Federal Regulations, Part 107, and/or the Certificate of Authorization (COA) issued to the Department by the Federal Aviation Administration (FAA), as well as all other applicable FAA regulations and federal, state, and local laws. Each member of TARU that operates a UAS has obtained their remote pilot certificate from the FAA and has passed the FAA's "Aeronautical Knowledge Test." If use is to take place outside of the NYPD's COA, TARU personnel are instructed to contact FAA and seek a Special Government Interest COA prior to deployment.

The decision of whether to deploy NYPD UAS must be made by an NYPD executive serving as a commanding officer, executive officer, or daily duty captain. Such member must request the UAS from TARU. TARU personnel will then assess whether such use comports with NYPD policy and evaluate weather conditions, airspace restrictions, and safety in determining the appropriateness of use. If there is disagreement concerning the permissible use of a NYPD UAS, conferral with a

TARU supervisor will occur. If such disagreement cannot be resolved, the daily duty chief will make the final determination.

When appropriate, TARU personnel make notifications to the NYPD Aviation Unit and Operations Unit of the time, location, and flight path prior to use of UAS in order to avoid any airspace conflict with other aircraft operating in the area. Radio dispatch must also be notified to alert responding NYPD members of a NYPD UAS in the area. TARU is to maintain a log of each UAS flight by date, time, location, purpose, flight time, pilot name, and authorizing member.

UAS are securely stored in NYPD facilities when not in use, in a location that is inaccessible to the public. Additionally, a supervisor must periodically inspect and account for the devices. Access to UAS is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to NYPD UAS is removed when access is no longer necessary for NYPD personnel to fulfill their duties (e.g., when personnel are transferred to a command that does not use the technology).

NYPD UAS transmit video images to NYPD personnel reviewing the transmission on a remote monitor through an encrypted signal on a closed, stand-alone network. Data is encrypted both at rest on the device and in transit. The signal can only be decrypted by vendor-provided proprietary software.

Recordings obtained from UAS are retained within a NYPD computer or case management system. Only authorized users have access to these recordings. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. The NYPD maintains an enterprise architecture (EA) program, which includes an architecture review process to determine system and security requirements on a case by case basis. System security is one of many pillars incorporated into the EA process. Additionally, all NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory (AD) authentication. Passwords are never stored locally; user authentication is stored within the AD. The AD is managed by a Lightweight Directory Access Protocol (LDAP) to restrict/allow port access. Accessing NYPD computer systems remotely requires dual factor authentication. All data within NYPD computer systems are encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with computer and case management systems of the NYPD, including those governing user passwords and logon procedures. NYPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose

information to others, including other members of the NYPD, only as required in the execution of lawful duty.

NYPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

POLICIES & PROCEDURES RELATING TO RETENTION, ACCESS & USE OF THE DATA

Information obtained from UAS use will be retained for thirty (30) days by TARU. The NYPD's Legal Bureau may extend the retention period if the images are needed for civil litigation, subpoena production, Freedom of Information Law requests or other legal processes.

TARU personnel distribute recorded information to the NYPD personnel responsible for investigating the matter where the UAS was utilized. The NYPD investigator will store this information in an NYPD computer or case management system.

Recordings may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings. Recordings will be stored in an appropriate NYPD computer or case management system. NYPD personnel utilizing case management and computer systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty.

The Retention and Disposition Schedule for New York Local Government Records (the Schedule) establishes the minimum length of time local government agencies must retain their records before the records may be legally disposed.[2] Published annually by the New York State Archives, the Schedule ensures compliance with State and Federal record retention requirements. The NYC Department of Records and Information Services (DORIS) publishes a supplemental records retention and disposition schedule (the Supplemental Schedule) in conjunction with the Law Department specifically for NYC agencies in order to satisfy business, legal, audit and legal requirements.[3]

The retention period of a "case investigation record" depends on the classification of a case investigation record. The classification of case investigation records is based on the final disposition of the case, i.e., what the arrestee is convicted of or pleads to. Further, case

[2] *See* N.Y. Arts & Cult. Aff. Law § 57.19 - 25, *and* 8 NYCRR Part 185.
[3] *See* NYC Charter 3003.

investigations are not considered closed unless it results in prosecution and appeals are exhausted, it results in a settlement, it results in no arrest, or when restitution is no longer sought.

