DOMAIN AWARENESS SYSTEM: IMPACT AND USE POLICY

APRIL 11, 2021

SUMMARY OF CHANGES BETWEEN DRAFT AND FINAL POLICY

Update	Description of Update
Removed statement that the Domain Awareness System does not use artificial intelligence and machine learning.	Public comments highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon Domain Awareness System capabilities.	Added language clarifying Domain Awareness System capabilities. Added language regarding what information is accessible using the Domain Awareness System. Added language describing how the Domain Awareness System compliments other NYPD technologies.
Expanded upon Domain Awareness System rules of use.	Added language clarifying Domain Awareness System rules of use.
Expanded upon Domain Awareness System safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to the Domain Awareness System when job duties no longer require access.
Expanded upon Domain Awareness System data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon Domain Awareness System external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

ABSTRACT

To help ensure public safety and security, and to detect, deter, and prevent potential terrorist activities, the New York City Police Department (NYPD) coordinated with Microsoft to develop a networked Domain Awareness System (DAS). Today, DAS is not only a tool aiding in the detection and prevention of terrorist attacks; it greatly enhances the quality of criminal investigations and the effectiveness of members of service. DAS allows officers to access critical information relevant to ongoing security and public safety efforts, and boosts the collaborative nature of those efforts by employing the resources of the private sector and other city agencies. DAS 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 NYPD produced this impact and use policy because DAS is capable of sharing video images, still images, location, and acoustic data with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

Originally designed as a counterterrorism platform, DAS is now a program that aggregates a substantial quantity of the information NYPD personnel use to make strategic and tactical decisions. DAS is a software that efficiently centralizes vital information that would otherwise be kept throughout different isolated data compartments within the NYPD.

DAS allows NYPD personnel to efficiently access critical information such as real-time 911 information, past history of call locations, crime complaint reports, arrest reports, summonses, NYPD arrest and warrant history, as well as a person's possible associated vehicles, addresses, persons, phone numbers, date of birth, and firearm licensure history. DAS is capable of distributing wanted posters and missing person alerts amongst NYPD personnel, increasing the potential of a timelier recovery, rescue and if appropriate, arrest.

If a person has been arrested by the NYPD, DAS can provide NYPD personnel with an arrest photo and physical description of the person. The arrest photo can be downloaded and may be used as a probe image for facial recognition analysis.[1] The NYPD Criminal Group Database[2] cannot be accessed through DAS. However, if DAS is used to search for information connected to a person included in the criminal group database, that inclusion will appear along with the name of the criminal group.

DAS provides officers with critical alerts on any issues or potential threats at queried locations. DAS allows NYPD members to access environmental data, view electronic injury and accident reports, and allows NYPD personnel to search for previously prepared domestic violence reports and police forms.

The NYPD utilizes Closed Circuit Television (CCTV[3]) cameras throughout the five (5) boroughs. DAS behaves as a centralized repository through which authorized users can access CCTV cameras. NYPD Detectives, Sergeants, and higher ranked members can use DAS to view live feed

[1] For additional information on Facial Recognition, please refer to the facial recognition impact and use policy.
[2] For additional information on the Criminal Group Database, please refer to the Criminal Group Database impact and use policy.
[3] For additional information on CCTV systems, please refer to the CCTV systems impact and use policy.

from CCTV cameras. A limited number of select NYPD personnel with the rank of police officer may be granted CCTV viewing privileges based on the nature of their assignment. DAS cannot be used to download or retain CCTV video.

License plate readers (LPRs[4]) are specialized cameras that quickly capture images of license plate numbers mounted to vehicles that pass within their range-of-view. An internal processor then converts the image of the license plate a text the computer can process. This data, along with the date and time the plates were scanned and the location of the LPR, is automatically stored within an administrative database. DAS behaves as a centralized repository through which this LPR data can be accessed. The DAS software itself is incapable of reading license plates.

ShotSpotter[5] is a gunfire or gunshot detection system. ShotSpotter captures the time, location, and audio associated with a potential gunfire incident. DAS behaves as a centralized repository through which ShotSpotter data can be accessed. The DAS software itself is incapable of detecting gunshots or gunfire.

DAS does not contain any editing features, and does not have the ability to change the accessible information. DAS does not use video analytics or any biometric measurement technologies. DAS does not use facial recognition technologies and cannot conduct facial recognition analysis. However, still images within DAS may be used as a probe image for facial recognition analysis.[6]

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD DAS policy seeks to balance the public safety benefits of this technology with individual privacy. DAS 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.

NYPD personnel may only DAS for legitimate law enforcement purposes. NYPD personnel may only access the DAS features they have been authorized to view. NYPD personnel must do so only under circumstances required in the execution of lawful duty relating to the official business of the NYPD. Access rights within DAS is limited based on lawful duty.

