Public Security Privacy Guidelines

I. Background

In order to help ensure public safety and security and to detect, deter, and prevent potential terrorist activities, the New York City Police Department (NYPD) has developed a networked Domain Awareness System. The Domain Awareness System not only supplies critical supplemental assistance to officers' ongoing security and public safety efforts, but also enhances the collaborative nature of those efforts by leveraging the resources of the private sector and other City agencies. Given the ongoing threat of terrorist attack, the Domain Awareness System is an important part of the NYPD's integrated approach to providing protection for those who work in, live in, and visit New York City.

The *Public Security Privacy Guidelines* (the *Guidelines*) establish policies and procedures to limit the authorized use of the Domain Awareness System and to provide for limited access to and proper disposition of stored data. To ensure that appropriate privacy protections exist, the NYPD has considered and consciously incorporated technical, operational, legal, policy, and oversight safeguards throughout the development life cycle of the Domain Awareness System.

II. Legal Authority

The NYPD created the Domain Awareness System under the authority provided by Chapter 18, §435(a) of the New York City Charter, which gives the NYPD plenary power to:

> …preserve the public peace, prevent crime, detect and arrest offenders, suppress riots, mobs and insurrections, disperse unlawful or dangerous assemblages…protect the rights of persons and property, guard the public health, preserve order…
>
> …regulate, direct, control and restrict the movement of vehicular and pedestrian traffic for the facilitation of traffic and convenience of the public as well as the proper protection of human life and health…inspect and observe all places of public amusement, all places of business…enforce and prevent the violation of all laws and ordinances in force in the city; and for these purposes to arrest all persons guilty of violating any law or ordinance for the suppression or punishment of crimes or offenses.

III. Policy

A. Definitions

Archival Data: data types and/or specific data instances collected by the Domain Awareness System which have been approved by the Authorized Agent, or a designee

approved in writing by the Authorized Agent, for further retention beyond the Pre-Archival Period.

Authorized Agent: the designated NYPD official whose approval is required before certain actions may be taken.

Domain Awareness System: technology deployed in public spaces as part of the counterterrorism program of the NYPD's Counterterrorism Bureau, including: NYPD-owned and Stakeholder-owned closed circuit television cameras (CCTVs) providing feeds into the Lower Manhattan Security Coordination Center; License Plate Readers (LPRs); and other domain awareness devices, as appropriate.

Environmental Data: environmental data collected by devices designed to detect hazards related to potential terrorist threats, or to respond to terrorist attacks.

License Plate Reader (LPR) Data: license plate data collected by fixed or mobile LPR devices that are part of the Domain Awareness System.

Metadata: information about data collected by the Domain Awareness System that increases the usefulness of that data.

Pre-Archival Data: data types and/or specific data instances collected by the Domain Awareness System that are destroyed as a matter of course after the Pre-Archival Period, unless approved by the Authorized Agent, or a designee approved in writing by the Authorized Agent, for further retention.

Pre-Archival Period: the data retention period designated for routine review.

Stakeholders: companies and other government agencies that have partnered with the NYPD via memorandum of understanding, some of whom have agreed to provide feeds from their proprietary CCTVs into the Lower Manhattan Security Coordination Center.

Stakeholder Representative: a non-NYPD person affiliated with a Stakeholder who is granted access to the Lower Manhattan Security Coordination Center based on his/her specific knowledge of the Stakeholder's premises and duties in connection with maintaining the safety and security thereof.

Video: data collected from CCTVs that are part of the Domain Awareness System.

B. Statement of Purpose

The Domain Awareness System is a counterterrorism tool designed to:

- Facilitate the observation of pre-operational activity by terrorist organizations or their agents
- Aid in the detection of preparations to conduct terrorist attacks

- Deter terrorist attacks
- Provide a degree of common domain awareness for all Stakeholders
- Reduce incident response times
- Create a common technological infrastructure to support the integration of new security technology

C. Operation

The Domain Awareness System will be operated 24 hours a day, seven days a week, in a professional manner and only in furtherance of legitimate law enforcement and public safety purposes.

