MANNED AIRCRAFT SYSTEMS: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that manned aircraft systems do not use artificial intelligence, machine learning.	Public comment highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon manned aircraft systems capabilities language.	Added language regarding how manned aircraft systems compliment other NYPD technologies.
Expanded upon manned aircraft systems court authorization language.	Added language clarifying that use of manned aircraft systems for aerial surveillance is limited to areas openly available to the public.
Expanded upon manned aircraft systems safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to manned aircraft systems when job duties no longer require access.
Expanded upon manned aircraft systems data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon manned aircraft systems external entities section.	Added language to reflect NYPD obligations under local privacy laws.
Minor grammar changes.	Minor syntax edits were made.

ABSTRACT

Manned aircraft systems enable the New York City Police Department ("NYPD") to conduct air-and-sea rescues, and provide incomparable aerial tactical support to police officers on the ground. The use of manned aircraft systems is subject to privacy, confidentiality, and dissemination restrictions according to NYPD policy and Federal Aviation Administration ("FAA") rules and regulations, as well as applicable federal, state, and local laws and rules.

The NYPD produced this impact and use policy because manned aircraft systems are capable of processing and recording video images, thermal measurements and location data, and sharing it with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

The manned aircraft systems used by the NYPD consist of helicopters and fixed wing aircraft. Manned aircraft systems aid the NYPD with the air-and-sea rescue missions and provide investigative and tactical support to police officers on the ground, including: conducting fast rope deployments, fire suppression, maritime security operations, high-rise and roof-top insertions, hoist operations, air ambulance service and water searches and rescues.

Manned aircraft systems are equipped with video, radar and temperature and location sensor technologies to support operational capabilities. Infrared thermal imaging cameras equipped to NYPD manned aircraft systems measure temperature by capturing different levels of infrared light omitted from all people and objects. The cameras provide an enhanced picture of incident scenes by layering heat signatures of individuals and objects on top of the aerial video simultaneously being recorded. Thermal imaging cameras equipped to NYPD manned aircraft systems cannot detect temperature data through solid objects.

The video recording devices equipped to NYPD manned aircraft systems intake video images and stores the video locally within the manned aircraft, and simultaneously transmits the video to the Lower Manhattan Security Initiative (LMSI).

Video recording devices equipped to NYPD manned aircraft systems do not use facial recognition technologies and cannot conduct a facial recognition analysis. However, a still image can be created from the video images and may be used a probe image for facial recognition analysis.[1] Other than the processing of the infrared light emitted by a person or object, the devices do not contain any other biometric measuring capabilities.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD manned aircraft system policy seeks to balance the public safety benefits of this technology with individual privacy. Manned aircraft systems must be used in a manner consistent with the requirements and protection of the Constitution of the United States, the New York State Constitution and applicable statutory authorities.

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

Assistance from NYPD manned aircraft systems may be requested by NYPD personnel, as well as local, state, or federal authorities. In non-urgent cases, requests for manned aircraft system support are made by contacting the Special Operations Division. In urgent cases, the request may be made directly to the Chief of Special Operations. Requests for support from NYPD manned aircraft systems by other agencies must be approved by the Office of Chief of Department.

Manned aircraft systems are not to be utilized for private assistance unless authorized by the Chief of Special Operations; for example, the rescue of injured persons on publically accessible, but privately owned nature trails. Any situation which is determined to be a serious police emergency has priority over other planned utilizations. Any flight in progress is reassigned to any life threatening emergency. Final determinations for the flights are made by the Commanding Officer of the Aviation Unit based on performance and safety factors.

The NYPD does not seek court authorization prior to the use of manned aircraft systems. When NYPD manned aircraft systems are used to conduct aerial surveillance, only of areas exposed to public observation are observed.

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 manned aircraft systems.

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 manned aircraft systems will subject employees to administrative and potentially criminal penalties.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

NYPD manned aircraft systems are securely stored at NYPD and City/State facilities when not in use, in locations that are inaccessible to the general public. Additionally, a supervisor must periodically inspect and account for all manned aircraft. Access to NYPD manned aircraft systems is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to manned aircraft systems is removed when the technology 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 manned aircraft system video is transmitted to LMSI over a secured stand-alone network. The transmission is encrypted both at rest on the device and in transit. Access to the transmission is limited to LMSI personnel.

Manned aircraft system recordings are stored within an appropriate NYPD computer or case management system. Only authorized users have access to the retained data. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to computer and case management 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. Access levels are only granted for functions and abilities relevant to individual commands. 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

NYPD manned aircraft system video is saved locally to the aircraft. The video data is overwritten on what is known as a “first-in-first-out” basis. The period of retention of the recorded video is dependent on restrictions based on local storage capacity.

In addition to local retention, video processed by NYPD manned aircraft systems is transmitted to LMSI. Only NYPD personnel assigned to LMSI are capable of retaining video transmitted by NYPD manned aircraft systems. Unless there is a request to retain and/or copy video obtained through the use of manned aircraft systems, the video is retained by LMSI for thirty (30) days before it is permanently deleted from the servers.

Retained 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 are 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 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

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

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 manned aircraft systems 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 NYPD policy.

EXTERNAL ENTITIES

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

Other law enforcement agencies may request recordings contained in NYPD computer or case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide the recording, or information related to it, 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, members of the NYPD 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 manned aircraft systems 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 manned aircraft systems 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 manned aircraft systems 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

In order to operate a NYPD manned aircraft system, NYPD personnel must be a member in good standing of the NYPD Aviation Unit. Officers must maintain a valid pilots license and successfully complete the NYPD's specialized training course for Tactical Flight Officers. Training on the operation of the various components of the NYPD manned aircraft system is provided through classroom instruction as well as practical training while in flight.

NYPD personnel must operate manned aircraft systems in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Only members of the NYPD Special Operations Division may use or operate manned aircraft systems. All requests for assistance from NYPD manned aircraft systems must be submitted and reviewed by the Special Operations Division.

Supervisors of personnel utilizing manned aircraft systems and computer systems are responsible for security and proper utilization of the technologies and associated equipment. The Integrity Control Officer (ICO) of the NYPD Aviation Unit periodically reviews video recorded by NYPD manned aircraft systems in order to ensure the technologies are being used as intended.

Supervisors of personnel using manned aircraft systems are responsible for security and proper 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.

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 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).

ICOs within each Command are responsible for maintaining the security and integrity of all recorded media 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

NYPD manned aircraft comply with all applicable FAA safety standards.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols described in the impact and use policy for NYPD manned aircraft systems mitigate the risk of impartial and biased law enforcement. Manned aircraft systems do not use video analytics or any other biometric measurement technologies beyond equipped thermal imaging imbedded into video, radar, temperature, and location sensor technologies.

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. When an officer's decision to initiate enforcement action against a person is 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 just race, age, and gender, but other identifying characteristics or information.