The City of New York
Department of Investigation

JOCELYN E. STRAUBER
COMMISSIONER

180 MAIDEN LANE
NEW YORK, NY 10038
212-825-5900

Release #20-2022
nyc.gov/doi

FOR IMMEDIATE RELEASE
THURSDAY, NOVEMBER 3, 2022

CONTACT: DIANE STRUZZI
(212) 825-5931

DOI'S OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD ISSUES REPORT ASSESSING NYPD'S RESPONSE TO THE PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY ACT OF 2020

Today, the Department of Investigation's ("DOI") Office of the Inspector General for the New York City Police Department ("OIG-NYPD") released its first Public Oversight of Surveillance Technology ("POST") Act Report pursuant to Local Law 65. This legislation requires the New York City Police Department ("NYPD") to produce and publish Impact and Use Policies ("IUPs") for surveillance technologies used by the Department and directs OIG-NYPD to prepare annual audits of the Department's compliance with these IUPs. In this first Report, among other things, OIG-NYPD assessed NYPD's overall compliance with the POST Act. A copy of OIG-NYPD's Report is attached to this release and can be found at the following link: https://www1.nyc.gov/site/doi/newsroom/public-reports.page.

DOI Commissioner Jocelyn E. Strauber said, "Surveillance technologies serve important public safety objectives. To ensure public confidence that these technologies are used appropriately, there must be rigorous oversight and transparency. The POST Act furthers that goal by requiring NYPD to make public policies about the impact and use of surveillance tools, and directing DOI's OIG-NYPD to audit compliance with those policies. This Report reflects that NYPD has largely complied with the Act's requirements, but that improvements to the impact and use policies would enable more robust oversight and even greater transparency."

Acting Inspector General Jeanene Barrett said, "Compliance with sound policies and robust oversight is necessary to assure the public that NYPD's surveillance technologies are being used responsibly. The recommendations in this Report, when implemented, will help NYPD move towards increased transparency with the public in a manner consistent with the requirements of the POST Act and best practices in other jurisdictions, as well as the needs of New York City."

To prepare this Report, OIG-NYPD (1) interviewed a range of individuals including NYPD officials, supporters of the POST Act, and experts on various surveillance technologies; (2) reviewed all published IUPs and performed a section-by-section assessment of one IUP; (3) conducted an in-depth assessment of two selected surveillance technologies; and (4) researched similar ordinances in other jurisdictions to better understand other models for achieving transparency.

OIG-NYPD's investigation determined that NYPD largely complied with the POST Act's requirements with respect to the issuance of IUPs. However, OIG-NYPD also found that the IUPs do not contain sufficient detail to allow OIG-NYPD to conduct full annual audits (as the Act also requires) and to provide full transparency to the public. In particular, the IUPs contain, in part, boilerplate language that fails to provide sufficiently specific information about the nature of the technologies, the retention period for data obtained via use of the technologies, and the entities with which the data can be shared.

OIG-NYPD also found that NYPD grouped certain related technologies, and issued a single IUP for each group. This approach significantly limits the information made available to the public concerning the nature and use of individual technologies (to the extent technologies within the group differ as to capability and

more

function) and impedes OIG-NYPD's ability to conduct meaningful oversight. OIG-NYPD interprets the POST Act to require an IUP for each surveillance technology and disagrees with NYPD's view that grouping is permitted.

The Report makes fifteen recommendations based on OIG-NYPD's findings, including:

- NYPD should issue an IUP for each individual surveillance technology, as opposed to continuing its practice of grouping similar technologies under a single IUP.
- NYPD should identify in each IUP each agency, by name, with which the Department can share surveillance data.
- NYPD should include in each IUP the specific safeguards/restrictions on use or dissemination of the surveillance data, for each entity with which the Department can share such data.
- NYPD should include in each IUP the potential disparate impacts on protected groups of the use and deployment of the surveillance technology itself.
- Within 180 days, NYPD should convene a working group of NYPD personnel, relevant City Council members or their appointees, and representatives from select advocacy groups and community groups who have expertise in surveillance technologies. The purpose of the working group is to make recommendations to NYPD on necessary updates to the existing IUPs and on any information that should be included in any future IUPs for new technologies, based on the group's expertise. NYPD's procedures applicable to the working group should ensure the protection of sensitive information as appropriate.

The POST Act Report was prepared by DOI's Office of the Inspector General for the NYPD, specifically, Assistant Inspector General Justyn Richardson; Deputy Inspector General – Policy Percival Rennie; Senior Attorney Tyler Gibson; and Investigative Attorney Julie Marling, under the supervision of Acting Inspector General Jeanene Barrett.

New York City
Department of Investigation

Office of the Inspector General for the NYPD (OIG-NYPD)

An Assessment of NYPD's Response to the POST Act

Jocelyn Strauber
Commissioner

Jeanene Barrett
Acting Inspector General for the NYPD

November 2022

Table of Contents

I. Executive Summary 1
II. Introduction and Background 8
III. The POST Act's Requirements and Community Expectations 11
A. The POST Act Imposes Limited Requirements 11
B. The POST Act as Enacted Failed to Meet Some Community Expectations 12
1. Surveillance Technology Oversight Legislation 12
2. Drafters of the POST Act 14
3. Statutory Minimums vs. Best Practices 15
IV. Methodology 15
V. Section-by-Section Assessment of LPR IUP 17
VI. In-Depth Assessment of Selected Technologies 21
A. Facial Recognition Technology 21
1. Public Concerns 22
2. Assessment of NYPD's Facial Recognition Technology IUP 23
B. Social Network Analysis Tools 28
1. Public Concerns 28
2. Assessment of NYPD's Social Network Analysis Tools IUP 29
VII. Key Findings from Review of All IUPs 30
A. NYPD Uses Vague, Non-Specific Boilerplate Language Throughout the IUPs 31
1. External Entities' Access to Data 32
2. Health and Safety Reporting 33
3. Retention, Access, and Use of the Data 33
B. NYPD Has Interpreted the Requirement to Include Information About Potentially Disparate Impacts in a Narrow Manner 34
C. NYPD Has Grouped Related Tools Together in a Way That Limits Public Oversight 35
VIII. Recommendations 37
IX. Appendix A: Text of POST Act Legislation 40
X. Appendix B: Example of Public Comment Template 44
XI. Appendix C: Text of NYPD's License Plate Readers IUP 45
XII. Appendix D: Text of NYPD's Social Network Analysis Tools IUP 55
XIII. Appendix E: Text of NYPD's Facial Recognition IUP 63

I. Executive Summary

The New York City Police Department ("NYPD") conducts widespread surveillance in the public domain using data gathered by sophisticated technology throughout New York City.[1] That technology has the capability to gather information about millions of people who move around the City. Examples of the technologies include License Plate Readers ("LPRs") and Facial Recognition Technology ("FRT"). Cars that travel from Queens to Manhattan pass dozens of Automated LPRs, which take a snapshot of a car's license plate at particular locations and times, enabling authorities to later approximate a vehicle's route. Subway passengers traveling in Manhattan from Uptown to Midtown pass hundreds of surveillance video cameras, which collect images that can later be processed by FRT. These are just two of the many types of surveillance technologies that generate data that can be used and accessed by NYPD.

These powerful law enforcement tools can play an important role in protecting public safety and aiding law enforcement in the search for missing persons or individuals suspected of committing crimes, but under certain circumstances their use may infringe on significant public rights. Therefore, sound policies and robust oversight are necessary to ensure that the capacities of these law enforcement technologies are not misused and to assure the public that these tools are being used appropriately.

Advocacy groups and community organizations across New York City have expressed concern about the Department's use of surveillance technologies.[2] Those concerns

* DOI Commissioner Jocelyn Strauber and Acting Inspector General Jeanene Barrett thank the staff of OIG-NYPD for their efforts in producing this Report, specifically, Justyn Richardson, Assistant Inspector General; Percival Rennie, Deputy Inspector General – Policy; Tyler Gibson, Senior Attorney; and Julie Marling, Investigative Attorney. Appreciation is extended to the New York City Police Department and representatives of other organizations for their assistance and cooperation during this investigation.

Special thanks are given to the former OIG-NYPD team members who contributed to the advancement of this investigation: Renell Grant and Kevonte M. Mitchell.

[1] The surveillance technologies discussed in this Report include technologies owned, operated, and maintained by other entities, such as the Department of Transportation (with respect to License Plate Readers) or the Metropolitan Transit Authority (with respect to subway surveillance cameras), which generate data to which the NYPD has access.

[2] *See, e.g.*, Albert Fox Cahn, *20 Years After 9/11, Surveillance Has Become a Way of Life*, WIRED (Sept. 9, 2021).

principally relate to the technologies' impact on civil liberties, reduced privacy in public spaces, the risk of racially targeted monitoring, and NYPD's potentially unauthorized retention of individuals' identifying data. The available equipment — including aerial drones, surveillance towers, and social media monitoring software — enables the Department to observe a range of public activity, including conduct that is political in nature.[3] Some surveillance technologies lawfully and automatically capture information about individuals who are not suspected of criminal activity and are not involved in any criminal conduct. Concerns about potential use of information obtained through this type of surveillance has fueled distrust of NYPD, particularly among communities of color and certain religious groups.[4]

To provide public oversight of the use of this technology, and to promote transparency with respect to NYPD's use of surveillance technology, on June 18, 2020, New York City Council passed the Public Oversight of Surveillance Technology (POST) Act requiring "comprehensive reporting and oversight of New York City Police Department surveillance technologies."[5] Among other directives, the POST Act requires NYPD to produce and publish Impact and Use Policies ("IUPs") for each of its qualifying surveillance technologies.[6]

---

https://www.wired.com/story/20-years-after-911-surveillance-has-become-a-way-of-life/.

[3] Aerial drones are typically small, unmanned, remote-controlled flying machines capable of being outfitted with cameras, microphones, and other surveillance technologies. Surveillance Towers are mobile surveillance towers parked in public areas, which allow officers to monitor areas from several stories above street level as well as record movements within a targeted area. Social media monitoring software/Social Network Analysis Tools are software capable of monitoring social media content (e.g., posts, pictures, "likes") according to keywords or relationship to a target individual. For further information on the above technologies, see Angel Diaz, *New York City Police Department Surveillance Technology*, BRENNAN CTR. FOR JUSTICE (Oct. 4, 2019), https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

[4] *See, e.g.*, Matt Katz, *NYPD's Legacy of Police Surveillance, From Black Panthers to Mosques to Black Lives Matter*, GOTHAMIST (Sept. 7, 2021), https://gothamist.com/news/nypds-legacy-of-police-surveillance-from-black-panthers-to-mosques-to-black-lives-matter; Zainab Iqbal, *After Decades of Surveillance, Muslims Struggle With How Much to Share Online: The Long Shadow of NYPD Surveillance After 9/11*, THE VERGE (Dec. 7, 2021), https://www.theverge.com/22810372/muslim-surveillance-social-media-nypd-new-york-informants-mosque.

[5] Creating Comprehensive Reporting and Oversight of NYPD Surveillance Technologies (POST Act), N.Y.C. Local Law No. 65 (2020) (codified at N.Y.C ADMIN. CODE § 14-188 and N.YC. CHARTER § 803[c-1]).

[6] See Appendix A for the relevant POST Act language, including with respect to the IUP requirements.

The POST Act requires, among other things, that the IUPs describe the capabilities of surveillance technology, and include any rules, processes, and guidelines that regulate access to or use of the technology, and any prohibitions or restrictions on its use, and any potential disparate impacts. The POST Act mandates that the Department publish draft IUPs on its website within 180 days of the effective date of the law (i.e., no later than January 11, 2021) for existing surveillance technologies, and at least 90 days prior to the use of any new surveillance technology.

The POST Act gives the Department of Investigation's ("DOI") Office of the Inspector General for the NYPD ("OIG-NYPD") oversight responsibility to ensure that NYPD complies with its policies on surveillance technology use. The Act directs that OIG-NYPD prepare annual audits of NYPD's use of surveillance technologies that:

1. Assess whether NYPD's use of surveillance technologies complies with published IUPs;

2. Describe any known or reasonably suspected violations of the IUPs; and

3. Publish recommendations, if any, relating to revisions of any IUPs.

OIG-NYPD reviewed the IUPs posted by NYPD on April 11, 2021 and determined that it could not conduct the type of audit required by items 1 and 2 above for this Report.[7] As explained throughout this Report, the vast majority of the IUPs produced by NYPD were general and generic in part (in that similar language was used in many of the IUPs) making it impracticable for OIG-NYPD to meaningfully assess the Department's compliance with all of its IUPs. Instead of an audit, this Report makes a number of recommendations relating to revisions to the IUPs (item 3 above) that will facilitate the mandated audits in the future.

In connection with its preparation of this Report, OIG-NYPD (1) interviewed a range of individuals including NYPD officials, supporters of the Act, and experts on various surveillance technologies; (2) reviewed all published IUPs and performed a section-by-section assessment of one IUP; (3) conducted an in-depth assessment of two selected surveillance technologies and the related IUPs; and (4) researched the rules applicable in other jurisdictions with respect to surveillance technologies, to better

[7] *See Public Oversight of Surveillance Technology (POST) Act Impact and Use Policies*, N.Y.C. POLICE DEP'T., https://www1.nyc.gov/site/nypd/about/about-nypd/policy/post-act.page (last visited Nov. 1, 2022).

understand other approaches to transparency concerning the nature and use of such technologies.

From this assessment, OIG-NYPD found that:

- NYPD has largely complied with the POST Act legislation with respect to the issuance of IUPs. That is, NYPD has issued IUPs that describe the capabilities of surveillance technologies and include the other categories of information that the POST Act requires. However, based on its investigation, the Office finds that merely meeting these requirements of the POST Act is insufficient to enable OIG-NYPD to conduct full annual audits (as the Act also requires) and to achieve appropriate transparency with the public, consistent with practices in other jurisdictions, as to the nature and use of these technologies.

- The IUPs included, in many relevant parts, boilerplate language that failed to provide sufficient detail concerning the use or nature of the technology at issue, or to differentiate between technologies. For example, NYPD used general language, much of which was identical, to address access to data and data retention for various technologies, which did not clearly identify, among other things, the specific agencies with access to the data or the length of time such data would be retained by NYPD.

- The POST Act's language requires IUPs to include "any potentially disparate impacts of the surveillance technology *[I]mpact and [U]se [P]olicy* on any protected groups as defined in the New York City [H]uman [R]ights [L]aw [emphasis added]." Because the Act requires the IUP to address only the disparate impact of the policy, rather than *the disparate impact of the technology*, the Act does not ensure that NYPD will publicly disclose any disparate impact of the technology itself. While NYPD largely complied with the Act's limited requirements concerning disclosure of the disparate impact of the IUPs, and in 5 out of 36 IUPs (14%) went beyond these requirements by addressing the potential disparate impact of the *use of the technology*, NYPD did not provide such information with respect to the vast majority of the IUPs.[8]

[8] Some potential disparate impacts of the use of the technology are presented in the IUPs for Facial Recognition Technology, Criminal Group Database, Mobile X-Ray Technology, Data Analysis Tools, and Shotspotter (*see Public Oversight of Surveillance Technology (POST) Act Impact and Use Policies*, *supra* note 7).

- NYPD grouped related technologies and issued a single IUP for multiple technologies. This approach significantly limits the information made available to the public concerning the nature and use of individual technologies (to the extent grouped technologies differ). NYPD informed OIG-NYPD that time constraints and operational considerations contributed to this approach. Furthermore, NYPD takes the position that the functionality of many of the technologies are the same, such that individual IUPs are unnecessary, and claims that the Act does not require an inventory of every technology. It is OIG-NYPD's position that the POST Act does in fact require an IUP for each surveillance technology. NYPD's interpretation, which allows grouping of several technologies under a single IUP, is contrary to the intent of the POST Act.

- It is OIG-NYPD's position that the most logical reading of the POST Act's language is that it requires an IUP for each surveillance technology. Moreover, NYPD's interpretation of the POST Act that permits grouping significantly undermines other requirements of the Act. For example, grouping may enable NYPD to bypass the POST Act's disclosure requirements for new technologies. That is, NYPD's grouping approach allows it to introduce new technologies under an existing group category covered by an existing IUP, and begin use immediately without the required notification to the public and City Council. This allows NYPD to avoid the public notification process – a critical aspect of the POST Act – and thus cannot have been the intent of the legislation.

- NYPD's grouping of related technologies also poses a practical barrier to OIG-NYPD's ability to fulfill its duties under the POST Act. Although the Department provided OIG-NYPD access to its list of technologies, the list did not include information concerning the functionality/capability of each technology — information necessary to assess whether the technologies might appropriately be grouped and whether NYPD is actually issuing IUPs with respect to each functionality and capability. Furthermore, without more information about the functionalities of the various technologies, OIG-NYPD cannot assess whether NYPD's use of surveillance technologies complies with published IUPs. For instance, the "DigiDog" robot— deployed as part of a pilot program by NYPD— has significant capabilities that potentially overlap with multiple IUP groups. It is unclear, from an oversight perspective, which IUP(s) govern the use of this technology, and, if more than one, which aspect of each IUP applies to this robotic device. This lack of clarity underscores the need for an IUP for each specific technology.

Based on these and other findings, OIG-NYPD makes the following recommendations:

1. NYPD should issue an IUP for each individual surveillance technology, as opposed to continuing its practice of grouping similar technologies under a single IUP.

2. NYPD should identify in each IUP each external agency, by name, with which the Department can share surveillance data.

3. NYPD should include in each IUP the specific safeguards/restrictions on use or dissemination of the surveillance data, for each external agency with which the Department can share such data.

4. NYPD should include in each IUP the potential disparate impacts on protected groups of the use and deployment of the surveillance technology itself.

5. NYPD should revise the Health & Safety Reporting sections of all published IUPs, to include any safety hazards that are identifiable on the basis of existing research, manufacturer warnings, or evaluations by experts in the field, or to state that no such hazards have been identified after a search for relevant information.

6. Within 180 days, NYPD should convene a working group of NYPD personnel, relevant City Council members or their appointees, and representatives from select advocacy groups and community organizations who have expertise in surveillance technologies. The purpose of the working group is to make recommendations to NYPD on necessary updates to the existing IUPs and on any information that should be included in any future IUPs for new technologies, based on the group's expertise. NYPD's procedures applicable to the working group should ensure the protection of sensitive information as appropriate.

7. Within 180 days, NYPD should create an internal tracking system for every instance in which NYPD provides an external agency with data collected via surveillance technologies that NYPD controls, including the name of the agency and the date of that the data was provided.

8. Within 90 days, in order to facilitate OIG-NYPD's statutorily obligated audit under the POST Act, NYPD should provide OIG-NYPD with information indicating, for each surveillance technology, the various types of data collected and which NYPD units maintain that information. NYPD should include

information about the retention procedures and practices for each type of data collected so that OIG-NYPD can assess NYPD's compliance with the IUPs.

9. NYPD should provide OIG-NYPD with any data access and retention policies that are included in the existing contracts with vendors who supply the surveillance technologies used by NYPD.

10. NYPD should provide OIG-NYPD with the data access and retention policies contained in any newly executed contracts with surveillance technology vendors by the 15th of each quarter (i.e., January, April, July, and October).

11. Within 30 days, NYPD should provide OIG-NYPD an itemized list of the surveillance technologies that it uses. This list should include information concerning the functionalities of each technology, so that OIG-NYPD can assess whether NYPD has, in fact, issued an IUP that covers each surveillance technology that has a distinct functionality or capability.

12. NYPD should create written policies establishing guidelines to specify the modifications that can be made to probe images used for Facial Recognition Technology.

13. NYPD should conduct periodic audits of its Facial Identification Section's use of facial recognition technology to ensure compliance with its policies related to the use of the technology and its data. This auditing process should be memorialized in writing.

14. To facilitate the OIG-NYPD's mandated annual audits, beginning January 15, 2023, NYPD should provide OIG-NYPD with quarterly updates, reflecting newly acquired or discontinued technologies in an itemized list of the surveillance technologies that it uses. Thereafter, updates should be made available by the 15th of each quarter (i.e., January, April, July, and October).

15. NYPD should issue a press release announcing the publication, related public comment period of any new IUPs, and subsequently publish the press release on its website.

II. Introduction and Background

On July 15, 2020, then-Mayor Bill de Blasio signed the Public Oversight of Surveillance Technology ("POST") Act into law.[9] The measure, New York City's adaptation of the Community Control over Police Surveillance ("CCOPS") model, requires NYPD to publicly disclose information concerning its surveillance technology and to develop policies on the use of those tools.[10]

The POST Act defines surveillance technology as "equipment, software, or systems capable of, used or designed for, collecting, retaining, processing, or sharing audio, video, location, thermal, biometric, or similar information, that is operated by or at the direction of [NYPD]."[11] For each qualifying technology, NYPD must publish an Impact and Use Policy ("IUP") that reports on the following ten areas (see Appendix A for a copy of the relevant portion of the statute):

1. A description of the capabilities of the technology;

2. Rules, processes, and guidelines issued by NYPD regulating access to or use of the technology, including whether NYPD obtains court authorization for use;

3. Safeguards designed to protect information collected by the technology from unauthorized access;

4. Policies and/or practices relating to law enforcement's retention, access, and use of data collected by the technology;

[9] POST Act, s*upra* note 5.
[10] The Community Control Over Police Surveillance (CCOPS) model provides a template for legislation in the United States (*Community Control over Police Surveillance (CCOPS) Model Bill,* AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/legal-document/community-control-over-police-surveillance-ccops-model-bill (last updated April 2021). Introduced by the American Civil Liberties Union (ACLU), the model aims to improve communities' ability to review and control law enforcements' use of surveillance technologies. It has served as a model for similar legislation enacted around the country (*Community Control Over Police Surveillance (CCOPS)*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance [last visited Nov 1, 2022]).
[11] POST Act, *supra* note 5.

5. Policies and procedures relating to access or use of data collected by the technology by members of the public;

6. Details about whether outside entities have access to the data collected by the technology;

7. Information regarding any training that NYPD requires for individuals to use the technology;

8. A description of internal audit and oversight mechanisms to ensure compliance with the IUPs;

9. Any tests or reports regarding the health and safety effects of the technology; and

10. Any potential disparate impacts "of the surveillance technology [I]mpact and [U]se [P]olicy" on any protected groups as defined by NYC Human Rights Law.[12]

The Act requires NYPD to publish draft IUPs for its existing surveillance technologies for public comment within 180-days from the date of enactment.[13] It also requires NYPD to publish an IUP on its website at least 90 days prior to the use of any new surveillance technologies; Figure 1 illustrates this process. After publication, for both existing and new technologies, the public has 45 days to submit comments. NYPD then has an additional 45 days to publish the final IUPs on its website.