As with all NYPD operations, no person will be targeted or monitored by the Domain Awareness System 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 Domain Awareness System will be used only to monitor public areas and public activities where no legally protected reasonable expectation of privacy exists.

Facial recognition technology is not utilized by the Domain Awareness System.

All NYPD-owned CCTVs that are part of the Domain Awareness System will have accompanying signage, and the NYPD will recommend that signage accompany each Stakeholder-owned CCTV that is part of the Domain Awareness System.

In certain cases, technologies governed by the *Guidelines* may utilize or be integrated with systems and technologies deployed by other bureaus and divisions of the NYPD. In such cases, the application of the *Guidelines* will be controlled by separate memorandum from the Deputy Commissioner of Counterterrorism to the Deputy Commissioner for Legal Matters.

D. Data Storage

Generally, data gathered through the use of the Domain Awareness System will be destroyed as a matter of course at the end of the relevant Pre-Archival Period; any decision to retain certain data possessing evidentiary or other value beyond the Pre-Archival Period must be approved and documented in writing by the Authorized Agent, or a designee approved in writing by the Authorized Agent.

- **Video**:
  - → The Pre-Archival Period for Video is 30 days. For any decision to retain Video beyond the Pre-Archival Period, the Authorized Agent is the

Deputy Commissioner of Counterterrorism. All Video from CCTVs will be recorded.

- **Metadata**:
  - → The Pre-Archival Period for Metadata is five years. For any decision to retain Metadata beyond the Pre-Archival Period, the Authorized Agent is the Deputy Commissioner for Legal Matters.
- **LPR Data**:
  - → The Pre-Archival Period for LPR Data is five years. For any decision to retain LPR Data beyond the Pre-Archival Period, the Authorized Agent is the Deputy Commissioner for Legal Matters.
- **Environmental Data**:
  - → Environmental Data will be retained indefinitely.

After the conclusion of five years, Archival Data must be reviewed by the Deputy Commissioner of Counterterrorism and the Deputy Commissioner for Legal Matters for continuing law enforcement or public safety value or legal necessity; all Archival Data determined not to have continuing law enforcement or public safety value or legal necessity will be destroyed as a matter of course.

E. Data Usage

Data from the Domain Awareness System may be used in furtherance of the purposes set out in the Statement of Purpose (III.B).

In limited circumstances, data from the Domain Awareness System may also be used in furtherance of legitimate law enforcement and public safety purposes beyond the scope of those purposes set out in the Statement of Purpose (III.B). Such use is subject to certain restrictions:

- **Incidental Use**: occurs when data from the Domain Awareness System is used in furtherance of a purpose set out in the Statement of Purpose (III.B), and the user incidentally notices something useful for a legitimate law enforcement or public safety purpose beyond the scope of those purposes set out in the Statement of Purpose (III.B).
  - → For Incidental Use, no additional approval is required.
- **Secondary Use**: occurs when data from the Domain Awareness System, with the exception of LPR Data, is intentionally used for a legitimate law enforcement or public safety purpose beyond the scope of those purposes set out in the Statement of Purpose (III.B). Any decision to make Secondary Use of data from the Domain Awareness System must be approved and documented in writing by the Authorized Agent, or a designee approved in writing by the Authorized Agent. Any individual seeking to make Secondary Use of data from the Domain

Awareness System must have a reason to believe that the data will further a law enforcement or public safety purpose.

→ For Secondary Use of Pre-Archival Data, the Authorized Agent is the Deputy Commissioner of Counterterrorism.

→ For Secondary Use of Archival Data, generally the Authorized Agent is the Deputy Commissioner for Legal Matters; however, when the data to be Secondarily Used is to be accessed in furtherance of the purpose for which that data was retained beyond the Pre-Archival Period, the Authorized Agent is the Deputy Commissioner of Counterterrorism.

F. Data Sharing

It is the policy of the NYPD to place limits on the sharing of data with third parties.

Video, Metadata, LPR Data, or Environmental Data may only be used for law enforcement or public safety purposes; except as required by law, subpoena, or other court process, such data will not be otherwise disclosed by the NYPD.