Case investigation records classified as a homicide, suicide, arson (first, second or third degree), missing person (until located), aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), active warrant, or stolen or missing firearms (until recovered or destroyed), must be retained permanently. Case investigation records classified as a fourth degree arson or non-fatal (including vehicular accidents) must be retained for a minimum of ten (10) years after the case is closed. Case investigation records classified as any other felony must be retained for a minimum of twenty-five (25) years after the case is closed. Case investigation records classified as a misdemeanor must be retained for a minimum of five (5) years after the case is closed. Case investigation records classified as a violation or traffic infraction must be retained for a minimum of one (1) year after the case is closed. Case investigation records classified as an offense against a child as defined by the Child Victims Act, excluding aggravated sexual assault (first degree), course of sexual conduct against a child (first degree), must be retained until the child attains at least age fifty-five (55). Case investigation records connected to an investigation that reveals no offense has been committed by an adult must be kept for a minimum of five (5) years after the case is closed. Case investigation records connected to an investigation that reveals the individual involved was a juvenile and no arrest was made or no offense was committed must be kept for at least one (1) year after the juvenile attains age eighteen (18).

Personal information data files on criminals and suspects must be retained for at least five (5) years after the death of the criminal or suspect, or ninety (90) years after the criminal or suspect's date of birth as long as there has been no arrest in the last five (5) years, whichever is shorter. Personal information data files on associated persons, such as victims, relatives and witnesses must be retained as long as, or information as part of relevant case investigation record.

The misuse of any recording will subject employees to administrative and potentially criminal penalties.

POLICIES & PROCEDURES RELATING TO PUBLIC ACCESS OR USE OF THE DATA

Members of the public may request recordings obtained from NYPD use of UAS pursuant to the New York State Freedom of Information Law. The NYPD will review and evaluate such requests in accordance with applicable provisions of law and Department policy. Additionally, the NYPD voluntary discloses information related to UAS use on a quarterly basis on its website: (https://www1.nyc.gov/site/nypd/stats/reports-analysis/uas-drones.page).

EXTERNAL ENTITIES

If a UAS obtains data related to a criminal case, the NYPD will turn it over to the prosecutor with jurisdiction over the matter. The prosecutor will provide the data to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request information obtained by UAS from the NYPD. Such disclosure by the NYPD is governed by applicable laws and regulations, and NYPD policies. Additionally, the NYPD may provide the information to partnering law enforcement and city

agencies pursuant to on-going criminal investigations, civil litigation and disciplinary proceedings. Information is not shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, the recording or information related to it may be provided to community leaders, civic organizations and the news media in order to further an investigation, create awareness of an unusual incident, or address a community-concern.

Pursuant to NYPD policy and local law, NYPD personnel may disclose identifying information externally only if:

1. Such disclosure has been authorized in writing by the individual to whom such information pertains to, or if such individual is a minor or is otherwise not legally competent, by such individual's parent or legal guardian and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
2. Such disclosure is required by law and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
3. Such disclosure furthers the purpose or mission of the NYPD and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
4. Such disclosure has been pre-approved as in the best interests of the City by the City Chief Privacy Officer;
5. Such disclosure has been designated as routine by the Agency Privacy Officer assigned to the Legal Bureau;
6. Such disclosure is in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime;
7. Such disclosure is in connection with an open investigation by a City agency concerning the welfare of a minor or an individual who is otherwise not legally competent.

Government agencies at the local, state, and federal level, including law enforcement agencies other than the NYPD, have limited access to NYPD computer and case management systems. Such access is granted by the NYPD on a case by case basis subject to the terms of written agreements between the NYPD and the agency receiving access to a specified system. The terms of the written agreements also charge these external entities with maintaining the security and confidentiality of information obtained from the NYPD, limiting disclosure of that information without NYPD approval, and notifying the NYPD when the external entity receives a request for that information pursuant to a subpoena, judicial order, or other legal process. Access will not be given to other agencies for purposes of furthering immigration enforcement.

The NYPD purchases UAS and associated equipment or Software as a Service (SaaS)/software from approved vendors. The NYPD emphasizes the importance of and engages with vendors and contractors to maintain the confidentiality, availability, and integrity of NYPD technology systems.

Vendors and contractors may have access to NYPD UAS associated software or data in the performance of contractual duties to the NYPD. Such duties are typically technical or proprietary in nature (e.g., maintenance or failure mitigation). In providing vendors and contractors access to

equipment and computer systems, the NYPD follows the principle of least privilege. Vendors and contractors are only allowed access on a "need to know basis" to fulfill contractual obligations and/or agreements.