Consistent with the requirements of the Act, on January 11, 2021, NYPD published 36 draft IUPs on its website, 180 days after the signing of the POST Act.[14] The posted policies remained open 45 days for public comments to be uploaded directly through its website. NYPD did not issue a press release announcing the posting or the public comment period, which the Act does not require.

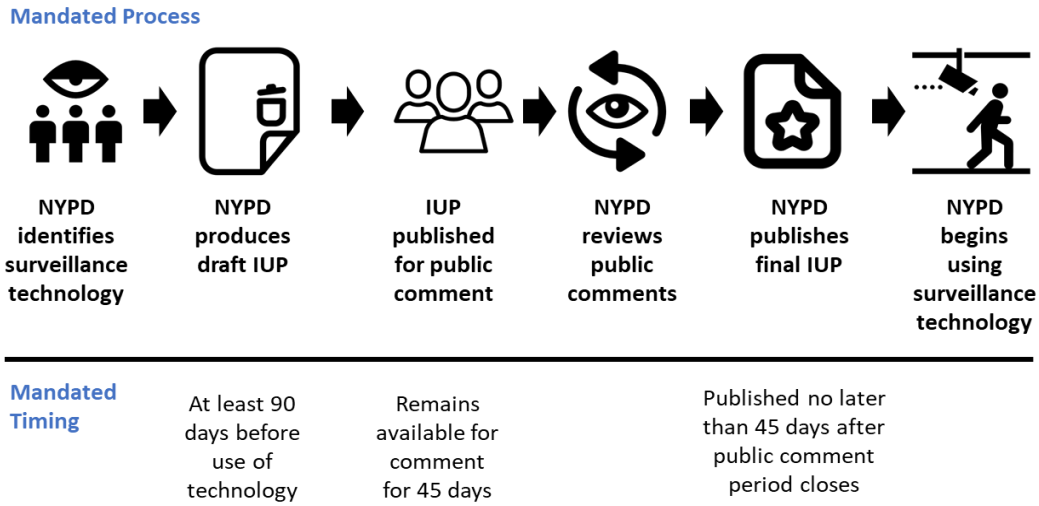
[12] *Id.*
[13] This 180-day deadline corresponded to the end of January 2021.
[14] *Draft Policies for Public Comment*, N.Y.C. POLICE DEP'T., https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page [https://perma.cc/AV44-UJHL?type=image].

NYPD received 7,819 public comments on the IUPs during the 45-day period from January 11, 2021 through February 25, 2021. Of those, 7,392 comments (95%) were identified by the Department as potential spam. NYPD informed OIG-NYPD that the remaining 5% of the comments on the IUPs were identical. According to the Department, those comments were sent via the websites of two advocacy groups, Amnesty International and Surveillance Technology Oversight Project (STOP), that provided a pre-filled template concerning the draft IUPs for submission.[15]

In interviews, members of the Department explained that during the above-mentioned 45-day period, the public comments were reviewed by a three-person team of NYPD attorneys in order to determine whether any changes would be made. A summary of the changes made to the draft policies appears on the first page of the IUPs. As an example, for the two IUPs that are analyzed in this Report – Facial Recognition and Social Analysis Network Tools – the public comments highlighted that there is no industry-standard definition for "artificial intelligence" and "machine learning" (terms used in the draft IUPs). The POST Act does not require that NYPD comment on whether the technologies include such functionalities, nor does it require that these terms be defined. In the final IUP, NYPD did not include a definition of these terms, but instead removed them entirely. While not in violation of the POST Act, this change heightened public suspicion that the Department's IUPs were not transparent with respect to the surveillance technologies' functionalities.[16]

Figure 1: Mandated Process for New Surveillance Technology as Defined by the POST Act Legislation[17]

[15] See Appendix B for an example of this pre-filled template.
[16] *See* Michael Sisitzky, & Ben Schaefer, *The NYPD Published Its Arsenal of Surveillance Tech. Here's What We Learned,* ACLU OF N.Y. (Feb. 24, 2021), https://www.nyclu.org/en/news/nypd-published-its-arsenal-surveillance-tech-heres-what-we-learned.
[17] POST Act legislation graphic created by OIG-NYPD staff.



III. The POST Act's Requirements and Community Expectations

The POST Act directs the Office of the Inspector General for the NYPD ("OIG-NYPD") to publish any recommendations relating to the revision of IUPs. Aside from some gaps in compliance discussed herein, OIG-NYPD has concluded that NYPD has largely complied with the limited requirements of the POST Act. However, it is OIG-NYPD's position that NYPD can and should provide greater transparency than the POST Act requires, with respect to the technologies it employs, without disclosing sensitive law enforcement information that might compromise public safety. The Office's position with respect to the need for greater transparency is principally based on community expectations, the practices of other jurisdictions with respect to surveillance technologies, and the City's practices with respect to public involvement in rulemaking in other areas.

A. The POST Act Imposes Limited Requirements

As noted above, the POST Act's requirements are limited. The Act directs NYPD to, at a minimum, publish information on its surveillance technologies in the required ten areas within the mandated time period. For existing technologies, the Department published draft IUPs, allowed requisite time for public comment, and thereafter published final drafts, all within the required time periods. Each IUP included information for each of the ten required areas. NYPD therefore has largely complied with this limited requirement of the POST Act, with certain specific

exceptions discussed further herein.[18] OIG-NYPD's recommendations, as noted above, are based on its determination that additional transparency would better serve the public and be consistent with the practices in other jurisdictions.

B. The POST Act as Enacted Failed to Meet Some Community Expectations

This investigation concluded that the POST Act did not require the same level of transparency with respect to the use of surveillance technology as other jurisdictions require, and as advocates involved in the passage of the Act expected. A review of comparable legislation in other jurisdictions, New York City practice with respect to proposed rulemaking in other contexts, and interviews of advocates support this conclusion.

1. Surveillance Technology Oversight Legislation

To better inform OIG-NYPD's understanding of the initial objectives of the POST Act, the Office reviewed surveillance technology oversight legislation from around the country.[19] This review revealed similar legislation in at least seven states and nearly two dozen cities: some requiring other administrative agencies or working groups to assist with the creation, review, and approval of surveillance technology policies; some requiring an opportunity for public comment during properly noticed public meetings; and some giving separate administrative bodies, or City Councils, the authority to approve or reject acquisitions of surveillance technologies. See Figure 2 for an example process from Seattle.

In contrast to all other city ordinances reviewed, New York City's POST Act requires that NYPD disclose only basic details about the technology that is being deployed. For example, the Seattle Police Department's ("SPD's") Surveillance Impact Report on License Plate Readers ("LPRs"), which is comparable to an IUP, is 353 pages and

[18] There are some gaps in compliance, especially with regard to NYPD's practice of grouping multiple technologies within a single IUP. See Section VII.C below.

[19] The Office conducted a more in-depth comparative analysis of legislation from Santa Clara County, and San Francisco, California as well as Seattle, Washington, locations with population, urban density and security threats comparable to New York City's.
SANTA CLARA CNTY., CAL., CODE OF ORDINANCES § A40-1 to A40-12 (2016), http://sccgov.iqm2.com/Citizens/FileOpen.aspx?Type=4&ID=149330&MeetingID=7193;
SEATTLE, WASH., MUN. CODE 14.18.010-18.080 (2018), https://library.municode.com/wa/seattle/codes/municipal_code?nodeId=TIT14HURI_CH14.18ACUSSUTE_14.18.010DE;
S.F., CAL., ADMIN. CODE Ch. § 19B.1-B.10 (2019), https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320.

provides information including: (1) a reference list of research and media articles concerning the benefits of the technology; (2) how LPRs relate to SPD's mission; (3) the required training to use the technology; (4) details on when and how often LPRs are in operation; (5) who determines how LPRs are deployed; (5) whether LPRs are visible to the public; (6) a list of the specific outside entities with access to the data; and (7) the experts consulted about the technology.[20]

New York City is the only jurisdiction of those reviewed by OIG-NYPD that does not require community input or legislative decision-making with respect to the selection and use of surveillance technology and the policies and procedures applicable to that technology. The three-person group that reviews the public comments on the draft IUPs consists solely of attorneys employed by NYPD. There is far less robust public oversight of surveillance technologies in New York City than in other locations because (1) NYPD is the sole entity responsible for the collection and review of public comments on the IUPs; (2) the POST Act does not require extensive detail concerning the nature and use of surveillance technology to be included in IUPs (which are public); and (3) there is no legislative or other public body that controls the selection of surveillance technologies, the use of such technologies, and the policies concerning the technologies.

Figure 2: Seattle Surveillance Technology Review Process[21]

[20] SEATTLE POLICE DEP'T., 2018 SURVEILLANCE IMPACT REPORT: AUTOMATED LICENSE PLATE RECOGNITION (2019), https://www.seattle.gov/documents/Departments/Tech/Privacy/SPD%20ALPR%20%28Patrol%29%20-%20Final%20SIR.pdf.

[21] Seattle Information Technology, *Surveillance Technologies, Surveillance Impact Report Stages*, http://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies/about-surveillance- (last visited Nov. 1, 2022).

Furthermore, the POST Act does not require the same type of public comment process that is required by the New York City Administrative Procedure Act ("CAPA").[22] CAPA describes the general process for rulemaking by New York City agencies. Before adopting any rule under CAPA, the agency must not only afford the opportunity for public comment, but advertise that opportunity in specified ways. The comments received are placed into the public record.[23] Agencies must also permit and consider petitions by members of the public to adopt rules that the public proposes.[24] By contrast, the POST Act merely requires that the Department must receive and consider public comments, but does not require that those comments be posted, and does not provide a process for the public to propose, and the Department to consider, particular surveillance technology policies.

2. Drafters of the POST Act

In interviews with community organizations and advocacy groups that assisted in the drafting of the POST Act, the Office heard concerns about the manner in which NYPD complied with the legislation. These interviews, which took place after the Department's publication of its draft IUPs, highlighted the following perceived deficiencies of the final IUPs: information about how the tools were deployed was not included; an assessment of the disparate impact of the use of the technology was not included; information on who has access to the data collected was not included; and,

[22] *See generally* N.Y.C. CHARTER §§ 1041-1047.
[23] N.Y.C. CHARTER § 1043(e).
[24] N.Y.C. CHARTER § 1043(g).

detail about which vendors were used was not included. Disclosure of these details, according to the groups and organizations, would be more consistent with their expectations with respect to the POST Act.

3. Statutory Minimums vs. Best Practices

The POST Act imposes certain requirements on NYPD with respect to surveillance technologies, but it does not prohibit the Department from providing additional information in the interests of transparency and good governance. Beyond OIG-NYPD's specific responsibilities with respect to auditing NYPD's compliance with the POST Act, its mandate is to "study, audit and make recommendations relating to the operations, policies, programs and practices" of NYPD in order to increase public safety, protect civil rights and civil liberties, and to increase the public's confidence in the police force; thus building stronger police-community relations.[25] OIG-NYPD's position is that NYPD can and should provide additional information about these technologies, where doing so does not compromise the confidentiality of sensitive law enforcement information. The POST Act's requirements establish the minimum with respect to disclosures. But in light of the expectations of community organizations and advocacy groups, the practices in other jurisdictions, and the notice and comment procedure of CAPA, OIG-NYPD recommends improvement to the IUPs, consistent with the requirements of similar legislation around the country and the expectations of those involved in the drafting of the legislation. The Office is sensitive to the need to balance law enforcement confidentiality and public transparency, and the recommendations in this Report offer concrete proposals with this balance in mind.

IV. Methodology

OIG-NYPD reviewed all 36 draft and final IUPs, examined the POST Act legislation and its history, interviewed a range of individuals including officials from NYPD's Legal Bureau, searched for any complaints received by the Department of Investigation (DOI) alleging that NYPD violated the IUPs, reviewed comparable legislation from other jurisdictions across the country, and conducted a section-by-

[25] N.Y.C. CHARTER § 803(c)(1).

section assessment of one IUP, and an in-depth assessment of two selected technologies and related IUPs.[26]

Interviews with legal experts, advocacy groups (including those who supported and participated in the drafting of the POST Act), community organizations, and subject matter specialists, were central to the data-gathering process. These interviews, as well as a review of City Council hearing testimony concerning the development of the legislation, provided background on the Act.

In its discussions with the Department, OIG-NYPD gathered details related to the processes of drafting IUPs, considering public comments, and finalizing the policies. These discussions informed the Office's understanding of NYPD's process with respect to the POST Act's requirements, and clarified various points related to the content of the IUPs.

As required by the POST Act, OIG-NYPD conducted a review of complaints (from individuals and entities) received by DOI in the 2021 calendar year to identify any potential allegations of violations of the POST Act or IUPs; none of the complaints alleged violations of the IUPs.[27]

To inform any recommendations regarding revisions of the IUPs, OIG-NYPD conducted an in-depth comparative analysis of legislation similar to the POST Act in other relevant jurisdictions. This review was limited to surveillance technology oversight laws in effect for Santa Clara County, California; Seattle, Washington; and San Francisco, California.[28] These jurisdictions were selected due to certain similarities with New York City as to population, urban density, and security threats.

---

[26] OIG-NYPD received one document, from the Legal Aid Society, presenting arguments that NYPD had violated the POST Act, not any specific IUP. While this complaint does not fall squarely into the Office's responsibility to review and "describe any known or suspected violations of surveillance technology [IUPs]," it was considered for background on public concerns.

[27] Consistent with DOI's policies and practices, OIG-NYPD reviews all complaints received from members of the public or other entities and generally investigates those complaints that raise systemic issues. OIG-NYPD also refers complaints to other agencies (and/or squads at DOI) where the complaints fall within their areas of focus.

[28] While Santa Clara has a smaller population than the other cities, it was selected in part because it was the first city to introduce surveillance technology legislation in the United States (Selena Larson, *Communities Call for More Control Over Police Surveillance*, CNN (Feb. 7, 2017), https://money.cnn.com/2017/02/07/technology/cop-surveillance-aclu-santa-clara-bart/.

OIG-NYPD conducted a section-by-section assessment of the IUP for LPRs. OIG-NYPD assessed each section to evaluate the sufficiency of the information provided (see Appendix C for the full text of the IUP). The language highlighted in blue in Appendix C is included, largely verbatim, in many of the IUPs, and illustrates that much of the content did not clearly identify, among other things, relevant details such as the particular agencies with access to the data gathered via the surveillance technology or the length of time such data would be retained. Following each section of blue highlighted language is a "note box" that indicates the number of IUPs that contain identical or nearly identical statements.

For the in-depth assessments of the IUPs, OIG-NYPD selected FRT and Social Network Analysis Tools. The Office interviewed supervisors from the units responsible for handling the two selected technologies, as well as experts in these technologies. These interviews provided valuable information about NYPD's actual use of the technologies and was supplemented by the Office's review of certified training programs on the use of the surveillance technologies.

V. Section-by-Section Assessment of LPR IUP

For each section of the IUP for License Plate Readers, OIG-NYPD concluded that the information provided by NYPD largely complied with the requirements of the POST Act, although the IUP could be improved by the inclusion of additional information and clarification about the technology in certain areas, as discussed further below.[29]

1. Capabilities of Technology

The POST Act requires that an IUP include "a description of the capabilities of a surveillance technology." The information provided by NYPD in this section provides an overview of what License Plate Readers are, how the technology works, and the three types of data that are collected. The Department's description of the technology appears both clear and comprehensive, providing information found in other publicly available sources.[30]

2. Rules, Processes, and Guidelines Relating to Use of the Technology

[29] See Appendix C for the full text of the License Plate Readers IUP.
[30] *See*, *e.g.*, *Automated License Plate Readers*, ACLU OF N.Y., https://www.nyclu.org/en/automatic-license-plate-readers#:~:text=What%20are%20automatic%20license%20plate,its%20date%2C%20time%20and%20location (last visited Nov. 1, 2022).

The POST Act requires that an IUP include "rules, processes[,] and guidelines issued by the [D]epartment regulating access to or use of" the tool, in particular: (1) the rules, processes, and guidelines; (2) any prohibitions or restrictions on its use; and (3) whether court authorization is obtained prior to use. The Office observed that with respect to part (1), the rules, processes, and guidelines governing the use of LPRs, the IUP provides minimal detail. A full list of rules, processes, and guidelines for the use of the data obtained via this technology may exist within relevant Patrol Guide sections, policy memoranda, or Interim Orders, if so, the IUP should link or make clear reference to these materials.

The IUP clearly states the prohibitions and restrictions on use of LPRs, as well as the fact that court authorization is not required to use LPRs, and thus satisfies requirements (2) and (3) noted above.

3. Safeguards and Security Measures Against Unauthorized Access

The POST Act requires the IUP to include the following information with respect to safeguards and security measures against unauthorized access: (1) description of the safeguards or security measures; (2) whether encryption exists; and (3) description of access control mechanisms. The LPR IUP gives sufficient detail about the safeguards and security measures that protect against unauthorized access, notes that the information obtained via LPR is encrypted within NYPD computer systems, and adequately describes the access control mechanisms.

4. Policies and Procedures Relating to Retention, Access, and Use of the Data

The POST Act requires that IUPs include policies and procedures related to (1) the retention of data; (2) access to data; and (3) the use of data. NYPD's IUP provides sufficient information with respect to access to data and lists five circumstances under which use of the data is allowed.

The IUP states that NYPD collects three types of LPR data: (1) a vehicle's license plate number and state of issuance; (2) images of a vehicle and the license plate; and (3) the date, time, and location the vehicle passed the LPR. According to the IUP, these three types of data are retained for five years. The IUP also states that data retention time periods are based on the nature of the "case investigation record," and those periods range from permanent retention of the data to retention for one year. However, the IUP does not make clear under what circumstances LPR data may qualify as a case investigation record or how the 5-year retention period relates to the periods determined based on the nature of the "case investigation records."

5. Policies and Procedures Relating to Public Access or Use of the Data

The POST Act requires that the IUP include information regarding policies and procedures related to the public's access to and use of data from surveillance technologies. The LPR IUP makes clear that data obtained from LPRs is available to the public only via a Freedom of Informational Law ("FOIL") request. It would be preferable to include in the IUP a link or reference to the NYPD policy on handling FOIL requests, so that the public could be better informed of the circumstances under which such data could become public.

6. External Entities

The POST Act requires IUPs to include the following information concerning third parties' access to surveillance technology data: "whether entities outside the [D]epartment have access to the information and data collected by such surveillance technology, including: (a) whether the entity is a local governmental entity, state governmental entity, federal governmental entity[,] or a private entity, (b) the type of information and data that may be disclosed by such entity, and (c) any safeguards or restrictions imposed by the department on such entity regarding the use or dissemination of the information collected by such surveillance technology[.]"[31] The IUP makes clear that data may be shared with third parties, including government agencies at all levels as well as private vendors and contractors performing contractual duties for NYPD. However, while the IUPs make general references to the types of entities that have access, none of the entities are listed by name.

The IUPs do not make clear whether third parties have access to all three types of LPR data and if not, which third parties have access to which type of data. Furthermore, despite the POST Act's requirement, the IUP does not make clear what, if any, safeguards and restrictions apply to the use of such data by third parties.

7. Training

The POST Act requires that IUPs include information regarding whether training is required to use or access information from surveillance tools. The LPR IUP states that users receive "command level training," a vague description that does not give any details about the kind or frequency of training that is required for use or access. Adding this detail would improve the public's understanding of the type of training

[31] POST Act, *supra* note 5.

received by NYPD staff entrusted with access to and use of the data generated by this technology.

8. Internal Audit and Oversight Mechanisms

The POST Act requires a description of any internal audit and oversight mechanisms that ensure compliance with the IUP. The IUP provides general information about who has oversight responsibilities, but gives little detail about the oversight mechanism. Specifically, it is unclear what information is audited by NYPD to monitor compliance with the IUP or how breaches in policy are identified and addressed.

9. Health and Safety Reporting

The POST Act requires information on any tests or reports regarding health and safety impacts of the surveillance tool. The LPR IUP states that there are no "known health and safety issues" with LPRs. In light of the nature of LPRs, this assessment is sufficient for this IUP. However, as noted below, for other technologies, OIG-NYPD recommends that NYPD provide additional information, including, for example, describing efforts made to identify any relevant health and safety tests and reports that may exist and a review of manufacturer warnings or evaluations by experts in the field.

10. Disparate Impacts

The POST Act requires that the IUP include information concerning the "potentially disparate impacts of the surveillance technology [I]mpact and [U]se [P]olicy on any protected groups." In this section, the Department first states that "the safeguards and audit protocols built into this [I]mpact and U]se [P]olicy for LPRs mitigate the risk of impartial [sic] and biased law enforcement." The Department notes that biometric measurements are not collected by LPRs, and then states its policy on impartial enforcement of the law. The IUP does not address the potential disparate impacts of *the use of the technology* and the Act does not require that NYPD provide that information.

Although not required by the POST Act, the Office recommends that NYPD include in the IUP any available information about the potential disparate impacts of the use of the technology. For example, the potential impacts of deploying LPRs in a community are not explored. Important questions about this impact are: Where is this technology typically deployed? Is it deployed more frequently in particular neighborhoods? Does the location and use of technology result in the gathering of

more data with respect to members of particular demographic groups, as opposed to other groups? Does NYPD access LPR data obtained from particular neighborhoods more frequently than from other neighborhoods? What are the demographics of the neighborhoods where data is most frequently obtained by NYPD? Does that data more frequently relate to members of particular demographic groups?

VI. In-Depth Assessment of Selected Technologies

OIG-NYPD conducted in-depth assessments of the Facial Recognition and Social Network Analysis technologies and concluded that the IUPs related to these technologies could be improved by including additional details about: (1) the capabilities of the tools used by NYPD; (2) the extent to which external entities control data captured by the Department's use of these tools; and (3) how NYPD ensures compliance with the IUPs (in particular, what information NYPD reviews to do so).

A. Facial Recognition Technology

Facial Recognition Technology ("FRT") refers to computer programs that compare facial images to assess their similarity. FRT utilizes a complex series of algorithms and data science to render a photograph of a face into a series of data points — a faceprint — that can then be compared to other faceprints.