Unless otherwise provided for in a memorandum of understanding between the NYPD and a third party, any decision to share Video, Metadata, LPR Data, or Environmental Data with third parties, beyond Stakeholder Representatives, must be approved and documented in writing by the Authorized Agent, or a designee approved in writing by the Authorized Agent.

- **Video:**
  - → For Video requested by a third party to be used in furtherance of a purpose consistent with those purposes set out in the Statement of Purpose (III.B), the Authorized Agent is the Deputy Commissioner of Counterterrorism.
  - → For Video requested by a third party to be used in furtherance of a purpose beyond the scope of those purposes set out in the Statement of Purpose (III.B), the Authorized Agent is the Deputy Commissioner for Legal Matters.
- **Metadata:**
  - → For all Metadata requested by a third party, the Authorized Agent is the Deputy Commissioner for Legal Matters.
- **LPR Data:**
  - → For LPR Data requested by another government entity or Stakeholder to be used in furtherance of a purpose consistent with those set out in the Statement of Purpose (III.B), the Authorized Agent is the Deputy Commissioner of Counterterrorism.
  - → For LPR Data requested by any other third party, or for LPR Data requested by another government entity or Stakeholder to be used in furtherance of a purpose beyond the scope of those purposes set out in the

Statement of Purpose (III.B), the Authorized Agent is the Deputy Commissioner for Legal Matters.

- **Environmental Data**
  - → For Environmental Data requested by another government entity or Stakeholder to be used in furtherance of a purpose consistent with those set out in the Statement of Purpose (III.B), the Authorized Agent is the Deputy Commissioner of Counterterrorism.
  - → For Environmental Data requested by any other third party, or for Environmental Data requested by another government entity or Stakeholder to be used in furtherance of a purpose beyond the scope of those purposes set out in the Statement of Purpose (III.B), the Authorized Agent is the Deputy Commissioner for Legal Matters.

G. Safeguarding and Protecting Stored Data

The NYPD will take all appropriate technological, physical, administrative, procedural, and personnel measures to protect the confidentiality and integrity of all sensitive data, whether in transit or in storage.

Accordingly, the NYPD will observe the following safeguards regarding access to and use of data:

- Physical access to the Lower Manhattan Security Coordination Center is limited to NYPD personnel, authorized invited guests, and Stakeholder Representatives. Physical security protections include: guards who will keep access logs and locked facilities requiring badges or access cards for entry.
- Prior to accessing the Domain Awareness System database, all Stakeholder Representatives must be authorized, and all non-sworn law enforcement Stakeholder Representatives must be screened. All authorized Stakeholder Representatives will be briefed on the *Public Security Privacy Guidelines* and will be required to sign both a confidentiality agreement, which strictly limits the purposes for which accessed data may be used and imposes sanctions for any violation, and an agreement promising to adhere to the *Guidelines*.
- Direct access to the Domain Awareness System database is limited to authorized NYPD personnel and Stakeholder Representatives; administrative rules governing which operators may use various system capabilities will create a differentiated access system. As part of the differentiated access system, Stakeholder Representatives will not have access to NYPD-generated data that includes personally identifiable information, except as specified by the Deputy Commissioner of Counterterrorism or a designee approved in writing by the Deputy Commissioner of Counterterrorism.
- All Stakeholder Representatives and NYPD personnel with access to the Domain Awareness System and the Domain Awareness System database will complete

privacy training, based, in part, upon a curriculum covering the proper use and handling of such information, with periodic assessments.

- The Domain Awareness System will employ data security technologies to protect the integrity of its data from hacking and other risks.
- Digital watermarking or an equivalent technique will be used to create an immutable audit log of where and when data is accessed.

H. Accountability

Any violation of these *Guidelines* will result in appropriate disciplinary action.

A Counterterrorism Bureau Integrity Control Officer (ICO) is tasked with conducting periodic reviews of audit logs to ensure full compliance with these *Guidelines*.

Nothing in these *Guidelines* is intended to create any private rights, privileges, benefits or causes of action in law or equity. Rather, these *Guidelines* are designed to ensure that the Domain Awareness System is properly used based on legally appropriate and relevant law enforcement and public safety considerations and information.