Court authorization is not necessary in order to use DAS. DAS is software that centralizes lawfully obtained data and information that would otherwise be kept isolated in different data compartments within the NYPD.

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 DAS.

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.

[4] For additional information on LPRs, please refer to the LPR impact and use policy.
[5] For additional information on ShotSpotter, please refer to the ShotSpotter impact and use policy.
[6] For additional information on facial recognition, please refer to the facial recognition impact and use policy.

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

SAFEGUARD & SECURITY MEASURES AGAINST AUTHORIZED ACCESS

DAS is confidential-password-protected and access is restricted to only authorized users. Authorized users consist only of NYPD personnel in various commands, whose access has been requested by their commanding officer, and approved by the Information Technology Bureau (ITB).

DAS access is limited to authorized users who are authenticated by username and password. Access to DAS is limited to NYPD personnel with an articulable need to use the software in furtherance of a lawful duty. DAS access 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).

Information contained within DAS features may be downloaded and retained in an appropriate NYPD computer or case management system. Only authorized users have access to NYPD computer and case management systems. 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 related to the official business of the NYPD. Access levels are only granted for functions and abilities relevant to individual commands.

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. Case management system access levels are adjusted or removed when the access is no longer necessary for NYPD personnel to fulfill their duties (e.g., when personnel are transferred to a command).

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

DAS efficiently centralizes vital information that would otherwise be kept throughout different isolated data compartments within NYPD computer systems. Information contained within DAS 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.

Authorized users can use DAS to download various NYPD records as complaint reports, arrest reports, Intergraph Computer Aided Dispatch (ICAD) call data, and ShotSpotter and LPR data for retention in an appropriate case management system. CCTV video cannot be downloaded by the vast majority of DAS users. To retain CCTV video, NYPD personnel must make a request for retention to the NYPD Lower Manhattan Security Initiative (LMSI). Only LMSI personnel are capable of downloading CCTV video.

Information contained within DAS 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. Relevant information is stored in an appropriate NYPD computer or case management system. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to computer and case management 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.[7] 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.[8]

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

[7] *See* N.Y. Arts & Cult. Aff. Law § 57.19 - 25, *and* 8 NYCRR Part 185.
[8] *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 information 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 information related to DAS 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

External stakeholders providing NYPD with access to their public-space facing cameras have the ability to designate one of their own employees as their stakeholder representative. Stakeholder representatives only have access to their own public-space facing CCTV camera(s). Stakeholder representatives do not have access to any of the searchable databases accessible within DAS, ShotSpotter, LPR readings, or any other technology contained within DAS.

Stakeholders and stakeholder representatives must agree to NYPD confidentiality and privacy guidelines. Stakeholders and stakeholder representatives are informed that use of NYPD computer systems beyond authorized access, or for personal or non-NYPD business matters is strictly

prohibited. Stakeholder representatives who are found in violation of this policy are notified that they will be subject to a termination of assignment.

The information accessible through DAS is often connected to a criminal investigation. Where an arrest occurs, the NYPD will turn any such relevant data over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the information to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request data accessible through DAS from the NYPD in accordance with applicable laws and regulations, and NYPD policies. Additionally, the NYPD may provide data accessible through DAS 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, information taken from DAS 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. However, unless they are an external-stakeholder, community leaders, civic organizations and members of the news media do not have direct access to any DAS CCTV video or any of the searchable databases within the system.

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 DAS 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 DAS 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 information contained within DAS is 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

All recruits attending the NYPD Academy receive training on the proper operation of DAS and its associated equipment. NYPD personnel receive additional command level training on accessible DAS features. All NYPD personnel must use DAS in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Immutable audit logs are created when any information is searched or accessed through DAS. The log-in and use of the system is traceable to a particular user and periodically audited for misuse by the precinct or unit's Commanding Officer. Allegations of misuse are internally investigated at the command level or by the Internal Affairs Bureau (IAB).

All members of the NYPD 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 IAB.

Supervisors of personnel utilizing DAS 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.

Integrity Control Officers (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 ITB.

HEALTH & SAFETY REPORTING

There are no known health and safety issues attributable to DAS or its associated equipment.

DISPARATE IMPACTS OF THE IMPACT & USE POLICY

The safeguards and audit protocols built into this impact and use policy for DAS mitigate the risk of impartial and biased law enforcement. DAS is a program that centralizes a large quantity of lawfully obtained data, information and resources to aid NYPD personnel in making tactical and strategic decisions. DAS does not use video analytics, facial recognition, or any other biometric measurement 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.