Law enforcement agencies typically use FRT for two purposes: (1) to confirm the identity of a suspect, victim, missing person, or to exonerate those who have been wrongfully accused after a crime has occurred; or (2) real-time public surveillance. FRT compares images to a database of known suspects images. Some FRT is capable of facilitating real-time surveillance by comparing known suspect images with images captured by continuously scanning individual's faces (e.g., in a crowd) with a video-capturing device, and responding to those results that reach a threshold of similarity.[32] However, according to NYPD, and as discussed in the FRT IUP, the Department does not have FRT capable of conducting real-time public surveillance. Examples of NYPD's use of this technology to confirm the identity of a suspect after

[32] Any video can be fed through the FRT algorithm, which identifies and isolates faces for comparison.

a crime has occurred include an attempted rape case in August 2020 and an investigation involving suspected bomb containers in the subway in August 2019.[33]

1. Public Concerns

Public concern around the use of FRT centers on the risk that its use leads to increased bias in policing, and can curtail the exercise of public speech. There have been allegations that this technology results in disproportionate misidentification of individuals within certain demographic groups.[34] This perception may in part be due to the fact that FRT algorithms most accurately identify members of demographic groups whose photos have been used to "train" the algorithm. For example, studies show that FRT algorithms have higher false positive rates for Asian and Black individuals than for white individuals.[35] An algorithm's inability to distinguish between faces of a particular demographic group can result in increased numbers of mistaken "matches" when used with respect to that group (i.e., false positives).[36] Similarly, the make-up of the database used to search for a possible-match candidate can affect the likelihood of a match. For example, if a database is comprised mostly of men, but the possible-match candidate is a woman, the likelihood of a mistaken identity is increased.

In the wake of various protests in the United States, there have been claims, including by the media, that after protests, police officers outside of New York City were using FRT in order to find and arrest activists, in particular those with outstanding warrants.[37] In one example, Pennsylvania State Police, aided by FRT,

---

[33] Frank Miles, *NYPD Uses Facial Recognition to Arrest Brazen Sex Offender Accused of Attempted Rape on Subway Platform*, FOX NEWS (Aug. 30, 2020), https://www.foxnews.com/us/nypd-uses-facial-recognition-to-arrest-brazen-sex-offender-accused-of-attempted-rape-on-subway-platform; Craig McCarthy, *How NYPD's Facial Recognition Software ID'ed Subway Rice Cooker Kook*, THE N.Y. POST (Aug. 25, 2019), https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/.

[34] Davide Castelvecchi, *Is Facial Recognition Too Biased to Be Let Loose?*, NATURE (NOV. 18, 2020), https://www.nature.com/articles/d41586-020-03186-4.

[35] Jan Lunter, *Beating the Bias In Facial Recognition Technology*, BIOMETRIC TECH. TODAY, Oct. 2020, at 5, 5–7, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7575263/.

[36] *See generally* PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS AND TECH, FACE RECOGNITION VENDOR TEST (FRVT), PART 3: DEMOGRAPHIC EFFECTS (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[37] See, *e.g.*, Kevin Rector & Alison Knezevich, *Social Media Companies Rescind Access to Geofeedia, Which Fed Information to Police During 2015 Unrest*, THE BALTIMORE SUN (Oct. 11, 2016), https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html;

used social media posts to identify individual protesters from details as small as a cross tattoo in the corner of an eye.[38] Advocates warn that such use can discourage people from engaging in protected public speech.[39]

2. Assessment of NYPD's Facial Recognition Technology IUP

As required by the POST Act legislation, NYPD published an IUP on its use of FRT. Similar to other IUPs, the policy for FRT largely complies with the Act's requirements, but provides minimal information about NYPD's uses of this surveillance technology, its data sharing and retention practices, oversight of the handling of data generated by this technology, and the potential disparate impacts of its applications.

NYPD informed OIG-NYPD that its staff access FRT through a portal provided by the United States Office of National Drug Control Policy ("ONDCP") New York/New Jersey High Intensity Drug Trafficking Areas ("HIDTA") program. This portal, which uses the DataWorks Face Plus program, compares arrest images, from arrests made in New York or New Jersey, to an image provided by the Department (referred to herein as a "probe" image).[40] The Department informed OIG-NYPD that the DataWorks Face Plus program does not make comparisons to images from drivers licenses or other forms of official identification documents but only to arrest images. As stated in the IUP, NYPD maintains records of all requests, including the original probe image(s) submitted to the Facial Identification Section ("FIS"), which is the unit within the Department charged with FRT administration. Additionally, NYPD

Juliette Rihl, *Emails Show Pittsburgh Police Officers Accessed Clearview Facial Recognition After BLM Protests*, PUBLICSOURCE, (May 20, 2021), https://www.publicsource.org/pittsburgh-police-facial-recognition-blm-protests-clearview/.

[38] Katie Shepherd, *An Artist Stopped Posting Protest Photos Online to Shield Activists from Police. Then, He Was Arrested*, THE WASH. POST (Aug. 3, 2020), https://www.washingtonpost.com/nation/2020/08/03/philadelphia-arrest-protest-photos/

[39] *Street-Level Surveillance, Face Recognition*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/face-recognition#:~:text=Face%20recognition%20is%20a%20method,identify%20people%20during%20police%20stops (last updated Oct. 24, 2017).

[40] Details regarding the DataWorks Plus programs may be referenced on the company's website at www.dataworksplus.com. For information on the FACE Plus program, see *Face Plus, Facial Recognition Technology & Case Management*, DATAWORKSPLUS, https://www.dataworksplus.com/bioid.html#face (last visited Nov. 1, 2022). DataWorksPlus does not create FRT algorithms itself. Instead, it uses algorithms supplied by NEC, Rank One Computing, and Cognitec (Dave Gershgorn, *California Police are Sharing Facial Recognition Databases to ID Suspects*, MEDIUM [Aug. 1, 2019], https://onezero.medium.com/california-police-are-sharing-facial-recognition-databases-to-id-suspects-3317726d31ad; *see also* Grother et al., *supra* note 36).

maintains records of output from the FIS (e.g., possible match candidates). As discussed further below, it is a standard practice in certain circumstances to alter an original probe image to facilitate a search; NYPD also maintains copies of any altered images used for the FRT search. NYPD does not keep records of the results of the searches conducted, and related acts of the FIS staff relating to the search. These acts could include modifying a probe image, which NYPD reported can be done on NYPD computers before uploading the image or it can be done through the DataWorks Face Plus program software accessed through HIDTA.

The way in which NYPD accesses FRT (via a portal provided by HIDTA) has significant implications for NYPD's data retention, data sharing, and auditing practices because many of the details related to the parameters of FRT searches conducted by NYPD are held by HIDTA, the portal owner. In other words, NYPD keeps records of the requests to the FIS unit (i.e., a request to determine whether a probe image matches a known individual in the available databases), the original probe image and any altered images run through the databases, and the output *from* the FIS unit, such as the report to the field investigator of possible matches. However, many other records are controlled by and would need to be requested from HIDTA. Such records would reflect the particulars of each round of searches conducted, including the likelihood that the probe image and the possible match candidates depict the same individual, as well as the details with respect to precisely how altered probe images were modified.

NYPD informed OIG-NYPD that it is capable of auditing FRT searches. However, OIG-NYPD maintains that the need to request search history records from a third-party entity (e.g., the DataWorks Face Plus program run through HIDTA) introduces additional barriers to NYPD and OIG-NYPD's ability to regularly review searches for misuse or policy violations (e.g., searches unrelated to an investigation). How long these records are kept, in what format, and with whom the records could be shared are all controlled by HIDTA. Moreover, NYPD does not have a policy in place to review these past FRT searches and it may have difficulty doing so, because it does not control the database and all of the records that would be subject to review. NYPD also has no policy or process in place to audit how the DataWorks Face Plus program handles the data. NYPD informed OIG-NYPD that its agreement with DataWorks had no terms and conditions in relation to its Face Plus program accessed through HIDTA, including with respect to how data is retained, stored, and protected from disclosure. These terms and conditions would set forth the data retention standards necessary to craft policies around and conduct such an audit. Agreements with HIDTA setting forth polices around data use and auditing are not without precedent. For example, the partnership between the Northern California Regional Intelligence

Center ("NCRIC") and HIDTA produced a policy on Facial Comparison Analysis, which sets forth, among other things, data retention standards, data dissemination standards, and that designated managers and supervisors should conduct periodic audits regarding access to HIDTA's data.[41] NYPD should have a similar policy in place regarding periodic audits of the FIS unit's use of the DataWorks Face Plus program accessed through HIDTA. OIG-NYPD will continue to monitor whether NYPD has sufficient audit-related policies established for other technologies.

NYPD also informed OIG-NYPD that FIS has a process in place (although it is not memorialized in a written policy) for conducting face comparisons. That process includes both the use of the FRT software as well as human reviewers and some internal oversight. In the first step of this process, an investigator in the FIS reviews the quality of the images to be used as probe images. If these images are of poor quality, the risk of misidentification increases. Thus, consistent with industry standards, NYPD FIS investigators have the authority to reject the image and refuse to conduct an FRT software comparison or to modify the image in limited ways in order to improve the quality of the image.[42] NYPD reported to OIG-NYPD that the modifications to the probe images can be made by NYPD prior to uploading the image to the HIDTA portal or within the HIDTA portal after upload, or both.

Modifying probe images to facilitate FRT searches is a common and appropriate manner of using the technology, but model practices emphasize the need to maintain records of any modifications made.[43] For example, model practices include a specified order of modifications, the first step of which is that the probe image can be cropped, resized and/or rotated, the background blurred, and the posing of the face corrected. Those initial changes should be made, and the altered probe image run through the FRT software before the subject's face is modified in any way. The next modification phase of the model practice for an FRT search involves image processing (typically using Adobe Photoshop or GNU Image Manipulation Program [GIMP]) including, but

[41] *Facial Comparison Analysis Policy*, HIDTA/NCRIC (Oct. 2021), https://ncric.ca.gov/wp-content/uploads/2021/10/NCRIC-Facial-Comparison-Analysis-Policy.pdf.
[42] For an example of New York State's model policy on FRT, see N.Y. STATE MUN. POLICE TRAINING COUNCIL, FACIAL RECOGNITION MODEL POLICY (Dec. 2019), https://www.criminaljustice.ny.gov/crimnet/ojsa/standards/MPTC%20Model%20Policy-Facial%20Recognition%20December%202019.pdf.
[43] *See* FACIAL IDENTIFICATION SCI. WORKING GRP., STANDARD PRACTICE/GUIDE FOR IMAGE PROCESSING TO IMPROVE AUTOMATED FACIAL RECOGNITION SEARCH PERFORMANCE (July 17, 2020). https://fiswg.org/fiswg_image_proc_to_improve_fr_search_v2.0_2020.07.17.pdf.

not limited to, color/tint correction, de-blurring or sharpening, lens distortion correction, red eye reduction, and other modifications. The altered probe images resulting from these modifications should be run through the FRT software at specific points in that process and may produce a different candidate search result set. Finally, the subject's face can be modified including, but not limited to, changes to hair, head coverings, replacing or creating missing facial landmarks, and altering excessive make-up, which may produce yet another candidate set. According to the model practices, after certain points in the progression of image processing, an FRT search should take place and the match candidates evaluated.[44]

In contrast with the stringent model practices set forth above, NYPD did not report using *any* guidelines to specify the types, order, or number of modifications that could be conducted, and at what points in the alteration process searches should be run. Also, in contrast with the model practices, NYPD edits probe images using Microsoft Paint, a basic graphics editor, among other programs. Although NYPD also uses Adobe Photoshop to make modifications, which is in accordance with model practices, notably NYPD does not utilize Adobe Photoshop's Edit History log and stated that it was unaware of how much detail the Edit History log contains with respect to modifications. Adobe Photoshop allows users to turn on and off the Edit History log and to choose what level of modification detail is retained. However, NYPD does not have a policy requiring the Edit History log to be turned on. Therefore, it is unclear which, if any, of NYPD's edits in Adobe Photoshop have been retained and can be reviewed.

Moreover, although NYPD retains records of rejections by the FIS due to low quality, as well as the altered probe images run through the FRT software, it does not retain logs of each individual modification made to produce the altered probe images, whether modifications occurred on NYPD computers or through the HIDTA portal nor does NYPD retain notes about the points in time during the modification process that searches were conducted. The failure to track individual modifications that are made to the probe images limits potential oversight of how images are altered in the course of a search – failure to alter images in the appropriate manner can result in misidentification. However, this concern could be readily avoided if NYPD used the model practice of (1) making the process of face comparison iterative and (2)

[44] *Id.*

documenting modifications to the images.[45] NYPD should put policies and procedures in place delineating the process by which FIS investigators should modify a probe image in a specified manner and order and run the modified image through the FRT software, review the FRT software output, modify the probe image again, conduct the FRT comparison again, and retain the search results with respect to each altered probe image used to search. If the Department tracked modifications to probe images, it would have a record that could be used to determine whether the FIS modified images pursuant to stated policy (and the industry standard) or in a way that might raise the risk of misidentification. Without an accurate log of these modifications, the record of exactly which modifications created the altered images is lost, foreclosing review by NYPD or OIG-NYPD.

NYPD *did* provide information about the potential disparate impact of the use of FRT itself (as opposed to the disparate impact of the IUP) in the FRT IUP. As noted above, however, NYPD did not provide this information in 31 out of 36 IUPs, opting instead to address the potential disparate impact of the IUPs themselves. In the FRT IUP, the Department acknowledged research highlighting poor performance by some algorithms in matching photographs of individuals from certain racial and/or ethnic groups, if the algorithms were not trained with respect to those groups.[46] The IUP also noted "an important federal government study on the subject" that suggested that human review of FRT matches could alleviate such errors. This study, however, is not cited in the IUP. When asked for the study in connection with the preparation of this Report, NYPD claimed that a National Institute of Standards and Technology study presents evidence that "erroneous software matches can be swiftly corrected by human observers." OIG-NYPD reviewed that study and concluded that it does not support NYPD's claim that human observation can remedy erroneous software matches. In fact, to the contrary, the study does not address human observation

[45] For example, the NCRIC and HIDTA policy on Facial Comparison Analysis sets forth that any enhancements to a probe image should be made on a copy, saved separately, and documented to show what enhancements were made, including the date and time of the change and the results of the search (*Facial Comparison Analysis Policy*, HIDTA/NCRIC [Oct. 2021], https://ncric.ca.gov/wp-content/uploads/2021/10/NCRIC-Facial-Comparison-Analysis-Policy.pdf.)

[46] Brendan F. Klare et al., *Facial Recognition Performance: Role of Demographic Information*, 7 IEEE TRANSACTIONS ON INFO. FORENSICS AND SEC. 1789 (2012), https://s3.documentcloud.org/documents/2850196/Face-Recognition-Performance-Role-of-Demographic.pdf.

except to state that "the interaction of machine and human is beyond the scope of this [study], as is human efficacy."[47]

B. Social Network Analysis Tools

While the applicable IUP refers to "social network analysis tools," NYPD's use of such tools, which create network maps illustrating social relationships, is limited. In fact, NYPD uses social *media* analysis technology. This technology searches social media platform (e.g., Facebook, Instagram) content using artificial intelligence, allowing law enforcement to track and monitor publicly available social media content for information relevant to investigations and potential threats.[48]

1. Public Concerns

Public concerns about the use of social media analysis technology centers around the constitutional right to privacy and the ethical implications of law enforcement's use of fake social media accounts. For example, the Brennan Center claims that law enforcement tracking of individuals and political events through social media is an invasion of privacy and violates the public's First Amendment right to free speech. Similarly, the Brennan Center claims that such tracking violates an individual's First Amendment freedom to assemble and protest.[49]

Advocacy groups also expressed concern about law enforcement's use of fake social media accounts to gain access to individuals' posted information and social networks. These groups noted that police used inappropriate lures such as photos of young women to gain access, and pointed out that, once a person 'friends' or 'follows' NYPD's

---

[47] Grother et al., *supra* note 36 at 5.
In response to OIG-NYPD, the Department cited the above National Institute of Standards and Technology (NIST) study as stating that, "the application of facial recognition algorithms can be used as part of a hybrid machine-human system," and that, "the full consideration of systems comprised of automated face search algorithms and human reviewers remains an issue for further academic and operational attention." As noted above, the study references hybrid machine-human systems, but notes that assessing a human reviewer's accuracy and efficiency is "beyond the scope" of the study.
[48] *See generally* JOHN S. HOLLYWOOD, ET AL., THE RAND CORP., USING SOCIAL MEDIA AND SOCIAL NETWORK ANALYSIS IN LAW ENFORCEMENT (2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2301/RAND_RR2301.pdf.
[49] *Statement of Civil Rights Concerns About Monitoring of Social Media by Law Enforcement,* BRENNAN CTR. FOR JUSTICE (Nov. 6, 2019), https://www.brennancenter.org/our-work/research-reports/statement-civil-rights-concerns-about-monitoring-social-media-law.

fake account, the Department may then scan that individual's connections to create lists of affiliations (e.g., to determine whether that individual has potential gang affiliations).[50]

2. Assessment of NYPD's Social Network Analysis Tools IUP

NYPD's IUP concerning "social network analysis tools" presents minimal detail about the capabilities, use, data sharing, and oversight with respect to these types of surveillance technologies. Although not included in the IUP, OIG-NYPD's investigation discovered that the Department uses a specific social media analysis tool to support its investigations and intelligence-gathering functions.[51] For example, in the course of an investigation, NYPD officers may obtain a first name or social media handle for a suspect, and then use the tool to conduct a sweep of major social media platforms for likely matches with that individual suspect in an effort to identify them.

The IUP states that "information accessible to NYPD personnel using social network analysis technology is limited to publicly available information, or information that is viewable as a result of user privacy settings or practices."[52] While this statement is accurate, OIG-NYPD found that the Department also seeks and obtains access to information otherwise shielded by privacy settings by creating fake accounts to which targets of surveillance grant access. Moreover, the Department has publicly disclosed its use of fake accounts in investigations and indicated that guidelines exist around their use.[53] The Office's review found that although these guidelines provide a process

---

[50] *See* Miranda Murillo, Leah Rosenberg & Michael Rebuck, *Undercover Policing in the Age of Social Media,* POLICING PROJECT, NYU SCHOOL OF LAW (December 17, 2018), https://www.policingproject.org/news-main/undercover-policing-social-media; Joseph Goldstein & J. David Goodman, *Frisking Tactic Yields to a Focus on Youth Gangs*, N.Y. TIMES (Sept. 18, 2013), https://www.nytimes.com/2013/09/19/nyregion/frisking-tactic-yields-to-a-focus-on-youth-gangs.html?ref=todayspaper&pagewanted=all&_r=0.

[51] At NYPD's request and based on its position that the name of the social media analysis tool is law enforcement sensitive information, this Report does not include the name.

[52] N.Y.C. POLICE DEP'T., SOCIAL NETWORK ANALYSIS TOOLS: IMPACT AND USE POLICY (Apr. 11, 2021) https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/social-network-analysis-tools-nypd-impact-and-use-policy_4.9.21_final.pdf.

[53] Rocco Parascandola, *New York Police Dept. Issues First Rules for Use of Social Media During Investigations*, N. Y. DAILY NEWS (Sept. 11, 2012), https://www.nydailynews.com/new-york/new-york-police-dept-issues-rules-social-media-investigations-article-1.1157122.

for officers to obtain permission to use fake accounts, the guidelines were not specific to *how* the fake account could be used.

The Department does not create or maintain the records necessary to audit or otherwise review the use of the social media analysis tool. The Department does not maintain a history of investigator activity in the program. The Department does not know whether the company, which owns the program, retains such records. As a practical matter this means that NYPD cannot and does not review the social media sweeps that it conducts with the assistance of the company for potential misuse. This third-party ownership of the data greatly limits NYPD and/or OIG-NYPD's ability to audit officers' use of the technology. It also limits the Department's ability to determine whether its officers' search histories and results are shared with other entities/parties.

VII. Key Findings from Review of All IUPs

The information provided by NYPD in the IUPs largely complies with the requirement**s** of the POST Act legislation. As set out in detail above, the POST Act requires NYPD to publish IUPs that include information relating to ten areas, such as capabilities of the surveillance technologies, rules and guidelines governing their use and access to the collected data. The IUPs largely comply with that requirement because information that relates to these areas is included in each IUP. OIG-NYPD observed, however, that rather than develop policies specific to these surveillance technologies, the IUPs largely restate existing Department policy. With respect to disparate impact, for example, the majority of the IUPs simply refer to NYPD's existing policies concerning the Department's commitment to unbiased enforcement of the law; the IUPs do not explore whether or how a particular surveillance technology might have a disparate impact. In an interview with OIG-NYPD, NYPD specifically stated that, given the way in which the disparate impact section of the POST Act is drafted, NYPD interprets the Act to require disclosure of the potential disparate impact of *the IUP itself* – but not the potential disparate impact of use of the technology (see below sub-section B for examples of these policies).

As noted above, while the IUPs largely comply with the requirements of the POST Act, OIG-NYPD recommends the improvements described herein in order to improve transparency, as well as meaningful public oversight with respect to NYPD's use of surveillance technology, and also to facilitate OIG-NYPD's audit of NYPD's compliance with the IUPs. These improvements would also be consistent with the expectations of those organizations involved in drafting the POST Act, and with the

requirements of similar legislation across the country. In particular, these organizations expressed the view that the IUPs were intended to provide detailed information such as the exact surveillance technologies used, to identify any outside agency that has access to data obtained thereby, and to disclose any potential disparate impacts of the use and deployment of the technology.[54]

As illustrated in OIG-NYPD's section-by-section assessment and in-depth assessments, many of the existing IUPs, while largely complying with the POST Act, do not provide more than a generic level of detail with respect to the above-referenced topics and thus limit meaningful public oversight of NYPD's use of surveillance technologies.