Vendors and contractors providing equipment and services to the NYPD undergo vendor responsibility determination and integrity reviews. Vendors and contractors providing sensitive equipment and services to the NYPD also undergo background checks.

Vendors and contractors are legally obligated by contracts and/or agreements to maintain the confidentiality of NYPD data and information. Vendors and contractors are subject to criminal and civil penalties for unauthorized use or disclosure of NYPD data or information.

If recordings obtained using NYPD UAS are disclosed in a manner violating the local Identifying Information Law, the NYPD Agency Privacy Officer, upon becoming aware, must report the disclosure to the NYC Chief Privacy Officer as soon as practicable. The NYPD must make reasonable efforts to notify individuals effected by the disclosure in writing when there is potential risk of harm to the individual, when the NYPD determines in consultation with the NYC Chief Privacy Officer and the Law Department that notification should occur, or when legally required to do so by law or regulation. In accordance with the Identifying Information Law, the NYC Chief Privacy Officer submits a quarterly report containing an anonymized compilation or summary of such disclosures by City agencies, including those reported by the NYPD, to the Speaker of the Council and makes the report publically available online.

TRAINING

TARU personnel must obtain their FAA remote pilot certificate from the FAA and pass the FAA's "Aeronautical Knowledge Test" in order to operate a NYPD UAS. The exam covers the following topics: FAA regulations, airspace classifications and requirements, meteorology, emergency operations, aeronautical decision-making, flight inspections, airport operations, and others. Certification is valid for two years, and certificate holders must pass a recurrent knowledge test every two years.

Additionally, the NYPD engages in in-service training which encompasses further understanding of FAA regulations as well as practice flights and simulations. NYPD personnel must operate UAS in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The request for use of NYPD UAS may only come from an NYPD uniformed executive serving as a commanding officer, executive officer, or daily duty captain. Prior to use, TARU personnel supervisors will also assess whether such use comports with NYPD policy and evaluate weather conditions, airspace restrictions, and safety in determining the appropriateness of deployment. If there is disagreement concerning the permissible use of a NYPD UAS, conferral with a TARU supervisor will occur. If such disagreement cannot be resolved, the daily duty chief will make the final determination.

TARU must maintain a log of each UAS flight by date, time, location, purpose, flight time, pilot name, and authorizing member. TARU supervisors are responsible for the security and proper

utilization of UAS equipment. The Commanding Officer of TARU also directly reports to the Chief of Department, the highest ranking uniformed member of the NYPD.

All NYPD personnel are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. The misuse of any system or equipment will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by the Internal Affairs Bureau (IAB).

Supervisors of personnel utilizing NYPD computer and case management systems are responsible for security and property utilization of the technology and associated equipment. Supervisors are directed to inspect all areas containing NYPD computer systems at least once each tour and ensure that all systems are being used within NYPD guidelines.

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all information in the possession of the NYPD. ICOs must ensure all authorized users of NYPD computer systems in their command understand and comply with computer security guidelines, frequently observe all areas with computer equipment, and ensure security guidelines are complied with, as well as investigating any circumstances or conditions which may indicate abuse of the computer systems.

Requests for focused audits of computer activity from IAB, Commanding Officers, ICOs, Investigations Units, and others, may be made to the Information Technology Bureau.

HEALTH & SAFETY REPORTING

There are no known health and safety issues with UAS operated by the NYPD or its associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for NYPD UAS mitigate the risk of impartial and biased law enforcement. NYPD UAS do not facial recognition software and cannot conduct facial recognition analysis. Other than the processing of thermal data, NYPD UAS do not contain biometric measuring capabilities.

The NYPD is committed to the impartial enforcement of the law and to the protection of constitutional rights. The NYPD prohibits the use of racial and bias-based profiling in law enforcement actions, which must be based on standards required by the Fourth and Fourteenth Amendments of the U.S. Constitution, Sections 11 and 12 of Article I of the New York State Constitution, Section 14-151 of the New York City Administrative Code, and other applicable laws.

Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action. Should an officer initiates enforcement action against a person, motivated even in part by a person's actual or perceived race, color, ethnicity, or national origin, that enforcement action violates NYPD policy unless the officer's decision is based on a specific and reliable suspect description that includes not only race, age, and gender, but other identifying characteristics or information.