A. NYPD Uses Vague, Non-Specific Boilerplate Language Throughout the IUPs

As previously noted, in many of the sections of the IUPs, NYPD repeatedly used the same boilerplate language to respond to the information requirements of the POST Act. As a reference point, the table in Appendix C illustrates the extent to which NYPD used identical or nearly identical content for many sections of the final 36 IUPs. For example, 83% of the IUPs use essentially the same language in the "Rules, Processes, and Guidelines Relating to Use" section. While boilerplate language may be sufficient to describe rules and processes that are in fact identical, some of the general language at issue here was insufficiently specific and thus failed to provide relevant information to the public. For example, the IUPs use the same language to describe access to information, without addressing circumstances in which a third-party vendor that supplies a particular technology may have access to the data collected by that technology. NYPD also used boilerplate language to address the Health and Safety component of the technologies, despite readily available individualized information for certain technologies, such as the FCC's potentially hazardous electromagnetic interference classification for electronic devices. This sort of general language also fails to provide clear direction to NYPD — for example with respect to what access is permissible on the part of third-party vendors — and hinders OIG-NYPD's ability to conduct meaningful audits of compliance with the IUPs.

[54] *See Coalition of Advocates and Academics Submit Joint Comments Documenting the NYPD's Failure to Comply with the POST Act*, BRENNAN CTR. FOR JUSTICE (Feb. 24, 2021), https://www.brennancenter.org/our-work/research-reports/coalition-advocates-and-academics-submit-joint-comments-documenting-nypds.

1. External Entities' Access to Data

For all categories of surveillance technologies, the IUP sections titled "External Entities," include the same boilerplate language and very little additional information. The POST Act requires information concerning, "whether entities outside the [D]epartment have access to the information and data collected by such surveillance technology, including: (1) whether the entity is a local governmental entity, state governmental entity, federal governmental entity or a private entity, (2) the type of information and data that may be disclosed by such entity, and (3) any safeguards or restrictions imposed by the [D]epartment on such entity regarding the use or dissemination of the information collected by such surveillance technology."[55]

The IUPs for all categories of surveillance technologies address the first requirement by stating: "Government agencies at the local, state, and federal level, including law enforcement agencies other than NYPD, have limited access to NYPD computer and case management systems. Such access is granted by NYPD on a case-by-case basis subject to the terms of written agreements between NYPD and the agency receiving access to a specified system." While this policy statement largely complies with the POST Act by addressing the types of entities with access to surveillance technology data, it is so broad and general that it fails to convey to the public any specific information about the agencies that can access the relevant data. The public would benefit from additional transparency with respect to those agencies that can be granted access to the data, at an appropriate level of generality so as to protect law enforcement sensitive or confidential information. Furthermore, NYPD does not meet the POST Act's second requirement because the IUPs generally do not specify the type of information and data that may be disclosed by such entity. NYPD should begin complying with the provision of the POST Act by providing such information going forward.

Moreover, NYPD includes boilerplate language in numerous IUPs that states "[t]he terms of the written agreements also charge these external entities with maintaining the security and confidentiality of information obtained from NYPD, limiting disclosure of that information without NYPD approval." However, NYPD does not satisfy the third requirement with this language because the IUP does not set forth the particular safeguards and restrictions imposed on each entity with respect to the information to which that entity has access.

[55] POST Act, *supra* note 5.

Additionally, the third-party ownership of some of NYPD's surveillance technologies (e.g., FRT, social media analysis tools) presents challenges to the maintenance of NYPD safeguards and restrictions on the use or dissemination of data, as well as to transparency and oversight with respect to what entities can access data. In light of third-party ownership, it is possible that data generated by certain technologies may be owned, shared, and sold by the third-party owners of the technology, overriding NYPD's control of data sharing and access. A vendor's right of access and disclosure of the data is generally included within the agreements between NYPD and the vendors that supply the technology, and may be limited by such agreements. But, to take just one example, the Department was unable to produce the third-party vendor's Terms of Use agreement for its social network analysis tools provider because it had arranged the purchase through the New York Department of Information Technology & Telecommunications ("DoITT"). Furthermore, the Department was unable to supply the terms and conditions or other information concerning these vendor's access. Without this agreement (or the terms of the agreement) in hand, it is unclear to OIG-NYPD how the Department could comprehensively report on data access by external entities in the IUP.

2. Health and Safety Reporting

The Act directs NYPD to provide information in the IUPs concerning, "any tests or reports regarding the health and safety effects of the surveillance technology." The IUPs use boilerplate language to address this issue, stating, in 33 of 36 IUPs (92%), that "there are no known health and safety issues with [technology name] or associated equipment." OIG-NYPD asked what efforts, if any, the Department made to learn about health and safety issues related to its surveillance technologies; NYPD responded that the Department did not conduct any new research. Although NYPD stated that it was not aware of any health and safety issues, it also made no effort to determine whether any tests or reports existed concerning the health and safety effects of specific surveillance technologies, nor did it review any such tests or reports in connection with the preparation of the IUPs. It is also unclear what efforts the Department previously made in this regard.

3. Retention, Access, and Use of the Data

For the IUP section on "Policies and Procedures Relating to Retention, Access & Use of the Data," NYPD is required to provide information about how data is held and used. NYPD's boilerplate response in this section begins by describing two sources of regulations concerning records retention generally: The Retention and Disposition

Schedule for New York Local Government Records; and the NYC Department of Records and Information Services supplemental records retention and disposition schedule.

NYPD's IUPs do not consistently explain which record retention policy applies for each technology. For example, NYPD's IUP for LPRs states "[d]ata collected through NYPD's LPRs is retained for five (5) years." But the IUP also references a scale of different retention periods applicable to "case investigation records;" the retention period depends on the nature of the investigation at issue. Within this section of the IUP, the Department lists 15 different types of offenses along with the record retention period. For example, case investigation records classified as a violation or traffic infraction must only be retained for one year after the case is closed. The IUP does not explain whether the five-year retention period applies or whether (and when) LPR data is subject to the case investigation retention period. At a minimum, the IUP should explain the method by which surveillance technology data is categorized for purposes of applying these record retention policies – for example, how is it determined whether the data gathered through use of a surveillance technology qualifies as a "case investigation record" of a particular offense type.

B. NYPD Has Interpreted the Requirement to Include Information About Potentially Disparate Impacts in a Narrow Manner

The POST Act requires NYPD to provide information regarding, "any potentially disparate impacts of the surveillance technology [I]mpact and [U]se [P]olicy on any protected groups as defined in the New York City [H]uman [R]ights [L]aw." In response, for all IUPs, the Department begins the disparate impacts section with: "The safeguards and audit protocols built into this [I]mpact and [U]se [P]olicy for [insert surveillance technology name] mitigate the risk of impartial [sic] and biased law enforcement." Additionally, in 31 of the 36 IUPs, the disparate impact section offers the above statement and little more than boilerplate language about NYPD's commitment to impartial enforcement of the law, while only five IUPs present the potential disparate impacts of the use of the technology.

The Department explained that it interpreted the Act, and in particular the reference to "disparate impacts of the surveillance technology [I]mpact and [U]se [P]olicy," to require disclosure of the potential disparate impact of *the IUP itself* – not the potential disparate impact of use of the technology.[56] While the language in the IUPs

[56] NYPD is prohibited by law from writing a policy (including IUPs) that would be biased against legally protected groups.

may largely comply with the POST Act's requirement, OIG-NYPD recommends that NYPD provide information about the potential disparate impact arising from the *use of the technology*, in the interests of transparency and so that NYPD can assure the public that any potential disparate impacts are being considered and addressed.

C. NYPD Has Grouped Related Tools Together in a Way That Limits Public Oversight

While NYPD claims that there are published IUPs applicable to all surveillance technologies as defined by the POST Act, NYPD stated that certain published IUPs cover groups of similar technologies, as opposed to individual technologies. That is, because of the similarity and overlap of some surveillance technologies, NYPD claimed that it was appropriate to group the technologies under a single IUP that described their general capabilities and use (e.g., Data Analysis Tools, Audiovisual Recording Devices, Situational Awareness Cameras). According to NYPD, grouping similar technologies together was also more efficient and facilitated its ability to meet the mandated 180-day deadline. The Department also stated that grouping similar technologies improved the effectiveness of the IUPs by limiting the number of repetitive policies that needed to be memorized by operational NYPD staff.

This approach poses a risk that groupings of technologies could shield individual technologies from public scrutiny and oversight. For example, there is no individual IUP for Digidog, a robot in the form of a dog with mounted microphones and cameras, which NYPD piloted in live operations on several highly publicized occasions.[57] Digidog was grouped into the IUP for Situational Awareness Cameras. As a result, the unique mobility capabilities, safety concerns, third-party ownership, and potential disparate impacts associated with Digidog, if any, were not disclosed to the public or City Council. Other technologies may be similarly shielded from disclosure by grouping.

[57] Mihir Zaveri, *N.Y.P.D. Robot Dog's Run is Cut Short after Fierce Backlash*, N.Y. TIMES (May 11, 2021), https://www.nytimes.com/2021/04/28/nyregion/nypd-robot-dog-backlash.html.

It is the OIG-NYPD's position that the most logical reading of the POST Act's language is that it requires an IUP for each surveillance technology.[58] Moreover, NYPD's interpretation of the POST Act that permits grouping significantly undermines other requirements of the Act. For example, grouping may enable NYPD to bypass the POST Act's disclosure requirements for new technologies. That is, NYPD's grouping approach could allow NYPD to introduce new technologies under an existing group category covered by an existing IUP, and begin use immediately without the required notification to the public and City Council. This allows NYPD to avoid the public notification process – a critical aspect of the POST Act – and thus cannot have been the intent of the legislation.[59]

Grouping also poses a practical barrier to OIG-NYPD's obligations and duties under the POST Act. When OIG-NYPD discussed this grouping strategy with the Department, NYPD stated that it had compiled an internal itemized list of its surveillance technologies to assemble the groups, and this list could be used to audit compliance with the POST Act. OIG-NYPD reviewed this list but the list did not include information concerning the functionality/capability of each technology — information necessary to assess whether the functionalities of various technologies are in fact the same. Without that level of detail, OIG-NYPD cannot assess whether NYPD has issued an IUP that covers each technology with distinct functionalities/capabilities. Furthermore, the list that OIG-NYPD received itself grouped various surveillance technologies. Therefore, due to the limited information provided by NYPD, it is not possible for OIG-NYPD to assess whether the grouping strategy allows for sufficient compliance with the POST Act, and whether NYPD is, in fact, issuing IUPs with respect to each individual surveillance technology (or functionality). OIG-NYPD recommends NYPD discontinue its practice of grouping.

[58] This reading also is supported by the language of the POST Act. It defines an IUP with reference to "*a* surveillance technolog*y*", the singular form of the noun, not "*the* surveillance technolog*ies*." N.Y.C. Admin. Code § 14-188(a) (emphasis added). Further, the definition of surveillance technology also uses a sentence structure that presumes the singular form of technology "that *is* operated by [NYPD]" as opposed to the plural form of technologies "that *are* operated by [NYPD]." *See id.* (emphasis added).

[59] If the POST Act allowed for grouping in the manner described, then the language in N.Y.C. Admin. Code § 14-188(b) mandating a 90-day waiting period before the use of new technology would appear to be unnecessary. In addition, N.Y.C. Admin. Code § 14-188(d) provides a separate path for addendums, thus the POST Act clearly distinguishes between the enhancement of existing technology and the acquisition of entirely new technology. This distinction suggests that the POST Act was not intended to allow grouping.

To the extent that the POST Act is ambiguous, OIG-NYPD's recommendations would benefit from codification from City Council to provide further clarity.

VIII. Recommendations

Based on the findings of this Report, OIG-NYPD makes the following recommendations:[60]

1. NYPD should issue an IUP for each individual surveillance technology, as opposed to continuing its practice of grouping similar technologies under a single IUP.

2. NYPD should identify in each IUP each external agency, by name, with which the Department can share surveillance data.

3. NYPD should include in each IUP the specific safeguards/restrictions on use or dissemination of the surveillance data, for each external agency with which the Department can share such data.

4. NYPD should include in each IUP the potential disparate impacts on protected groups of the use and deployment of the surveillance technology itself.

5. NYPD should revise the Health & Safety Reporting sections of all published IUPs, to include any safety hazards that are identifiable on the basis of existing research, manufacturer warnings, or evaluations by experts in the field, or to state that no such hazards have been identified after a search for relevant information.

6. Within 180 days, NYPD should convene a working group of NYPD personnel, relevant City Council members or their appointees, and representatives from select advocacy groups and community organizations who have expertise in surveillance technologies. The purpose of the working group is to make recommendations to NYPD on necessary updates to the existing IUPs and on any information that should be included in any future IUPs for new technologies, based on the group's expertise. NYPD's procedures applicable to the working group should ensure the protection of sensitive information as appropriate.

[60] Note that no recommendation requires NYPD to reveal information classified as sensitive to the public.

7. Within 180 days, NYPD should create an internal tracking system for every instance in which NYPD provides an external agency with data collected via surveillance technologies that NYPD controls, including the name of the agency and the date of that the data was provided.

8. Within 90 days, in order to facilitate OIG-NYPD's statutorily obligated audit under the POST Act, NYPD should provide OIG-NYPD with information indicating, for each surveillance technology, the various types of data collected and which NYPD units maintain that information. NYPD should include information about the retention procedures and practices for each type of data collected so that OIG-NYPD can assess NYPD's compliance with the IUPs.

9. NYPD should provide OIG-NYPD with any data access and retention policies that are included in the existing contracts with vendors who supply the surveillance technologies used by NYPD.

10. NYPD should provide OIG-NYPD with the data access and retention policies contained in any newly executed contracts with surveillance technology vendors by the 15th of each quarter (i.e., January, April, July, and October).

11. Within 30 days, NYPD should provide OIG-NYPD an itemized list of the surveillance technologies that it uses. This list should include information concerning the functionalities of each technology, so that OIG-NYPD can assess whether NYPD has, in fact, issued an IUP that covers each surveillance technology that has a distinct functionality or capability.

12. NYPD should create written policies establishing guidelines to specify the modifications that can be made to probe images used for Facial Recognition Technology.

13. NYPD should conduct periodic audits of its Facial Identification Section's use of facial recognition technology to ensure compliance with its policies related to the use of the technology and its data. This auditing process should be memorialized in writing.

14. To facilitate the OIG-NYPD's mandated annual audits, beginning January 15, 2023, NYPD should provide OIG-NYPD with quarterly updates, reflecting newly acquired or discontinued technologies in an itemized list of the surveillance

technologies that it uses. Thereafter, updates should be made available by the 15th of each quarter (i.e., January, April, July, and October).

15. NYPD should issue a press release announcing the publication, related public comment period of any new IUPs, and subsequently publish the press release on its website.

IX. Appendix A: Text of POST Act Legislation

The New York City Council

City Hall
New York, NY 10007

Legislation Text

File #: Int 0487-2018, **Version:** A

Int. No. 487-A

By Council Members Gibson, Rosenthal, Levine, Reynoso, Cumbo, Dromm, Kallos, the Public Advocate (Mr. Williams), Chin, Lander, Miller, Lancman, Rivera, Adams, Moya, Levin, Barron, Ayala, Cornegy, Powers, Louis, Brannan, Menchaca, Perkins, Rose, Ampry-Samuel, Treyger, Torres, Van Bramer, Rodriguez, Richards, Gjonaj, Constantinides, Salamanca, Cabrera, Vallone, Cohen and the Speaker (Council Member Johnson)

A Local Law to amend the administrative code of the city of New York, in relation to creating comprehensive reporting and oversight of New York city police department surveillance technologies

Be it enacted by the Council as follows:

Section 1. Chapter 1 of title 14 of the administrative code of the city of New York is amended by adding a new section 14-188 to read as follows:

§ 14-188 Annual surveillance reporting and evaluation. a. Definitions. As used in this section, the following terms have the following meanings:

Surveillance technology. The term "surveillance technology" means equipment, software, or systems capable of, or used or designed for, collecting, retaining, processing, or sharing audio, video, location, thermal, biometric, or similar information, that is operated by or at the direction of the department. Surveillance technology does not include:

1. routine office equipment used primarily for departmental administrative purposes;

2. parking ticket devices;

3. technology used primarily for internal department communication; or

4. cameras installed to monitor and protect the physical integrity of city infrastructure.

Surveillance technology impact and use policy. The term "surveillance impact and use policy" means a written document that includes the following information:

File #: Int 0487-2018, **Version:** A

1. a description of the capabilities of a surveillance technology;

2. rules, processes and guidelines issued by the department regulating access to or use of such surveillance technology as well as any prohibitions or restrictions on use, including whether the department obtains a court authorization for such use of a surveillance technology, and, if so, the specific type of court authorization sought;

3. safeguards or security measures designed to protect information collected by such surveillance technology from unauthorized access, including but not limited to the existence of encryption and access control mechanisms;

4. policies and/or practices relating to the retention, access, and use of data collected by such surveillance technology;

5. policies and procedures relating to access or use of the data collected through such surveillance technology by members of the public;

6. whether entities outside the department have access to the information and data collected by such surveillance technology, including: (a) whether the entity is a local governmental entity, state governmental entity, federal governmental entity or a private entity, (b) the type of information and data that may be disclosed by such entity, and (c) any safeguards or restrictions imposed by the department on such entity regarding the use or dissemination of the information collected by such surveillance technology;

7. whether any training is required by the department for an individual to use such surveillance technology or access information collected by such surveillance technology;

8. a description of internal audit and oversight mechanisms within the department to ensure compliance with the surveillance technology impact and use policy governing the use of such surveillance technology;

9. any tests or reports regarding the health and safety effects of the surveillance technology; and

10. any potentially disparate impacts of the surveillance technology impact and use policy on any protected groups as defined in the New York city human rights law.

b. Publication of surveillance technology impact and use policy. The department shall propose a surveillance technology impact and use policy and post such proposal on the department's website, at least 90 days prior to the use of any new surveillance technology.

c. Existing surveillance technology. For existing surveillance technology as of the effective date of the local law that added this section, the department shall propose a surveillance technology impact and use policy and post such proposal on the department's website within 180 days of such effective date.

d. Addendum to surveillance technology impact and use policies. When the department seeks to acquire or acquires enhancements to surveillance technology or uses such surveillance technology for a purpose or in a manner not previously disclosed through the surveillance technology impact and use policy, the department shall provide an addendum to the existing surveillance technology impact and use policy describing such enhancement or additional use.

e. Upon publication of any proposed surveillance technology impact and use policy, the public shall have 45 days to submit comments on such policy to the commissioner.

f. The commissioner shall consider public comments and provide the final surveillance technology impact and use policy to the speaker and the mayor, and shall post it on the department's website no more than 45 days after the close of the public comment period established by subdivision e of this section.

§ 2. Section 803 of the New York city charter is amended by adding a new subdivision c-1 to read as follows:

c-1. The commissioner shall prepare annual audits of surveillance technology impact and use policies as defined in section 14-188 of the administrative code that shall:

1. assess whether the New York city police department's use of surveillance technology, as defined in section 14-188 of the administrative code, complies with the terms of the applicable surveillance technology impact and use policy;

2. describe any known or reasonably suspected violations of the surveillance technology impact and use

policy, including but not limited to complaints alleging such violations made by individuals pursuant to paragraph (6) of subdivision c of this section; and

3. publish recommendations, if any, relating to revisions of any surveillance technology impact and use policies.

§ 3. This local law takes effect immediately.

DA/BG
LS 6645/Int.1482-2017
LS 5531
6/10/20 10:40PM

X. Appendix B: Example of Public Comment Template

XI. Appendix C: Text of NYPD's License Plate Readers IUP

License Plate Readers IUP language, organized by section required by POST Act.

Note: The blue blocked text in each section is repeated across multiple IUPs, as indicated by the below table.

Percent of final 36 IUPs containing identical or nearly identical repetitions of blue blocked text	
Section	**%**
Capabilities of the Technology	No instances of boilerplate language (0%)
Rules, Processes & Guidelines Relating to Use	83%
Safeguard & Security Measures Against Unauthorized Access	92%
Policies & Procedures Relating to Retention, Access & Use of Data	83%
Policies & Procedures Relating to Public Access or Use of Data	94%
External Entities	67%
Training	75%
Internal Audit & Oversight Mechanisms	64%
Health & Safety Reporting	92%
Disparate Impacts of the IUP	86%

Section 1: Capabilities of the surveillance technology

LPRs are specialized cameras that quickly capture images of license plate numbers affixed to vehicles that pass within the LPRs sensory range. An internal processor then converts the image of the license plate into a text the computer can process. This text is automatically compared against administrative databases containing enumerated lists of license plates of interest (i.e. stolen, wanted, etc.). LPRs are capable of properly functioning day or night, and in a variety of weather conditions.

NYPD makes use of two (2) kinds of LPRs: stationary and mobile. Stationary LPRs are permanently affixed to a specific location and record the license plates of all vehicles that pass within the LPR range. Mobile LPRs are attached to various NYPD vehicles and use the same technology to capture images of license plates the vehicle passes as it moves. Both stationary and mobile LPRs record a vehicle's license plate number and state of issuance, an [sic] images of a [sic] vehicle and the license plate, and the date, time and location the vehicle passed the LPR.

NYPD officers operating a NYPD vehicle imbedded with a NYPD tablet1 will receive an alert if the LPR scans a vehicle of interest, such as a vehicle reported stolen.

A limited number of authorized NYPD personnel can access a national commercial LPR data repository. LPR data obtained using NYPD LPRs or through the commercial repository cannot be used to track a vehicle in real-time.

NYPD LPRs do not use any biometric measurement technologies.

NOTE: No instances of repeated or boilerplate language was found in these sections.

Section 2: Rules, Processes, & Guidelines Relating to Use of the Technology

NYPD LPR policy seeks to balance the public safety benefits of this technology with individual privacy. LPRs [are 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.

Court authorization is not sought prior to NYPD use of LPRs. Motor vehicles are heavily regulated by the government. The field-of-view of the LPRs utilized by NYPD is strictly limited to public areas and locations. LPRs capture images of license plates that are readily observable to any member of the public.

NYPD LPRs may only be used for legitimate law enforcement purposes. LPRs do not by themselves establish probable cause for an arrest, but provide NYPD investigators with valuable leads. NYPD limits authorized use of LPRs to the following circumstances: 1. Routine vehicle patrol; 2. Creation of alerts for specified complete

or partial plate numbers; and 3. Capture movement of specified complete or partial plate numbers that momentarily pass the device.

In accordance with the Public Oversight of Surveillance Technology Act, an addendum to this [I]mpact and [U]se [P]olicy will be prepared as necessary to describe any additional uses of LPRs. 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 LPRs will subject employees to administrative and potentially criminal penalties.

NOTE: 30 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

Section 3: Safeguard & Security Measures against Unauthorized Access

LPR data is accessible by using the NYPD Domain Awareness System (DAS)2. 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 to LPR data 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).

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

LPR data can be downloaded and retained in an appropriate NYPD computer or case management system. Only authorized users have access to the data. 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.

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.

NOTE: 33 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

Section 4: Policies & Procedures Relating to Retention, Access & Use of the Data

Data recorded by NYPD LPRs is accessible through DAS. All NYPD authorized users may only access DAS to execute their lawful duties by making official inquiries, which relate only to official business of the NYPD. Historical searches of LPR data may be conducted: 1. To determine if specified complete or partial plate numbers were detected by one or more fixed or mobile LPRs; 2. To identify all complete plate numbers detected by one or more fixed LPR during a specified time period; 3. To identify all complete plate numbers detected by a mobile LPR mounted on one or more specified vehicles during a specified time period; 4. To identify all complete plate numbers detected within a specified area during a specified time period; and 5. To identify preceding or subsequent complete plate numbers associated with one or more specified complete or partial plate numbers detected by one or more fixed or mobile LPRs in order to identify possible associates.

Data collected through NYPD's LPRs is retained for five (5) years. Access to the commercial LPR repository is critically limited and may only be accessed by select NYPD personnel for legitimate law enforcement purposes. The commercial repository will not be used unless there is an articulable reason to believe the queried vehicle has left the boundaries of NYC.

LPR data 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 data will be 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.3 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.

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 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 data will subject employees to administrative and potentially criminal penalties.

NOTE: 30 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

Section 5: Policies & Procedures Relating to Public Access or Use of the Data

Members of the public may request data obtained from the NYPD's use of LPRs 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.

NOTE: 34 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

Section 6: External Entities

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

Other law enforcement agencies may LPR data (sic) from NYPD in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide LPR data 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.

Authorized agents within the state of New Jersey (NJ) have limited access to the NYPD LPR recorded data. Authorized agents of NJ law enforcement agencies are capable of conducting a search for pings of a specific license plate against NYPD owned or accessed LPR readers. However, NJ Authorized Agents do not have access to DAS.

Following the laws of the State and City of New York, as well as NYPD policy, information stemming from LPR use 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 LPRs 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 LPRs 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 LPR data 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.

NOTE: 24 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

Section 7: Training

NYPD officers using LPRs receive command level training on the proper operation of the technology and associated equipment. Officers must operate NYPD LPRs in compliance with NYPD policies and training.

NOTE: 27 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

Section 8: Internal Audit & Oversight Mechanisms

Supervisors of personnel utilizing LPRs 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.

Any search conducted in DAS relating to LPR associated information is auditable by ITB.

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 NYPD Internal Affairs Bureau (IAB).

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 the Information Technology Bureau.

NOTE: 23 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

Section 9: Health & Safety Reporting

There are no known health and safety issues with LPRs or associated equipment.

NOTE: 33 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

Section 10: Disparate Impacts of the Impact & Use Policy

The safeguards and audit protocols built into this [I]mpact and [U]se [P]olicy for LPRs mitigate the risk of impartial [sic] and biased law enforcement. LPRs capture images of vehicle license plates utilizing NYC's public roadways. LPRs do not use any 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. 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.

NOTE: 31 out of 36 IUPs contain identical or nearly identical language as the blue blocked text above in this section.

XII. Appendix D: Text of NYPD's Social Network Analysis Tools IUP

Section 1: Capabilities of the Technology

NYPD social network analysis tools process information on social networking platforms to aid personnel in discovering information relevant to investigations and to address public safety concerns. For example, in the aftermath of a terrorist attack committed outside of New York City, the NYPD may use social network analysis tools to quickly assess the social media profile of the perpetrator for connections to the New York City area and allocate resources in response.

Similarly, social network analysis tools assist the NYPD in addressing criminal activity in New York City. When investigating an assault committed by multiple subjects, social network analysis tools can reveal investigative leads by highlighting otherwise unknown connections between the subjects acting in concert.

However, the NYPD may miss information critical to investigations because users can easily remove information posted on social media and social media platforms routinely delete content and deactivate accounts for violations of terms of service. Accordingly, social network analysis tools allow the NYPD to retain information on social networking platforms relevant to investigations and alert investigators to new activity on queried social media accounts.

Information accessible to NYPD personnel using social network analysis tools is limited to publicly available information, or information that is viewable as a result of user privacy settings or practices. Publically available images may be downloaded and may be used a probe image for facial recognition analysis.1 Social network analysis tools cannot be used for computer hacking, do not perform facial recognition and do not use any other biometric measuring technologies.

Section 2: Rules, Processes & Guidelines Relating to Use of The Technology

NYPD social network analysis tools policy seeks to balance the public safety benefits of this technology with individual privacy. The NYPD must use social network analysis tools 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.

Social network analysis tools may only be used for legitimate law enforcement purposes. Information identified by using social network analysis tools does not by itself establish probable cause to arrest or obtain a search warrant. However, it may generate leads for further investigation.

The NYPD does not seek court authorization prior to using social network analysis tools. The processed information is limited to publicly available information or information that is viewable as a result of user-selected privacy settings or practices.

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 social network analysis tools.

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 activity 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 social network analysis tools will subject employees to administrative and potentially criminal penalties.

Section 3: Safeguard & Security Measures Against Unauthorized Access

Access to social network analysis tools is critically limited. Authorized users are authenticated by username and password. Account credentials for social network analysis tools must be securely maintained and stored at all times. Access to social network analysis tools is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to NYPD social network analysis tools 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 obtained from NYPD social network analysis tools are retained within an appropriate case management or computer systems. 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. Members of the NYPD 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 to any system will subject employees to administrative and potentially criminal penalties.

Section 4: Policies & Procedures Relating to Retention, Access, & Use of The Data

Information obtained from social network analysis tools may only be used for legitimate law enforcement purposes or official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings. Information relevant to a case or investigation is stored electronically in an appropriate NYPD case management and computer 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 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 system will subject employees to administrative and potentially criminal penalties.

Section 5: Policies & Procedures Relating to Public Access or Use of The Data

Members of the public may request information obtained from NYPD use of social network analysis tools 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.

Section 6: External Entities

If the use of social network analysis tools yields information relevant to a criminal case, the NYPD will share it with 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 information 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 information or details 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 information related to social network analysis 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; or

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 social network analysis tools 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 social network analysis tools 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 obtained using NYPD social network analysis tools 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.

Section 7: Training

NYPD personnel using social network analysis tools receive command level training on the proper operation of the technology and associated equipment. All NYPD personnel must use social network analysis tools in compliance with NYPD policies and training.

Section 8: Internal Audit & Oversight Mechanisms

Supervisors of personnel utilizing social network analysis tools 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 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).

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 the Information Technology Bureau.

Section 9: Health & Safety Reporting

There are no known health and safety issues with social network analysis tools or the associated equipment.

Section 10: Disparate Impacts of the Impact & Use Policy

The safeguards and audit protocols built into this impact and use policy for NYPD social network analysis tools mitigate the risk of impartial [sic] and biased law enforcement. Social network analysis tools are only capable of processing information a user chooses to share on social networking platforms. NYPD social network analysis tools do not use any 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.

XIII. Appendix E: Text of NYPD's Facial Recognition IUP

Section 1: Capabilities of the Technology

Since 2011, the NYPD has successfully used facial recognition technology to investigate criminal activity and increase public safety. The NYPD uses facial recognition to aid in the identification of suspects whose images have been recorded on-camera at robberies, burglaries, assaults, shootings, and other serious crimes. The NYPD also uses facial recognition to aid in the identification of persons unable to identify themselves (e.g., persons experiencing memory loss or unidentified deceased persons).

NYPD investigators often obtain video and photo over the course of an investigation. If a video or photo contains an image of a face of an unknown individual, the image can be submitted for facial recognition analysis in accordance with NYPD facial recognition policy.

Known as a probe image, NYPD facial recognition software compares the image to a controlled and limited group of photos already within lawful possession of the NYPD, called the photo repository. The photo repository only contains arrest and parole photographs of individuals that have been charged with a crime where criminal court has jurisdiction. Probe images are never entered into and do not become part of the photo repository.

NYPD facial recognition technology analyzes one probe image at a time. The software generates a pool of possible match candidates that are manually reviewed by specially trained NYPD facial recognition investigators to determine the differences and similarities between a probe image and a potential match.

The NYPD does not integrate facial recognition technology with any NYPD video cameras or systems (e.g., CCTV cameras, unmanned aircraft systems, and body worn cameras) for real-time facial recognition analysis. The NYPD does not have a capability for real-time facial recognition.

Facial recognition technology does not use any additional biometric measuring technologies.

Section 2: Rules, Processes & Guidelines Relating to Use of The Technology

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

The facial recognition process does not by itself establish a basis for a stop, probable cause to arrest, or to obtain a search warrant. However, it may generate investigative leads through a combination of automated biometric comparisons and human analysis.

Facial recognition technology must only be used for legitimate law enforcement purposes. Authorized uses of facial recognition technology are limited to the following:

1. To identify an individual when there is a basis to believe that such individual has committed, is committing, or is about to commit a crime;

2. To identify an individual when there is a basis to believe that such individual is a missing person, crime victim, or witness to criminal activity;

3. To identify a deceased person;

4. To identify a person who is incapacitated or otherwise unable to identify themselves;

5. To identify an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else's identification, or a false identification; or

6. To mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot).

For criminal investigations, a possible facial recognition match serves as a lead for additional steps. An arrest will not be made until the assigned investigator establishes, with other corroborating evidence, that the suspect identified as a possible match is the perpetrator in an alleged crime.

When an investigator obtains an image depicting the face of an unidentified suspect, victim, or witness, and intends to identify the individual using facial recognition technology, the investigator must submit a request for facial recognition analysis. Specifically, the request is made for the image depicting the face of the unknown person (the probe image) to be compared to photos in the NYPD arrest and parole photo repository. The request for facial recognition analysis must include a case or complaint number for the matter under investigation and the probe image(s) of the unidentified person.

The facial recognition investigator must confirm the basis of the request is in compliance with the enumerated list authorized uses of facial recognition technology. That confirmation must be documented by the requesting investigator in an appropriate NYPD case management system. The facial recognition investigator will select a probe image of the unidentified person from the submitted images. If image quality is unsuitable for facial recognition comparison, the requesting investigator will be notified and given the opportunity to submit additional images.

The facial recognition investigator will run a search using a facial recognition software for comparison of the probe image to images lawfully obtained by the NYPD. The software generates a pool of possible match candidates.

If a possible match candidate is identified, the facial recognition investigator must then manually review and analyze each result. This process, known as facial identification, consists of visual comparison of the facial characteristics of each candidate against the probe image. Comparisons are made with regard to various facial features such as the eyes, ears, nose, mouth, chin, lips, eyebrows, hair/hairline, scars, marks, and tattoos. A detailed background check is conducted by the facial recognition investigator to corroborate a possible match.

Next, a possible match candidate is submitted for peer review by other facial recognition investigators. A supervisor of the facial recognition investigator performs a final review of a possible match candidate and provides final approves, if appropriate.

If there is a difference of opinion with the findings, the supervisor will direct personnel to continue investigation for a possible match candidate. A report of negative results will be provided to the requesting investigator if a possible match candidate is not identified or approved by the supervisor.

If a possible match candidate is approved, the facial recognition investigator will prepare a possible match report and attach it to the requesting investigator's case file in the case management system. The possible match report includes the probe image, a notification stating that the determination of a possible match candidate alone does not constitute probable cause to effect an arrest or obtain an arrest or search warrant, and that further investigation is needed to establish probable cause.

Images obtained from body-worn cameras worn by NYPD officers are not routinely submitted for facial recognition analysis. For example, the NYPD does not use facial recognition technology to examine body-worn camera video to identify people who may have open warrants. However, if an officer, whose body-worn camera is activated, witnesses a crime but is unable to apprehend the suspect, a still image of

the suspect may be extracted from body-worn camera video and submitted for facial recognition analysis.

The NYPD does not use facial recognition technology to monitor and identify people in crowds or political rallies.

The NYPD does not seek court authorization prior to the use of facial recognition technology since the tool conducts analysis of images that have been lawfully-obtained by the NYPD.

The use of facial recognition technology that compares probe images against images outside the photo repository is prohibited unless approval is granted for such analysis in a specific case for an articulable reason by the Chief of Detectives or Deputy Commissioner, Intelligence and Counterterrorism.

In situations where use of a NYPD facial recognition technology has not been foreseen or prescribed in policy, the Chief of Detectives or Deputy Commissioner of Intelligence and Counterterrorism, will decide if use 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 facial recognition technology.

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 facial recognition technology will subject employees to administrative and potentially criminal penalties.

Section 3: Safeguard & Security Measures Against Unauthorized Access

Access to facial recognition technology is limited to NYPD facial recognition investigators. Access to facial recognition technology is removed when the technology is no longer necessary for NYPD personnel to fulfill their duties (e.g., when facial recognition investigators are transferred to a different command).

Facial recognition investigators using the software are first authenticated by username and password. Facial recognition investigators are provided with access only after completing mandatory training related to use of the technology.

Information resulting from use of facial recognition technology is retained within 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. 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.

Section 4: Policies & Procedures Relating to Retention, Access, & Use of The Data

The results of facial recognition analysis 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. Facial recognition analysis results relevant to a case or investigation are stored in appropriate NYPD computer or case management systems. These results 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.

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.1 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.2

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 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 information will subject employees to administrative and potentially criminal penalties.

Section 5: Policies & Procedures Relating to Public Access or Use of The Data

Members of the public may request information obtained from the NYPD use of facial recognition technology 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.

Section 6: Eternal Entities

If the use of facial recognition technology produces information related to a criminal case, the NYPD will turn it 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 information 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 information to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Such information will not be shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, information stemming from facial recognition technology 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 facial recognition technology 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 facial recognition technology associated program 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 facial recognition data 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.

Section 7: Training

NYPD personnel utilizing facial recognition technology receive training on facial recognition technology, image comparison principles, the proper operation of the technology and associated equipment. NYPD personnel must use facial recognition technology in compliance with NYPD policies and training.

Section 8: Internal Audit & Oversight Mechanisms

The use of facial recognition technology, including the reasons for its use, must be discussed with a supervisor. Supervisors of personnel utilizing facial recognition technology 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 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).

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 the Information Technology Bureau.

Section 9: Health & Safety Reporting

There are no known health and safety issues with facial recognition technologies or associated equipment.

Section 10: Disparate Impacts of The Impact & Use Policy

The safeguards and audit protocols built into this impact and use policy for facial recognition technology mitigate the risk of impartial [sic] and biased law enforcement. NYPD facial recognition policy integrates human investigators in all phases. All possible facial recognition matches undergo a peer review by other facial recognition investigators. Further, the possible match report includes the probe image, a notification stating that the determination of a possible match candidate alone does not constitute probable cause to effect an arrest or obtain an arrest or search warrant, and that further investigation is needed to establish probable cause.

Some studies have found variations in accuracy for some software products in analyzing the faces of African Americans, Asians Americans, women, and groups other than non-white males. However, an important federal government study on the subject noted that in "hybrid machine/human systems," where the software findings are routinely reviewed by human investigators, erroneous software matches can be swiftly corrected by human observers.

Facial recognition technology utilizes algorithms in order to identify possible match candidates to a probe image. The NYPD only uses facial recognition algorithms which have been evaluated by the National Institute of Standards and Technology (NIST) for matching efficiency and accuracy, which includes an evaluation of the accuracy of the algorithm across demographics. Algorithms utilized for facial recognition are periodically updated as necessary based on subsequent NIST evaluations.

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 initiate 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.

The City of New York
Department of Investigation

JOCELYN E. STRAUBER
COMMISSIONER

180 MAIDEN LANE
NEW YORK, NY 10038
212-825-5900

Release #08-2022
nyc.gov/doi

FOR IMMEDIATE RELEASE
THURSDAY, MARCH 31, 2022

CONTACT: DIANE STRUZZI
(212) 825-5931

EIGHTH ANNUAL REPORT ISSUED BY
DOI'S OFFICE OF THE INSPECTOR GENERAL FOR THE NEW YORK CITY POLICE DEPARTMENT

Today, the Department of Investigation's ("DOI") Office of the Inspector General for the New York City Police Department ("OIG-NYPD") released its Eighth Annual Report, which reviews the OIG-NYPD's completed investigations and systemic reviews to date, and analyzes the extent to which the New York City Police Department ("NYPD") has adopted or rejected its recommended proposals for reform. Approximately 82 percent of OIG-NYPD's 185 recommendations issued to NYPD, spanning 17 investigative reports since 2015, have been implemented, partially implemented, or accepted in principle by NYPD. A copy of the Annual Report is attached to this release and can be found at the following link: http://www1.nyc.gov/site/doi/newsroom/public-reports.page.

DOI Commissioner Jocelyn E. Strauber said, "This Annual Report provides critical transparency with respect to NYPD's handling of the matters we have examined and the recommendations we have issued and it demonstrates that NYPD has embraced the vast majority of improvements we have proposed in our public reports. This report also reflects that since its creation in 2014, OIG-NYPD has undertaken significant work on a range of policing issues that impact New York City."

Acting Inspector General Jeanene Barrett said, "The OIG-NYPD is dedicated to increasing public confidence in NYPD by conducting investigations and issuing recommendations aimed at enhancing the Police Department's effectiveness. This Annual Report demonstrates the broad array of issues we have tackled over the past seven years and the impact on NYPD. We are proud to issue this Report furthering transparency on policing in New York City."

The Annual Report provides a chart detailing NYPD's implementation status for all 185 recommendations issued in 17 investigative reports. The OIG-NYPD will continue to monitor the implementation status of these recommendations and issue follow-up reports as necessary.

While the pandemic and resulting impact on the City and its operations slowed OIG-NYPD's ability to advance investigations in 2021, highlights from 2021 noted in the Annual Report include:

- A report concerning "Sharing Police Body-Worn Camera Footage in New York City." This is the third report issued pursuant to Local Law 166, which instructs OIG-NYPD to "work[] with the law department, the comptroller, the police department, the civilian complaint review board, the commission to combat police corruption, and the commission on human rights [to] collect and evaluate information regarding allegations or findings of improper police conduct and develop recommendations relating to the … operations, policies, programs, and practices of the police department." This 2021 report examined the information-sharing procedures of the Police Department with the noted oversight agencies, specifically with respect to Body-Worn Camera ("BWC") footage. The report concluded that each agency has different procedures for requesting, accessing, and retaining NYPD BWC footage and that the current procedures do not provide

more

every agency with the appropriate level of access needed to perform their respective duties. Among other things, OIG-NYPD recommended that NYPD consult the six police oversight agencies, including OIG-NYPD, to determine whether additional access to BWC footage would benefit them in fulfilling their mandates, which the NYPD accepted. The NYPD rejected OIG-NYPD's recommendation that the Police Department provide the Civilian Complaint Review Board ("CCRB") with independent and direct remote access credentials to its BWC storage databases so BWC videos can be searched, viewed, and used as appropriate in CCRB's investigations of police misconduct.

- In 2021, as outreach activities transitioned back to in-person, OIG-NYPD met with community groups, engaged in public forums hosted by elected officials, and attended numerous precinct community council meetings. The OIG-NYPD's outreach work extends beyond New York City. For example, in 2021, OIG-NYPD's then-Inspector General presented to law enforcement officers in Mexico working in the field of police oversight. The OIG-NYPD continues to undertake outreach work in order to obtain feedback and build relationships with the public that support its mission of increasing public safety, protecting civil liberties and civil rights, and strengthening public confidence in the Police Department, all to build stronger police-community relations.

The OIG-NYPD Annual Report is mandated by Local Law 70, which calls for a summary report to be issued annually on April 1. To read more about Local Law 70, click here.

The Eighth Annual Report was compiled by DOI's Office of the Inspector General for the NYPD, specifically, Data Analyst Sara Hassan and Senior Auditor Renell Grant, under the supervision of Deputy Inspector General Percival Rennie and Acting Inspector General Jeanene Barrett.

New York City
Department of Investigation

Office of the Inspector General for the NYPD (OIG-NYPD)

EIGHTH ANNUAL REPORT
OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD

Jocelyn Strauber
Commissioner

Jeanene Barrett
Acting Inspector General for the NYPD

March 2022

Table of Contents

I. INTRODUCTION 1

II. 2021 OFFICE OF THE INSPECTOR GENERAL FOR THE NEW YORK CITY POLICE DEPARTMENT ACTIVITIES 5

A. *SYSTEMIC INVESTIGATIONS, REVIEWS, STUDIES, AND AUDITS: RECOMMENDATIONS AND NYPD RESPONSES* 5

i. Sharing Police Body Worn Camera Footage in New York City (November 2021) 5

B. *COMMUNITY OUTREACH AND ENGAGEMENT* 8

C. *COMPLAINTS* 9

III. 2015-2020 SYSTEMIC INVESTIGATIONS, REVIEWS, STUDIES, AND AUDITS: UPDATED NYPD RESPONSES TO RECOMMENDATIONS 10

A. Investigation Into NYPD Response To The George Floyd Protests (December 2020 Report) 10

B. An Investigation Of NYPD's Officer Wellness And Safety Services (September 2019 Report) 12

C. Complaints of Biased Policing in New York City: an Assessment of NYPD's Investigations, Policies, And Training (June 2019 Report) 15

D. 2019 Assessment of Litigation Data Involving NYPD (April 2019 Report) 23

E. Ongoing Examination Of Litigation Data Involving NYPD (April 2018 Report) 25

F. An Investigation of NYPD's Special Victims Division—Adult Sex Crimes (March 2018 Report) 27

G. An Investigation of NYPD's New Force Reporting System (February 2018 Report) 31

H. Review of NYPD's Implementation of Patrol Guide Procedures Concerning Transgender and Gender Nonconforming People (November 2017 Report) 36

I. When Undocumented Immigrants Are Crime Victims: an Assessment of NYPD's Handling of U Visa Certification Requests (July 2017 Report) 39

J. Addressing Inefficiencies in NYPD's Handling of Complaints: An Investigation of the "Outside Guidelines" Complaint Process (February 2017 Report) 42

K. Putting Training Into Practice: A Review of NYPD's Approach to Handling Interactions with People in Mental Crisis (January 2017 Report) 44

L. An Investigation of NYPD's Compliance with Rules Governing Investigations of Political Activity (August 2016 Report) 47

M. An Analysis of Quality-of-Life Summonses, Quality-of-Life Misdemeanor Arrests, and Felony Crime in New York City, 2010-2015 (June 2016 Report) 49

N. Police Use of Force in New York City: Findings and Recommendations on NYPD's Policies and Practices (October 2015 Report) 52

O. Body-Worn Cameras in New York City: An Assessment of NYPD's Pilot Program and Recommendations to Promote Accountability (July 2015 Report) 54

P. Using Data from Lawsuits and Legal Claims Involving NYPD to Improve Policing (April 2015 Report) 57

Q. Observations on Accountability and Transparency in Ten NYPD Chokehold Cases (January 2015 Report) 59

IV. APPENDIX A: RECOMMENDATIONS IMPLEMENTED OR NO LONGER APPLICABLE PRIOR TO 2021 60

I. INTRODUCTION

This is the Eighth Annual Report of the New York City Department of Investigation's (DOI) Office of the Inspector General for the New York City Police Department (OIG-NYPD or the Office). This Report summarizes the findings of systemic reviews conducted from 2015 through 2021 and assesses the extent to which the New York City Police Department (NYPD or the Department) has implemented OIG-NYPD's proposals for reform. This Report also discusses complaints the Office has received from the public, as well as its community outreach and engagement efforts.

DOI's OIG-NYPD is charged with external, independent review of NYPD.

Pursuant to Chapter 34 of the New York City Charter and Mayoral Executive Order 16, DOI's OIG-NYPD is charged with external, independent review of NYPD.[1]

The Office publishes written, publicly available reports based on its investigations, reviews, studies, and audits. The NYPD Commissioner is required to submit a written response to each published report within 90 days.[2]

This Report examines NYPD's implementation of the recommendations made in OIG-NYPD's investigative reports and classifies the statuses of those recommendations into the following categories:

- **Implemented or Partially Implemented (I or PI):** NYPD has accepted and implemented these recommendations completely or in part.
- **Accepted in Principle (AIP):** NYPD has agreed with the general intent of these recommendations but has not yet implemented them.
- **Under Consideration (UC):** NYPD has not yet decided whether to adopt or reject these recommendations.
- **Rejected (R):** NYPD does not agree with the recommendations and will not implement them.
- **No Longer Applicable (NLA):** Due to a change in technology or procedure by NYPD, these recommendations are no longer relevant. OIG-NYPD will

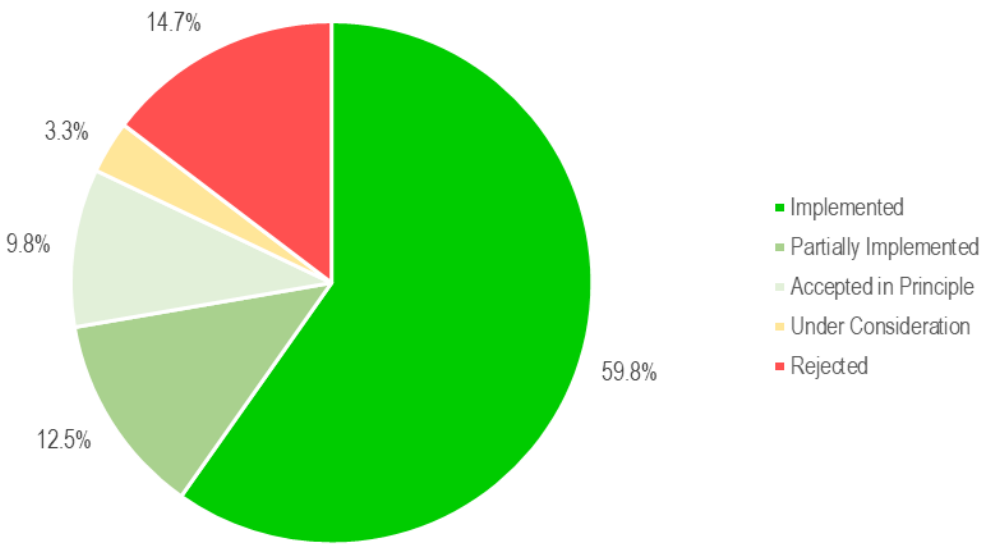
[1] The New York City Charter, as amended by Local Law 70 of 2013, empowers the DOI Commissioner to "investigate, review, study, audit and make recommendations relating to the operations, policies, programs and practices, including ongoing partnerships with other law enforcement agencies, of the New York city police department with the goal of enhancing the effectiveness of the department, increasing public safety, protecting civil liberties and civil rights, and increasing the public's confidence in the police force, thus building stronger police-community relations." N.Y.C. Charter § 803(c)(1).

[2] OIG-NYPD's reports and NYPD responses are available at: http://www1.nyc.gov/site/doi/offices/oignypd.page

continue to monitor these recommendations for future applicability as policies and procedures change.

In total, OIG-NYPD's 17 investigative reports from 2015-2021 contain 187 recommendations; 184 of those are currently applicable to the Department.[3] As depicted in the table and chart below, NYPD has implemented, partially implemented, or accepted in principle 82.1% of these 184 recommendations (59.8% have been implemented, 12.5% have been partially implemented, and 9.8% have been accepted in principle).

Status of Recommendations Applicable to NYPD



[3] The total count of 187 recommendations made by OIG-NYPD includes two recommendations addressed exclusively to CCRB and one recommendation that is no longer applicable to the Department.

Table 1: Status of Recommendations Addressed to NYPD

Report	I	PI	AIP	UC	R	NLA
Sharing Police Body-Worn Camera Footage In New York City (November 2021)	0	0	1	0	2	0
An Investigation of NYPD's Officer Wellness and Safety Services NYPD (September 2019 Report)	8	1	1	2	0	0
Complaints of Biased Policing in New York City: An Assessment of NYPD's Investigations, Policies, and Training (June 2019 Report)	8	0	3	0	10	0
2019 Assessment of Litigation Data Involving NYPD (April 2019 Report)	0	1	1	2	0	0
Ongoing Examination of Litigation Data Involving NYPD (April 2018)	1	2	0	0	2	0
An Investigation of NYPD's Special Victims Division-Adult Sex Crimes (March 2018)	5	4	2	1	0	0
An Investigation of NYPD's New Force Reporting System (February 2018)	17	4	1	0	2	1
Review of NYPD's Implementation of Patrol Guide Procedures Concerning Transgender and Gender Nonconforming People (November 2017)	5	0	2	0	2	0
When Undocumented Immigrants Are Crime Victims: An Assessment of NYPD's Handling of U Visa Certification Requests (July 2017)	3	3	2	0	2	0
Addressing Inefficiencies in NYPD's Handling of Complaints: An Investigation of the "Outside Guidelines" Complaint Process (February 2017)	3	2	0	1	0	0
Putting Training into Practice: A Review of NYPD's Approach to Handling Interactions with People in Mental Crisis (January 2017)	11	2	0	0	0	0
An Investigation of NYPD's Compliance with Rules Governing Investigations of Political Activity (August 2016)	6	0	2	0	3	0
An Analysis of Quality-of-Life Summonses, Quality-of-Life Misdemeanor Arrests, and Felony Crime in New York City, 2010-2015 (June 2016)	4	0	0	0	3	0
Police Use of Force in New York City: Findings and Recommendations on NYPD's Policies and Practices (October 2015)	12	2	1	0	0	0
Body-Worn Cameras in New York City: An Assessment of NYPD's Pilot Program and Recommendations to Promote Accountability (July 2015)	20	0	2	0	1	0
Using Data from Lawsuits and Legal Claims Involving NYPD to Improve Policing (April 2015)	3	2	0	0	0	0
Observations on Accountability and Transparency in Ten NYPD Chokehold Cases (January 2015)	4	0	0	0	0	0
Total	110	23	18	6	27	1

I = Implemented, PI = Partially implemented, AIP = Accepted in principle, UC = Under consideration, R = Rejected, NLA = No Longer Applicable

NYPD's acceptance and implementation of these recommendations is an important indicator of whether the Department takes seriously the issues identified by OIG-NYPD and whether it intends to address those issues. OIG-NYPD therefore continues to monitor the status of all recommendations until they have been implemented by NYPD, and to make that status public.

Pursuant to § 803(d)(3) of the New York City Charter, as of December 31, 2021 OIG-NYPD reports that it had nine investigations open for six to 12 months, 11 investigations open for 13 to 24 months, six investigations open for 25 to 36 months, and ten investigations open for more than 36 months. These figures include investigations that qualify as systemic reviews as well as investigations prompted by individual complaints received from members of the public.

II. 2021 Office of the Inspector General for the New York City Police Department Activities

A. Systemic Investigations, Reviews, Studies, and Audits; Recommendations and NYPD Responses

Pursuant to Section 803(d)(3) of the New York City Charter, summarized below are the findings and recommendations of the Report OIG-NYPD released in 2021, as well as an assessment of NYPD's progress in implementing the 3 recommendations in that Report. OIG-NYPD continually monitors NYPD's progress on all recommendations until implemented.

SHARING POLICE BODY-WORN CAMERA FOOTAGE IN NEW YORK CITY

NOVEMBER 5, 2021

On August 24, 2017, the New York City Council passed Local Law 166, which instructs OIG-NYPD to "work[] with the law department, the comptroller, the police department, the civilian complaint review board, the commission to combat police corruption, and the commission on human rights [to] collect and evaluate information regarding allegations or findings of improper police conduct and develop recommendations relating to the discipline, training, and monitoring of police officers and related operations, policies, programs, and practices of the police department," and to publish a written evaluation or recommendations stemming from that work in each of the following three years and then every three years thereafter.[4] This is the third Report, following reports on police use of litigation data in 2018 and 2019, published pursuant to Local Law 166.[5] This Report considers "[i]nformation on collaboration and information sharing procedures of the police department," with respect to those agencies with oversight responsibilities listed above, and focuses on the sharing of body-worn camera (BWC) footage.[6]

To conduct this assessment, OIG-NYPD interviewed officials from each of the cited agencies, reviewed documents detailing each agency's procedures for sharing information, and conducted research on comparable agencies in other cities to better understand model practices for the sharing of BWC footage between police departments and their oversight agencies.[7]

---

[4] N.Y.C. CHARTER § 808(c).

[5] Although, under Local Law 166, this Report was intended to be released in 2020, it was delayed due to operational constraints related to the COVID-19 pandemic.

[6] N.Y.C. CHARTER § 808(b).

[7] In an effort to gain insight into NYPD's perspectives on information sharing with the Charter § 808 agencies, OIG-NYPD requested to meet with NYPD on January 3, 2020. This request noted that the meeting was part of OIG-NYPD's compliance with NYC Charter § 808(b). NYPD opted against making any representatives available for a meeting (or meetings) to discuss information sharing with Charter § 808 agencies, instead committing to send a written memorandum by February 14, 2020, addressing the topic. NYPD submitted a four-page document to OIG-NYPD on March 3, 2020. The submission contained the following statement on BWCs: "With regard to footage recorded on body-worn cameras, the Legal Bureau's Body-Worn Camera Unit has signed (but, not yet implemented) a Memorandum of

This Report found that each agency follows a different procedure to access BWC footage from NYPD. Despite having these individualized procedures, NYPD does not provide each agency with the appropriate level of access to BWC footage to enable them to optimally perform their missions. The Civilian Complaint Review Board (CCRB), in particular, is negatively impacted by its lack of direct access because of its unique responsibilities. The current access procedures may contribute to unnecessary delays that impede CCRB investigations.

NYPD policy dictates that its staff must approve all requests for footage and perform all searches on behalf of CCRB. That is an area of concern. This requirement exists because NYPD's BWC footage platform commingles footage from sealed cases and cases involving juveniles with footage from unsealed matters. The commingling of footage creates a barrier to direct access to BWC footage for CCRB. This commingling also creates potential legal liability for the City because sealed records should not be commingled with unsealed records, nor should they be readily viewable by anyone with access to the database, including NYPD personnel.

This Report also examines the Memorandum of Understanding (MOU) that CCRB and NYPD are in the process of implementing, and that will change CCRB's process for accessing BWC footage.[8] The MOU contemplates an updated search and request procedure and the creation of a dedicated location that CCRB and NYPD will use as a BWC search and review facility.

Other issues with the BWC footage sharing process include the Department's discretion to redact footage or decline to provide it, which the MOU does not address. Furthermore, CCRB has faced extended wait times for the return of footage. According to the MOU, NYPD must produce footage to CCRB within a set period of time following the completion of a search, but there is no set period within which NYPD must complete the search for footage. If CCRB had direct access to NYPD's BWC system, as many oversight agencies do in other cities, it would be able to conduct its investigations more efficiently. Furthermore, this would reduce NYPD's workload.

While OIG-NYPD expects that the MOU will improve CCRB's access to BWC footage for use in its police misconduct investigations, direct access to BWC footage would further reduce investigative delay.

For more information about the findings and recommendations, a full copy of the Report can be found here.

Understanding (MOU) with CCRB to produce body-worn camera records directly to CCRB without the involvement of the IAB CCRB Liaison Unit."

[8] Memorandum of Understanding between CCRB and NYPD, (Nov. 21, 2019) (on file with author); *see also* CIVILIAN COMPLAINT REV. BD., STRENGTHENING ACCOUNTABILITY: THE IMPACT OF THE NYPD'S BODY-WORN CAMERA PROGRAM ON CCRB INVESTIGATIONS 35 (2020).

This Report made three recommendations. Those recommendations and an assessment of NYPD's responses to those recommendations are below.

SHARING POLICE BODY-WORN CAMERA FOOTAGE (NOVEMBER 2021 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
1	NYPD should conduct an internal review to ensure that sealed BWC footage is not being commingled with unsealed BWC footage, and, if necessary, enact software-level safeguards to prevent sealed BWC footage from being viewed (either within or without NYPD) without a court order or waiver.	**Rejected** NYPD asserts that it will enact necessary changes consistent with the outcome of ongoing litigation concerning other kinds of sealed records in *R.C., et al. v. City of New York*. However, NYPD declines to conduct an internal review, in the interim, to address the commingling of sealed and unsealed records on NYPD's BWC footage platform, which creates significant procedural obstacles to the CCRB's prompt receipt of footage. The commingling of sealed and unsealed records in the BWC database also creates potential further legal liability for the City. Therefore, OIG-NYPD deems this recommendation rejected.
2	In an effort to more efficiently produce BWC footage and assist CCRB in fulfilling its mandate, NYPD should provide CCRB with independent and direct remote access credentials to all BWC storage databases so that BWC videos can be searched and viewed as necessary for CCRB investigations. Such access should be subject to appropriate credentials and audit trails to address security and privacy concerns.	**Rejected** While CCRB and NYPD have entered into a MOU that has the potential to improve the exchange of BWC footage between the two agencies, the MOU does not grant direct access to all BWC footage storage databases to CCRB. Direct access would allow CCRB to search and view BWC footage as necessary for its investigations, as many police oversight agencies do in other jurisdictions. Since the Department declines to provide CCRB such access, OIG-NYPD deems this recommendation rejected.
3	Within six months of the release of this Report, NYPD should consult with each of the covered Charter § 808 agencies, as well as OIG-NYPD, to determine whether additional access to BWC footage would benefit them in fulfilling their mandates, and engage in good-faith discussions to expand or streamline access if necessary.	**Accepted in Principle** NYPD informed OIG-NYPD that it accepts this recommendation. OIG-NYPD will follow up with NYPD once the six-month time period concludes to ensure that the Department has engaged in good-faith discussions with each of the covered Charter § 808 agencies regarding improved access to BWC footage.

B. Outreach and Engagement

In 2021, OIG-NYPD continued to engage with a variety of community groups, advocacy organizations, city and state agencies, elected officials, religious organizations, police unions, police departments, and oversight agencies to strengthen the relationship between New York City residents and NYPD. As a result of these efforts, the Office identified important police accountability issues that, when addressed, could help further its mission to increase public safety while protecting people's civil liberties and civil rights.

Despite challenges presented by the COVID-19 pandemic in 2020 and 2021, the activities of the Outreach Unit have continued and expanded. As events and opportunities for outreach transition to in-person once again, the Office has implemented a robust schedule of community engagement. Additionally, the Director of Outreach assisted the Inspector General with a presentation to hundreds of law enforcement officers from Mexico working in the field of police oversight.

New York City residents can engage with the Outreach Unit in multiple ways, including formal meetings, by invitation to attend events related to policing issues, through sharing policy briefs, filing complaints about policing issues, and presenting issues at OIG-NYPD-hosted brown bag lunches.

In 2022, the Outreach Unit will seek to further expand its activities by hosting additional meetings with advocacy organizations, police-community relations professionals, law enforcement oversight agencies from other jurisdictions, and re-engaging with stakeholders the Office has met with in the past.

C. COMPLAINTS

Local Law 70 requires that OIG-NYPD receive complaints from the public about NYPD operations, policies, programs, and practices. The complaints received by the Office range in scope from allegations regarding misconduct by individual police officers to complaints regarding large-scale NYPD policies and practices. Through receiving and reviewing complaints, speaking with members of the public, connecting with other government agencies, and conducting investigations OIG-NYPD can address individual concerns and allegations while also identifying potential areas for systemic review.

In 2021, 732 complaints were received from members of the public, advocacy groups, and employees of NYPD. City agencies, including NYPD, the Office of the Mayor, the Conflicts of Interest Board, the City Council, and the Civilian Complaint Review Board also referred matters. Complaints received frequently allege inadequate police services, failure to investigate after a police report has been filed, police corruption, disputes involving summonses, harassment by police, and the use of excessive force. If complaints are received that fall squarely within the jurisdiction of, or would be more appropriately investigated by, another agency, those complaints are referred to another agency. OIG-NYPD's Investigations Unit conducts investigations of those complaints that are not referred to other agencies and which fall within OIG-NYPD's jurisdiction.

OIG-NYPD can be reached for a formal complaint by a variety of means, including in-person interviews, online form, phone, email, fax, and U.S. mail:

In-Person Interview | **Online Form** | **Phone** | **Email** | **Fax** | **U.S. Mail**

III. 2015-2020 Systemic Investigations, Reviews, Studies, and Audits: Updated NYPD Responses to Recommendations

This section summarizes the findings and recommendations made in the 16 reports OIG-NYPD released from 2015 through 2019, and assesses the progress made by NYPD towards implementing the recommendations in these reports. Previously implemented recommendations, and recommendations that are no longer applicable to the Department, are listed in Appendix A.

This section also summarizes DOI's 2020 Report regarding NYPD's protest response. The status of the recommendations made in that Report can be seen in the DOI Policy and Procedure Recommendations Portal, here.

INVESTIGATION INTO NYPD RESPONSE TO THE GEORGE FLOYD PROTESTS (DOI Report)

December 18, 2020

Following the killing of George Floyd by a Minneapolis police officer, New York City saw mass protests concerning racism, policing, and accountability. As these protests evolved, DOI received a directive from the Mayor's Office, and a written referral from members of City Council, to investigate NYPD's protest response.

DOI investigators reviewed thousands of pages of NYPD records and footage, in addition to publicly available video, witness statements, and observer reports to examine NYPD's institutional protest response. DOI also reviewed various studies and published reports on protest policing practices, and interviewed experts on policing issues. As part of this review, DOI interviewed a number of senior NYPD leaders, including then-Police Commissioner Dermot Shea and then-Chief of Department Terence Monahan.

This Report identified deficiencies in NYPD's protest response. NYPD lacked both a central community affairs strategy as well as a strategy for responding to large-scale protests. As a result, NYPD applied "disorder control" tactics, including use-of-force and crowd-control methods like kettling, which produced heightened enforcement and escalated tensions between protesters and police. Reliance on these tactics by police officers may have occurred, in part, because most responding officers had not received training on policing protests, although a specialized unit within NYPD did receive such training. In addition, DOI found that some decisions by NYPD relied on intelligence without appropriate consideration of context or proportionality, thereby contributing to enforcement responses disproportionate to the circumstances. DOI also found that NYPD did not have a system with the capacity to track sufficient protest data.

DOI's report made 22 recommendations, organized into two parts. The recommendations in Part I aimed to improve NYPD's policies related to policing protests, while those recommendations in Part II focused on external oversight of the

Department.

For more information about the findings or recommendations issued in this Report, a copy of the original report can be found here.

DOI and NYPD are working together to track the statuses of the recommendations in this report. DOI updates the statuses of the recommendations made to agencies City-wide on a quarterly basis in its DOI Policy and Procedure Recommendations Portal, here. An assessment of the recommendations' statuses can also be found on NYPD's website, here.

AN INVESTIGATION OF NYPD'S OFFICER WELLNESS AND SAFETY SERVICES

September 24, 2019 Report

OIG-NYPD's Officer Wellness and Safety Report examined the services available to NYPD's officers in need of assistance and explored the extent to which officers were aware of these services, were taking advantage of them, and how support services could be enhanced and made more widely available. The investigation included meeting with NYPD support services personnel and associated NYPD units, attending NYPD trainings, and speaking with several NYPD unions. As a key part of its review, OIG-NYPD also sought to understand the effectiveness and use of NYPD's mental health resources by administering a survey to uniformed NYPD personnel who had completed their service.

OIG-NYPD made 12 recommendations aimed at enhancing NYPD's mental health and wellness services.

For more information about the findings and recommendations, a full copy of the original Report can be found here.

NYPD has implemented eight of the 12 recommendations issued in this Report. Those recommendations (1, 4, 5, 8-10) not listed below were implemented prior to the issuance of this Annual Report, and are listed in Appendix A. The statuses of the outstanding recommendations are detailed below.

AN INVESTIGATION OF NYPD'S OFFICER WELLNESS AND SAFETY SERVICES (SEPTEMBER 2019 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
2	NYPD should use the results of its own recent 2019 officer survey on health and wellness (and, if necessary, conduct additional officer surveys with the assistance of outside experts) to inform the Department's overall Mental Health and Wellness policy referenced in Recommendation #1.	**Changed from Partially Implemented to Implemented** The responses to the 2019 survey demonstrated that NYPD officers were interested in additional services provided by the Department. The Health and Wellness Section (HWS) used the results of that initial survey to create programs for members of service, including the peer support program. NYPD reports that it has created and distributed a survey to participants of its Critical Incident Stress Management Program, which identifies and provides support to members of service who have been involved in traumatic incidents. The responses to that survey will be used to explore outcomes of the program.

		Additionally, the HWS leadership, are creating a follow-up wellness survey to be distributed Department-wide.
3	Consistent with the size of the Department, NYPD should increase the staffing levels in the Health and Wellness Section to include full-time licensed mental health professionals and support staff with appropriate levels of competency in the areas of mental health and wellness.	**Unchanged: Partially Implemented** Prior to the 2021 Annual Report, NYPD committed to hiring 17 full-time staff. To date, HWS is staffed by 11 personnel, including a Director, a Deputy Director, two level two psychologists, a clerical coordinator, and a uniformed team that assists with scheduling, training initiatives, incident identification, and various post-incident follow-up support. NYPD reports that it is working to onboard additional psychologists. OIG-NYPD will continue to monitor HWS staffing levels until sufficient.
6	NYPD should study the feasibility of establishing mandatory periodic mental health checks for all police officers or certain categories of at-risk officers.	**Unchanged: Under Consideration** According to NYPD, it is still exploring this option with labor unions, as it has been since this Report's release. Implementation of this recommendation would be subject to collective bargaining. OIG-NYPD will continue to monitor this issue.
7	NYPD should modify its early intervention system—Risk Assessment Information Liability System (RAILS)—to include an "officer wellness" category, based on various relevant indicators, so that NYPD personnel requiring officer wellness intervention can be identified.	**Changed from Rejected to Implemented** NYPD has designated a sergeant to identify potentially at-risk members, by reviewing RAILS for low evaluations, chronic sick time, suspensions or modifications potentially involving domestic incidents, force allegations, or military affiliations, all of which it considers indicators of officer wellness. Officers identified can be referred to the Employee Assistance Unit for debriefing. To date, 690 members of service have been identified and referred in this way. Although NYPD's RAILS system does not have an "officer wellness" category, the review of the existing categories in RAILS, as set out above, is an appropriate method of identifying officers who may require early intervention. As a result, OIG-NYPD will deem this recommendation implemented.

		NYPD reports that it will be integrating RAILS into a new system, the Central Personnel Resource System (CPRS), in August 2022. OIG-NYPD will re-evaluate this recommendation following the implementation of that system.
11	NYPD should explore the needs of its retired personnel and endeavor to make wellness support services available to them for a reasonable period of time following retirement or separation.	**Unchanged: Under Consideration** NYPD reports that a retirement coordinator has been hired. Pre-retirement informational sessions are now being held, as well as resume building programs, and wellness appointments for members of service. According to NYPD, a Post Transition Sponsorship Program is being developed to assist NYPD retirees with maintaining connections post-retirement. There is no timeline identified by which NYPD will provide *post-separation* services to retired personnel. OIG-NYPD will continue to monitor this issue.
12	NYPD should put in place mechanisms to ensure that the privacy rights of NYPD personnel are respected and strictly protected, both internally and externally, so that information relating to officer health and wellness is not misused and is accessible only by those who need to know. Such efforts should be informed by discussions with officers and representative organizations like police unions and fraternal organizations.	**Unchanged: Accepted in Principle** According to NYPD, the Department is committed to ensuring the privacy rights of NYPD personnel. NYPD plans to move the location of the HWS section to a private dedicated clinical space. Additionally, it seeks to begin using a confidential medical database for documentation storage, and a HIPPA compliant virtual platform designed for the provision of mental health care, pending approval. A start date for use has not been provided. OIG-NYPD will continue to monitor this issue.

COMPLAINTS OF BIASED POLICING IN NEW YORK CITY: AN ASSESSMENT OF NYPD'S INVESTIGATIONS, POLICIES, AND TRAINING

June 26, 2019 Report

Biased policing is any discriminatory action (or inaction) by law enforcement that is motivated, even in part, by a person's actual or perceived status protected by law (for example, race, gender, sexual orientation, etc.). Biased policing, whether perceived or actual, is a matter of significant public concern because some communities, including communities of color, report high levels of distrust of the police, as the remedial process of *Floyd v. City of New York* has documented.[9] After a Court found that NYPD's "stop, question, and frisk" policies and practices resulted in disproportionate and discriminatory stop-and-frisks of hundreds of thousands of Black and Latino people, the Court ordered NYPD to begin investigating complaints of biased policing, such as racial profiling. OIG-NYPD subsequently conducted an independent investigation that culminated in this 2019 Report. To perform its investigation OIG-NYPD analyzed over 5,000 pages of NYPD documents related to 888 allegations which covered a two-and-a-half year period, attended NYPD's trainings related to biased policing, and interviewed NYPD investigators who handled such allegations

The Report determined that from 2014, when NYPD began separately investigating and tracking such complaints, through the end of 2018, members of the public made at least 2,495 complaints of biased policing and the Department did not substantiate a single allegation. Among other findings, the Office found NYPD's method of investigation and tracking such allegations was inadequate in certain respects.

The investigation also revealed that the Civilian Complaint Review Board (CCRB), the City's primary agency charged with independently investigating allegations of police officer misconduct, is the *only* independent police review agency (of the agencies responsible for the 20 largest police departments in the U.S.) that does not investigate complaints of biased policing made against officers. Additionally, OIG-NYPD determined that NYPD does not investigate an officer's use of offensive or derogatory language related to a complainant's actual or perceived protected status, such as use of a racial slur, as biased policing. Instead, NYPD refers the matter to CCRB for investigation as Offensive Language.

Subsequent to the release of OIG-NYPD's 2019 Report, NYC Council passed legislation (Local Law No. 047 of 2021) in April 2021, which clarified that CCRB has the authority to investigate biased policing. This change is consistent with a recommendation made in this Report (recommendation #21). Furthermore, CCRB

[9] *See* Belen, et al., *New York City Joint Remedial Process: Final Report and Recommendations on NYPD's Stop, Question, and Frisk and Trespass Enforcement Policies* (May 15, 2018), *pursuant to* Opinion and Order in F*loyd v. City of New York*, 959 F. Supp. 2d 540 (2013) (No. 08-CIV-1034-SAS-HBP, ECF No. 372 at p. 8 (Aug. 12, 2013)).

informed OIG-NYPD that, in response to the legislation, it has "hired a Director and is in the process of staffing" it's new Racial Profiling and Bias Based Policing Unit. Although NYPD previously informed OIG-NYPD that biased policing "will no longer be investigated by [NYPD], but instead by CCRB and then either prosecuted or adjudicated by CCRB" once the unit is fully staffed, CCRB's investigative jurisdiction only covers *uniformed* members of NYPD.[10] Therefore, the approximately 19,000 non-uniformed members of NYPD (e.g., School Safety Agents, Traffic Enforcement Agents, etc.) will, in fact, continue to be investigated by NYPD for biased policing. OIG-NYPD has not yet received the requested information related to any policies, practices, and procedures for investigating non-uniformed members of NYPD who allegedly engage in biased policing. Progress towards implementation of the Report's recommendations will be assessed based on current NYPD and CCRB practices of which OIG-NYPD is aware.

The Report makes 23 recommendations, the majority of which are addressed to NYPD. Four of the recommendations in this Report relate to either CCRB and/or the City's Commission on Human Rights (CCHR); these recommendations also improve the City's handling of biased policing complaints.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has implemented eight of the 21 recommendations addressed to it. CCRB has not yet fully implemented the two recommendations addressed to it. Those recommendations (4-8, 10, 13, 22) not listed below were implemented prior to the issuance of this Annual Report and can be found in Appendix A. The statuses of the outstanding recommendations are as follows.

COMPLAINTS OF BIASED POLICING IN NEW YORK CITY: AN ASSESSMENT OF NYPD'S INVESTIGATIONS, POLICIES, AND TRAINING (JUNE 2019 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
1	NYPD should amend its Patrol Guide policies to explicitly require NYPD officers and non-uniformed employees to report instances of biased policing upon observing or becoming aware of such conduct.	**Unchanged: Rejected** NYPD's Patrol Guide § 207-21, "Allegations of Corruption and Other Misconduct Against Members of the Service," requires uniformed members who observe misconduct such as "the use of excessive force or perjury" to report it. Although NYPD explicitly cites "excessive force" and "perjury" in this Patrol Guide policy, NYPD continues to reject OIG-NYPD's

[10] N.Y.C. Charter § 440(c)(1)

		recommendation to also include explicit language requiring the reporting of biased policing. Therefore, OIG-NYPD has deemed this recommendation rejected.
2	NYPD should amend its Patrol Guide policies so that complaints alleging the use of offensive or derogatory language associated with an individual's actual or perceived protected status, such as racial slurs, are classified as biased policing if there is a discriminatory intent.	**Unchanged: Rejected** NYPD takes the position that a discriminatory slur, such as a racial slur, cannot satisfy the requirement under Administrative Code § 14-151, that prohibits biased policing, because only an "action" can constitute biased policing. OIG-NYPD maintains its view that slurs by active-duty officers directed towards members of the public because of their protected status are in fact actions. NYPD's Patrol Guide is inconsistent with the policies of other U.S. police departments in that it fails to recognize that the use of discriminatory slurs in this manner can constitute biased policing. Therefore, OIG-NYPD has deemed this recommendation rejected.
3	NYPD should amend its *written* investigative procedures related to biased policing so that offensive or derogatory language associated with an individual's actual or perceived protected status, such as an officer's use of racial slurs, is classified, investigated, and adjudicated as a biased policing matter.	**Unchanged: Rejected** The City plans to transfer responsibility for complaints of biased policing by uniformed officers to CCRB once its Racial Profiling and Bias Based Policing Unit is fully staffed. However, in the interim, NYPD declines to amend the written investigative procedures by which it conducts biased policing investigations. Additionally, non-uniformed members of NYPD (e.g., School Safety Agents, Traffic Enforcement Agents, etc.) will continue to be investigated by NYPD for biased policing using the existing written procedures (which do not classify the use of slurs related to protected status as biased policing), because CCRB's investigative jurisdiction is limited to *uniformed* members of NYPD. Therefore, OIG-NYPD has deemed this recommendation rejected.
9	NYPD should make records of complaints and investigations of biased policing allegations available to CCHR for analysis and review.	**Unchanged: Accepted in Principle** According to NYPD, it complies with appropriate request(s) for closed biased policing complaint

		information from CCHR. However, the Department has declined to provide documentation of such compliance to OIG-NYPD.
11	NYPD should develop a checklist of all the required protocols for investigating allegations of biased policing, such as interviewing complainants and sub-classifying all applicable protected statuses.	**Unchanged: Rejected** The City plans to transfer responsibility for complaints of biased policing by uniformed officers to CCRB once its Racial Profiling and Bias Based Policing Unit is fully staffed. However, in the interim, NYPD will continue to conduct these investigations by using existing processes, and without a checklist. Additionally, non-uniformed members of NYPD (e.g., School Safety Agents, Traffic Enforcement Agents, etc.) will continue to be investigated by NYPD for biased policing using the existing written procedures, because CCRB's investigative jurisdiction is limited to *uniformed* members of NYPD. Therefore, OIG-NYPD has deemed this recommendation rejected.
12	Investigators should be required to complete and submit to their supervisors the checklist with their case closing reports.	**Unchanged: Rejected** The City plans to transfer responsibility for complaints of biased policing by uniformed officers to CCRB once its Racial Profiling and Bias Based Policing Unit is fully staffed. However, in the interim, NYPD investigators continue to use the existing process that does not require investigators to complete and submit a checklist to their supervisors. Additionally, non-uniformed members of NYPD (e.g., School Safety Agents, Traffic Enforcement Agents, etc.) will continue to be investigated by NYPD under the existing process, because CCRB's investigative jurisdiction is limited to *uniformed* members of NYPD. Therefore, OIG-NYPD has deemed this recommendation rejected.
14	With respect to complaints of biased policing, NYPD should ensure that IAB's case management system contains the same controls found in the ICMT system used by NYPD's Bureau/Borough investigators,	**Unchanged: Rejected** The City plans to transfer responsibility for complaints of biased policing by uniformed officers to CCRB once its Racial Profiling and Bias Based Policing Unit is fully staffed. In the interim, Internal Affairs Bureau

	including controls regarding the requisite number of attempts to contact complainants. This will ensure that the necessary requirements of an investigation are completed prior to the closure of all biased policing cases.	(IAB) investigators continue to use its Internal Case Management System, which does not require a successful contact with the complainant or three documented contact attempts before the case can be closed. Additionally, non-uniformed members of NYPD (e.g., School Safety Agents, Traffic Enforcement Agents, etc.) will continue to be investigated by NYPD under the existing process, even after CCRB completes the staffing process of its new unit because CCRB's investigative jurisdiction is limited to *uniformed* members of NYPD. Therefore, OIG-NYPD has deemed this recommendation rejected.
15	NYPD should develop and implement a pilot mediation program for some biased policing complaints. As part of that program, NYPD should develop criteria for referring to mediation cases involving both uniformed and non-uniformed members.	**Changed from Accepted in Principle to Rejected** The City plans to transfer responsibility for complaints of biased policing by uniformed officers to CCRB once its Racial Profiling and Bias Based Policing Unit is fully staffed. However, in the interim, there is no mediation process in place for any biased policing complaints. Additionally, non-uniformed members of NYPD (e.g., School Safety Agents, Traffic Enforcement Agents, etc.) will continue to be investigated by NYPD under the existing process, because CCRB's investigative jurisdiction will be limited to *uniformed* members of NYPD. Therefore, OIG-NYPD has deemed this recommendation rejected.
16	NYPD's RAILS should be expanded to capture unsubstantiated biased policing allegations involving both uniformed and non-uniformed members.	**Unchanged: Rejected** NYPD has early intervention programs that may consider unsubstantiated biased policing allegations. However, RAILS, NYPD's early intervention program dedicated to providing real-time alerts to supervisors does not include unsubstantiated biased policing allegations as one of the triggers for early intervention. Therefore, OIG-NYPD has deemed this recommendation rejected.

17	NYPD's Performance Monitoring Program should develop monitoring criteria to include officers and non-uniformed employees who are the subject of biased policing complaints, regardless of substantiation, modeled on the metrics currently in use for excessive force complaints.	**Changed from Accepted in Principle to Rejected** The City plans to transfer responsibility for complaints of biased policing by uniformed officers to CCRB once its Racial Profiling and Bias Based Policing Unit is fully staffed. After this is done, some of these allegations will become CCRB complaints and thus have adequate performance monitoring criteria. However, in the interim, NYPD has not changed its performance monitoring criteria to include biased policing complaints, regardless of substantiation. Additionally, non-uniformed members of NYPD (e.g., School Safety Agents, Traffic Enforcement Agents, etc.) will continue to be investigated by NYPD under the existing process, because CCRB's investigative jurisdiction is limited to *uniformed* members of NYPD. Therefore, OIG-NYPD has deemed this recommendation rejected.
18	NYPD should develop written materials to educate the public about what biased policing is and how members of the public can file biased policing complaints. This information should be conspicuously visible on NYPD's website and in other locations where such information would be readily available to the public.	**Unchanged: Rejected** NYPD has not made the relevant biased policing information conspicuously visible on its website, nor has the Department developed written materials to educate the public about what biased policing is and how members of the public can file complaints. Therefore, OIG-NYPD has deemed this recommendation rejected.
19	NYPD should publish statistics for the public as part of an annual report covering biased policing. These statistics should, at a minimum, include a breakdown of the following: (i) the subject officer's uniformed versus non-uniformed status, bureau or unit assignment, gender, race/ethnicity, age, and length of service to the Department; (ii) the self-reported demographics (race/ethnicity, sex, age, etc.) of complainants;	**Unchanged: Rejected** The City plans to transfer responsibility for complaints of biased policing by uniformed officers to CCRB once its Racial Profiling and Bias Based Policing Unit is fully staffed. However, this does not prevent NYPD from publicly reporting the various statistics and information that OIG-NYPD recommends. Therefore, since the Department is not providing the recommended transparency to the public, OIG-NYPD has deemed this recommendation rejected.

	(iii) the types of police encounters that resulted in complaints of biased policing; (iv) the number of biased policing complaints initiated by borough and precinct; (v) the discriminatory policing conduct alleged; (vi) the sub-classifications and outcomes of such complaints; and (vii) the status of the Department's efforts to prevent biased policing. This information should be conspicuously visible on NYPD's website and in other locations where such information would be readily available to the public.	
20	CCRB should add all the protected statuses, such as "National Origin," "Color," "Age," "Alienage," "Citizenship Status," and "Housing Status" as outlined in § 14-151 of the NYC Administrative Code and § 203-25 of NYPD's Patrol Guide, to the sub-classifications of its Offensive Language category.	**Changed from Accepted in Principle to Rejected** CCRB's Offensive Language category contains some of the protected statuses as sub-classifications including "Race," "Ethnicity," "Gender," "Gender Identity," "Sexual Orientation," "Religion," "Physical Disability," and "Other." However, CCRB does not include *all* of the protected statuses that are outlined in § 14-151 of the NYC Administrative Code and § 203-25 of NYPD's Patrol Guide. Sub-classifications should also include "National Origin," "Color," "Age," "Alienage," "Citizenship Status," and "Housing Status." Therefore, OIG-NYPD has deemed this recommendation rejected.
21	CCRB should adopt a policy to classify and investigate allegations of biased policing by uniformed members of NYPD under its Abuse of Authority jurisdiction instead of referring such allegations to IAB for investigation. Consistent with this new authority, CCRB should request additional resources from the City to take on this new responsibility if the	**Unchanged: Accepted in Principle** CCRB informed OIG-NYPD that it has "hired a Director and is in the process of staffing" it's new Racial Profiling and Bias Based Policing Unit that will investigate uniformed members of NYPD accused of biased policing practices. According to CCRB, it will commence investigations once it completes its staffing process.

	agency can demonstrate that more resources are necessary.	
23	NYPD, CCRB, and CCHR should develop protocols and procedures to share data and information on biased policing complaints on a regular basis. To the extent that implementing this Report's recommendations would require CCRB or CCHR to have prompt access to NYPD records (*e.g.,* case files, data, body-worn camera video, etc.), protocols should be established so that NYPD will commit itself to providing such access to these agencies.	**Unchanged: Accepted in Principle** According to NYPD, it is committed to complying with requests related to biased policing from CCHR. According to CCRB, its new Racial Profiling and Bias Based Policing Unit will work with NYPD to develop protocols and procedures by which it will conduct its biased policing investigations.

2019 ASSESSMENT OF LITIGATION DATA INVOLVING NYPD

April 30, 2019 Report

Pursuant to Local Law 166 and as a follow-up to OIG-NYPD's previously issued reports on police use of litigation data in 2015 and 2018, in April 2019 the Office assessed NYPD's ongoing efforts to track and analyze data from claims and lawsuits, with a particular focus on the Department's early intervention system, the Risk Assessment Information Liability System (RAILS). OIG-NYPD conducted an analysis of civil actions filed against the Department alleging misconduct from the years 2014 to 2018 using litigation data publicly released by the New York City Law Department. The review of this five-year period found that while there was a 49 percent decline in the number of NYPD-related lawsuits alleging police misconduct during the period as a whole, there was a large uptick in the number of lawsuits filed from 2017 to 2018.

The review concluded that the Department was tracking more data on lawsuits and claims, including the nature of the claim, the location of the incident, and details about the subject officer than the Department tracked as of the Office's 2015 report. The Report made four recommendations for NYPD to continue to build upon RAILS as a tool for tracking misconduct allegations and to ensure that supervisors are effectively prepared to use the system.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has not fully implemented any of the four recommendations issued in this Report. The statuses of the recommendations are as follows.

ASSESSMENT OF LITIGATION DATA INVOLVING NYPD (APRIL 2019 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
1	NYPD should consider incorporating peer officer averages and performance indicator ratios in its thresholds for RAILS, or other approaches that would account for officers with greater activity who may not necessarily exhibit problematic behavior.	**Unchanged: Under Consideration** NYPD states that it has a target date of August 2022 to integrate RAILS into a new system, Central Personnel Resource System (CPRS), that, once functional, may be able to incorporate peer officer averages and performance indicator ratios. Therefore, OIG-NYPD deems this recommendation under consideration.

2	NYPD should seek input from supervisors in further developments of RAILS and create a mechanism for supervisors to direct their feedback. Supervisors should be involved in each stage of the development and implementation process for RAILS. NYPD should have a formal, standing mechanism for supervisors to direct their feedback, including any problems or concerns with the system.	**Unchanged: Partially Implemented** Although NYPD held a working group in January 2019 for supervisors, it has not created a formal, standing mechanism for supervisors to direct their feedback about RAILS. NYPD states that it has a target date of August 2022 to integrate RAILS into a new system, Central Personnel Resource System (CPRS), that, once functional, may be able to create such a formal, standing, mechanism. Since NYPD held the working group in January 2019, but did not create a formal, standing mechanism, OIG-NYPD deems this recommendation partially implemented.
3	NYPD should ensure that sufficient and ongoing training is available to all supervisors once RAILS is fully developed. Such training should specifically take into account supervisors' new roles and responsibilities with the system.	**Unchanged: Under Consideration** NYPD has had no new trainings on this subject since April 2019. Furthermore, NYPD states that it has a target date of August 2022 to integrate RAILS into a new system, Central Personnel Resource System (CPRS), that, once functional, may be able to allow such trainings. Therefore, OIG-NYPD deems this recommendation is under consideration.
4	NYPD should ensure there are procedures in place before RAILS is fully implemented to hold supervisors accountable for upholding their responsibilities concerning the system. These procedures should include a policy outlining how often supervisors should log on to RAILS and review their alerts. NYPD should also take steps to confirm that supervisors are following this policy as directed, such as by conducting regular audits of the system.	**Unchanged: Accepted in Principle** According to NYPD it has a target date of August 2022 to integrate RAILS into a new system, Central Personnel Resource System (CPRS). NYPD states that once that system is operational, the policies and procedures will be communicated to ensure that supervisors are appropriately discharging their duties under the system.

ONGOING EXAMINATION OF LITIGATION DATA INVOLVING NYPD

April 30, 2018 Report

In response to OIG-NYPD's 2015 Report, the City Council passed Local Law No. 166. The law required the Office of the Inspector General for the NYPD to collect, evaluate, and report on information concerning improper police conduct by analyzing claims and lawsuits filed against the Department. Pursuant to this law, the Office released its 2018 Report proposing how NYPD can use data from lawsuits to improve policing.

Though the filing of a lawsuit does not necessarily demonstrate improper police conduct, NYPD can still use lawsuit trends to identify areas warranting closer review of Departmental operations, and consider any needed policy or practice changes. This Report underscored the types of data trends NYPD should assess. OIG-NYPD identified precincts that experienced increases or decreases in various types of allegations (e.g., false arrests, excessive force, etc.), and found that, while NYPD acknowledged the benefits of analyzing litigation data, it was not using its early intervention system to track the number, types, and outcomes of lawsuits filed against individual officers. In addition, to the extent NYPD had conducted any litigation data analysis, the results had not been made public.

OIG-NYPD made five recommendations concerning NYPD's litigation data-tracking system, intended to use such data to identify both individual officers at risk, as well as Department-wide areas for improvement.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has only implemented one out of the five recommendations issued in this Report. That recommendation (3) can be found in Appendix A. The statuses of the outstanding recommendations are as follows.

ONGOING EXAMINATION OF LITIGATION DATA INVOLVING NYPD (APRIL 2018 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
1	In line with the considerations codified in Local Law 166, NYPD should analyze Department-wide litigation patterns and trends as well as observable patterns and trends within individual precincts and units in order to identify areas for improvement in Department policies, training, supervision, and tactics. In paying greater attention to data within individual precincts, NYPD	**Unchanged: Partially Implemented** NYPD has not included lawsuits that it believes to be "meritless" in its early intervention system. OIG-NYPD maintains that by not including supposedly "meritless" litigation in this system, NYPD's analysis is too limited. Additionally, the Department has raised concerns that this recommendation will require additional staffing.

	should review and analyze patterns and trends such as those shown in DOI's analysis of the 77th Precinct.	OIG-NYPD asserts that there is value in a broader, Department-wide analysis of litigation and claims data.
2	Based on the findings that result from such analyses, NYPD should create internal reports that describe specific Department-wide and precinct or unit level patterns and trends in legal claims and should share these reports with command leadership.	**Unchanged: Partially Implemented** While NYPD conducts some trend analysis of lawsuits and claims, the Department has continued to reject the OIG-NYPD's recommendation that the Department to conduct data analysis of all lawsuits. OIG-NYPD maintains there is value in a broader, Department-wide analysis and that reports can be generated without violating legal privileges.
4	NYPD should create public reports that do not violate rules of confidentiality, taking care to disclose only the number and the general nature of claims filed against the Department as well as the current state of any interventions or policy changes.	**Unchanged: Rejected** NYPD continues to reject OIG-NYPD's recommendation because it asserts that public reports would open the Department up to unnecessary litigation. OIG-NYPD maintains that NYPD could release such a report while taking care to disclose only the number and the general nature of claims filed against the Department. In an effort to provide greater transparency to the public, OIG-NYPD stands by the original recommendation.
5	NYPD should increase the number of employees focusing primarily on tracking litigation trends in order for NYPD to conduct proactive litigation analysis so that patterns and trends can be identified, tracked, and, where necessary, addressed.	**Changed from Under Consideration to Rejected** NYPD asserts that it continually assesses its staffing levels, despite staffing constraints. Nonetheless, NYPD has not increased the number of employees focusing primarily on tracking litigation trends since OIG-NYPD made it's 2018 recommendation and has not confirmed that it will do so, OIG-NYPD has deemed this recommendation rejected.

AN INVESTIGATION OF NYPD'S SPECIAL VICTIMS DIVISION—ADULT SEX CRIMES

March 26, 2018 Report

In 2018, OIG-NYPD released a Report focusing on NYPD's Special Victims Division's (SVD) staffing resources. The New York City Council took legislative action in response to the Report's findings, requiring public reporting on SVD's case-management system, staffing, caseload, and training. These reports can be found on NYPD's website.[11]

By 2021, NYPD appeared to make notable progress on almost every recommendation. At the time, however, two barriers remained that have a negative impact on full implementation: (1) the recommendations have not been "codified" as policies or procedural requirements and thus the progress that has been made could easily be reversed and (2) funding.

Over the course of the past year, progress on the remaining recommendations has largely stalled. City funding remains an obstacle to increasing promotional opportunities at SVD, and OIG-NYPD reiterates its call for the City Council and the Mayor to make invest the necessary resources in SVD. With respect to the recommendations within NYPD's control, NYPD has not yet codified the recommendations into official Department policy.

Overall, NYPD has made significant progress towards implementation and deserves recognition for its efforts. However, there is still more work to be done to achieve full implementation. The Office will continue to monitor NYPD's implementation of the Report's recommendations.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has fully implemented five of the 12 recommendations made in this Report. Those recommendations (1, 6, 7, 11, 12) not listed below were implemented prior to the issuance of this Annual Report, and are listed in Appendix A. The statuses of the outstanding recommendations are as follows.

AN INVESTIGATION OF NYPD'S SPECIAL VICTIMS DIVISION—ADULT SEX CRIMES (MARCH 2018 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
2	In order to prevent a recurrence of understaffing, NYPD should adopt an evidence-based investigative staffing model that relies on actual	**Unchanged: Accepted in Principle**

[11] These laws were codified as N.Y.C. Admin. Code §§ 14-178, 14-179, and 14-180; *Special Victims Division Reports,* N.Y.P.D., https://www1.nyc.gov/site/nypd/stats/reports-analysis/svd.page (last visited Mar. 30, 2020).

	investigative hours available and projected caseload (not caseload alone) and continuously monitor SVD caseloads and staffing levels to ensure the appropriate number of staff are available for the assigned caseloads.	NYPD provided to OIG-NYPD the underlying staffing model used to achieve implementation of recommendation 1. Instead of using the target of average "investigative hours" required to properly close a case, NYPD uses the target of the number of cases that have been properly closed in one month. With this new caseload model, the caseload target is no longer arbitrary, or based on other detective squads that do substantially different work. Instead, the caseload target was obtained by examining the investigative capacity of an SVD investigator's full tour in one month. OIG-NYPD has maintained that NYPD need not adopt the exact staffing formula proposed in its Report, as long as the formula is evidence-based and reliant on investigative hours available instead of caseload alone. While an acceptable formula, NYPD has not formalized this new staffing model as official Departmental policy. It is not codified as part of the Patrol Guide, Operation Order, or any official Department document. Without formal adoption, this recommendation is not considered implemented, and is instead accepted in principle.
3	Since staffing deficiencies are not unique to adult sex crime units alone, NYPD should use the staffing model adopted in Recommendation 2 to appropriately staff the other SVD sub-units.	**Unchanged: Accepted in Principle** See Recommendation 2 above. NYPD is using a seemingly appropriate staffing model in practice, but has yet to formalize this practice as official policy in writing.
4	NYPD should immediately take steps to improve SVD's ability to recruit and retain experienced detectives by making SVD a "graded" division. Once completed, NYPD should end the practice of transferring officers to SVD without extensive investigative experience.	**Unchanged: Under Consideration** NYPD continues to report that SVD is sufficiently staffed such that "white shield" investigators are no longer given primary investigative or case responsibility. Instead, they spend their time as white shields in a training capacity. This is a positive development. In terms of "grading" and promotions, according to NYPD SVD's promotional structure is again under consideration but promotions are a practical impossibility due to the City's fiscal situation. OIG-

		NYPD asks that the City Council and the Mayor prioritize funding these reforms. Until such structure is finalized this recommendation would not be considered implemented. OIG-NYPD will continue to monitor this recommendation.
5	NYPD should increase in-house training opportunities for SVD staff in order to better prepare them for the rigors and unique nature of SVD work. The depth and rigor of this training should be equivalent to the training provided to other specialized units in NYPD.	**Changed from Accepted in Principle to Partially Implemented** NYPD reiterates that it has implemented new in-house training opportunities for SVD investigators that largely meet the spirit of this recommendation. Further, as noted in recommendation 4 above, NYPD reports that SVD no longer uses white shields in a primarily investigative role. Instead, investigators spend their time as white shields in a six-month training and observation role. SVD has also reintroduced enhanced specialized training for SVD staff. This recommendation, however, is not yet considered implemented because these changes are not official Departmental policy and could change at any time. Therefore, OIG-NYPD will continue to monitor this recommendation to ensure full implementation.
8	NYPD should find new physical locations and/or completely renovate all five SVD adult sex crime unit locations. These new physical locations should be easily accessible from public transportation and built out in the model of the Children's Advocacy Centers now operational in New York City.	**Unchanged: Partially Implemented** While some progress has been made on this front, there is still additional work to be done. OIG-NYPD understands that the capital budget process is largely not within NYPD's control, and can take some time to complete. It has, however, been more than three years since the Report was published. As with recommendation 4, OIG-NYPD urges the City to provide adequate budget funding to implement this recommendation.
9	NYPD should invest in a new case management system for SVD that would replace ECMS. The new system should have the highest security protocols and limit access to the case detective and their immediate supervisors within SVD.	**Changed from Accepted in Principle to Partially Implemented** In the 2021 Annual Report, OIG-NYPD noted that NYPD had made changes to its ECMS practices to better limit access to SVD files. ECMS audit logs were reviewed and found to be satisfactory. These changes,

	In addition, any new system should have advanced caseload, staff management, and data analysis capabilities.	however, still rely on the legacy ECMS software. Therefore, the Office will continue to monitor to ensure full implementation of the spirit of this recommendation.
10	NYPD should take steps to safeguard the identifying information of sex crimes victims, including conducting a review of the various reports, forms, and memoranda generated during the course of a sex crimes investigation that unnecessarily require the victim's name, address, or other contact information.	**Changed from Rejected to Partially Implemented** NYPD states that while some paperwork outside of the ECMS system continues to be generated, these reports no longer include any identifying information of the victims of sex crimes. This recommendation, however, is not yet considered implemented because these changes are not official Departmental policy and could change at any time. Therefore, OIG-NYPD will continue to monitor this recommendation to ensure full implementation.

AN INVESTIGATION OF NYPD'S NEW FORCE REPORTING SYSTEM

February 6, 2018 Report

In June 2016, in response to OIG-NYPD's 2015 Report on Use of Force, the Department replaced its existing use-of-force policies and created a new form: the Threat, Resistance, and Injury Worksheet (T.R.I.). NYPD designed the new form to record certain uses of force by and against police officers, as well as any injuries that occurred during the course of a police action or while an individual was in police custody.

OIG-NYPD's 2018 Report, conceived as a follow-up to the earlier report, examined NYPD's compliance with its new policies. The 2018 Report revealed some gaps and initial missteps in the rollout of the Department's new policies. This Report contained 25 recommendations that, if implemented, would make NYPD's use-of-force data collection process more accurate and effective.

The Department was initially resistant to the 2018 Use of Force Report, rejecting most of the recommendations outright. Starting in 2019, however, the Department began to re-engage with OIG-NYPD to enhance its use-of-force policies. Those policies were re-imagined as T.R.I. 2.0, incorporating many of OIG-NYPD's recommendations.

This past year, NYPD continued to build on some positive changes with respect to its use-of-force policies. NYPD has fully implemented an additional four recommendations, reducing the total number of outstanding recommendations to seven. No progress was made, however, on any of those outstanding recommendations, as to which there are continuing disagreements.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has now implemented 17 of the 25 recommendations in this Report, and one additional recommendation is no longer applicable to the Department. Those recommendations not listed below (1, 3, 7, 11-14, 16, 17, 19, 21B, 21C, 21E) were implemented prior to the issuance of this Annual Report or are no longer applicable (20), and are listed in Appendix A. The statuses of the outstanding recommendations are as follows.

AN INVESTIGATION OF NYPD'S NEW FORCE REPORTING SYSTEM (FEBRUARY 2018 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
2	NYPD should continue to develop its software capabilities. Existing systems initiate the creation of a T.R.I. number when an officer indicates on an arrest report that force was used. Additional software capabilities could enable the system to prompt officers that they may have to complete a T.R.I. when certain arrest charges are entered (such as Resisting Arrest or Assault on a Police Officer), when the arrest report indicates an arrestee or officer injury has occurred, and in other similar scenarios.	**Unchanged: Accepted in Principle** In the Annual Report for 2020, issued in 2021, NYPD reported that it was still working on linking TRI Forms to arrest reports, and that it may take some time to implement due to fiscal considerations. For this Report, NYPD provided no update. Therefore, the recommendation status remains unchanged. OIG-NYPD will continue to monitor this recommendation. If NYPD does not make progress by the 2023 Annual Report, the recommendation may be considered rejected.
4	NYPD should add additional checkboxes to the T.R.I. worksheet to allow for more specificity in describing the force used by an officer, including a closed fist strike, an open hand strike, and a knee strike.	**Changed from Partially Implemented to Implemented** In 2019, NYPD made a series of changes to its use-of-force policies, including "T.R.I. 2.0." As noted in the two previous Annual Reports, while these changes did not actually add the check boxes proposed, these changes accomplished the same goal by capturing similar information using drop-down menus and other dynamic forms in the T.R.I. 2.0 system. In practice, OIG-NYPD observed that T.R.I. 2.0 appeared to be satisfying the spirit of this recommendation. Three years later, NYPD's T.R.I. 2.0 revisions have proven sustainable and continue to satisfy the spirit of this recommendation. Therefore, this recommendation is considered implemented.
5	NYPD should add a section to the T.R.I. worksheet that prompts officers to indicate where exactly on the person's body force was used.	**Changed from Partially Implemented to Implemented** As noted in the two previous Annual Reports, while these changes did not actually add the check boxes proposed, these changes accomplished the same goal by capturing similar information using drop-down menus and other dynamic forms in the T.R.I. 2.0 system. In

		practice, OIG-NYPD observed that T.R.I. 2.0 appeared to be satisfying the spirit of this recommendation. Three years later, NYPD's T.R.I. 2.0 revisions have proven sustainable and continue to satisfy the spirit of this recommendation. Therefore, this recommendation is considered implemented.
6	NYPD should impose (a) an "end of tour" deadline by which officers must complete a required T.R.I. form, with appropriate exceptions, and (b) appropriate discipline against officers who fail to meet the deadline, except when certain exceptions apply.	**Unchanged: Partially Implemented** NYPD reports that it has made no changes towards full implementation at this time. Without any changes since last year, this recommendation remains partially implemented.
8	NYPD should reinstate the "Force Used" checkbox on the arrest-processing stamp used in precinct command logs and add an entry on the stamp for force details and the T.R.I. incident number.	**Unchanged: Rejected** NYPD continues to reject this recommendation and has taken no steps towards implementation. NYPD maintains that this recommendation should be "rescinded" as it is overly "cumbersome," no longer required by the patrol guide, and made redundant by the T.R.I. 2.0 process. OIG-NYPD stands by its recommendation.
9	NYPD should prompt desk officers to record the details of a force incident and the T.R.I. incident number in the command log, including details from the "Force Used" checkbox on the arrest-processing stamp, as required by Patrol Guide Series 221.	**Unchanged: Rejected** NYPD continues to reject this recommendation and has taken no steps towards implementation. As with recommendation 8, the benefit of this recommendation applies not only to data capture, but also to the system of mutual accountability created by interconnected levels of responsibility in the use-of-force reporting process. The command log requirement created a system whereby the desk officer and arresting officer both relied on each other to comply with the regulation at the time of booking, and therefore held each other accountable while the arrest was still being processed. The T.R.I. 2.0 system has not replaced this kind of ad-hoc interaction at booking. OIG-NYPD stands by its recommendation.

10	NYPD must enhance supervisory review of all arrest-related documentation at the local command level. In high-volume commands, NYPD should assign specially-trained supervisors at the rank of sergeant or above to carefully review such documents during arrest processing to ensure that all uses of reportable force are properly documented.	**Changed from Partially Implemented to Implemented** As noted in the two previous Annual Reports, none of the T.R.I. 2.0 changes addressed this recommendation explicitly. In practice, however, OIG-NYPD observed that T.R.I. 2.0 appeared to satisfy the spirit of this recommendation. Three year later, NYPD's T.R.I. 2.0 revisions have proven sustainable and continue to satisfy the spirit of this recommendation. Therefore, this recommendation is considered implemented.
15	NYPD should revise policies to ensure that the narrative or "Remarks" section of Medical Treatment of Prisoner forms include fact-specific details sufficient to explain the individual's condition and, where known, what caused the condition. If an individual sustained an injury in the course of the police encounter, the form should specify the type of injury and its cause.	**Changed from Partially Implemented to Implemented** As noted in the two previous Annual Reports, none of the T.R.I. 2.0 changes addressed this recommendation explicitly. In practice, however, OIG-NYPD observed that T.R.I. 2.0 appeared to satisfy the spirit of this recommendation. Three year later, NYPD's T.R.I. 2.0 revisions have proven sustainable and continue to satisfy the spirit of this recommendation. Therefore, this recommendation is considered implemented.
18	NYPD should conduct an annual audit of T.R.I. compliance and include the results in its annual and public Use-of-Force report.	**Unchanged: Partially Implemented** NYPD continues its monthly T.R.I. audits as part of its monthly Force Review Meetings or "ForceStat." In 2020, NYPD began making much of this data publicly available on its "NYPD Force Dashboard." This public dashboard, however, has no information regarding T.R.I. compliance, only use-of-force statistics based on T.R.I. data. While NYPD should be commended for making available this public dashboard (see recommendation 21 below), this recommendation is not fully implemented without the publication of the audit results for T.R.I. compliance.
21A	NYPD should use data from T.R.I. forms to publish annual Use-of-Force reports that identify and analyze trends in all force categories. The report should	**Unchanged: Partially Implemented** NYPD has previously rejected any public reporting requirements that were not explicitly required by law.

	contain all information currently mandated by law and include the following trend analyses: A) All force encounters disaggregated by the reason force was used;	Starting in 2020, however, NYPD began making detailed statistics on use-of-force data from T.R.I.s publicly available on its "NYPD Force Dashboard." This new tool satisfies many of the subparts of recommendation 21. Specifically, with regard to this recommendation, the Dashboard includes summary statistics for the "Basis of Encounter." However, that information largely concerns the reason for the interaction that led to injuries, not the reason why force was used. Because the public dashboard represents real change in the Department's willingness to disclose, it would take only a few tweaks and additions to achieve full implementation. Therefore, this recommendation is partially implemented.
21D	D) Commands with the highest rates of force; • Is the frequency of force consistent with crime and arrest rates in these commands? • Are certain units more or less likely to employ force?	**Unchanged: Partially Implemented** The NYPD Force Dashboard makes statistics on use-of-force data from T.R.I.s publicly available, including summary data for each NYPD precinct. A user can select individual or multiple precincts and receive summary statistics for incident count, type of force, and basis for encounter. This data can be independently cross referenced with existing public CompStat 2.0 data to answer the hypothetical questions posed by this recommendation. However, the Dashboard only provides information by NYPD Precinct; it does not currently provide information on non-precinct commands such as Transit Bureaus, PSAs, commands in the Detective Bureau, and other specialized units. For this recommendation to be considered implemented, only a few tweaks and additions are needed. Because the dashboard provides data by NYPD Precinct, but not by other non-precinct commands, the status is changed from rejected to partially implemented.

REVIEW OF NYPD'S IMPLEMENTATION OF PATROL GUIDE PROCEDURES CONCERNING TRANSGENDER AND GENDER NONCONFORMING PEOPLE

November 21, 2017 Report

In 2012, following negotiations between NYPD, representatives of the Lesbian, Gay, Bisexual, Transgender and Queer (LGBTQ) community and members of the New York City Council, the Department revised its Patrol Guide to address officer approaches to interacting with members of the public who identify as transgender and gender nonconforming (TGNC) while they are being held in custody. Five years after the adoption of those 2012 revisions, OIG-NYPD initiated an evaluation of the changes and their implementation. The resulting 2017 report included nine recommendations for improvements.

As part of its efforts to ensure compliance with the revised Patrol Guide, NYPD released an internal bulletin entitled "Interactions with Members of the Transgender & Gender Nonconforming Communities" in 2020. That document outlined the Patrol Guide procedures regarding gender identity and expression for personnel. A companion guidebook on the topic created by the Department remains in circulation.

In 2021, the City passed legislation clarifying CCRB's authority to investigate complaints of biased policing (including LGBTQ-related complaints) made against uniformed officers, subsequent to OIG-NYPD's 2019 report regarding complaints of biased policing. As a result, CCRB created the Racial Profiling and Bias Based Policing Unit, which it is in the process of fully staffing. Moving forward, when allegations of such misconduct are substantiated, CCRB will recommend disciplinary actions for adoption by the Department. At present, those policy and practice changes have not been fully implemented as CCRB continues prepare for the integration of those duties into agency operations.

OIG-NYPD's assessment of the Department's progress toward the implementation of this Report's recommendations, including those which might be affected to some degree by the transfer of authority to CCRB, will continue.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has implemented five of the nine recommendations issued in this Report. Those recommendations (#2-4, 7) not listed below were implemented prior to the issuance of this Annual Report and can be found in Appendix A. The statuses of the outstanding recommendations are as follows.

REVIEW OF NYPD'S IMPLEMENTATION OF PATROL GUIDE PROCEDURES CONCERNING TRANSGENDER AND GENDER NONCONFORMING PEOPLE (NOVEMBER 2017 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
1	NYPD should provide mandatory in-service training and accompanying resource materials on the 2012 Patrol Guide revisions to all uniformed members through the NYPD-U webinar platform. Training attendance and completion should be tracked to ensure that all members of the police force have received this training. NYPD should conduct this training within the next six months.	**Changed from Accepted in Principle to Implemented** NYPD reports that since 2012, 47,131 members of service, 90.3% of all personnel, have received the required Equal Employment Opportunity (EEO) training, which includes a module on LGBTQIA+ Diversity and Inclusion, and relevant Patrol Guide revisions. Participation data is collected by the Office of the Chief of Training. In 2021, the Department also issued two updates to the Patrol Guide intended to increase inclusivity for staffers. The first broadened the ways in which employees may update personal information electronically using the Central Personnel Resource System (CPRS), while the second modified the procedure entitled "Member of the Service Seeking to Notify the Department of Transgender or Gender Non-Conforming Transition or Status" to include the personal pronoun "their" in addition to the standard "his" or "her." Previously developed tools including a gender identity and expression guide, a gender inclusive language resource and an LGBTQ terminology reference are available to members of service via the internal Office if Equity and Inclusion website. On the basis of those procedural and policy changes, this recommendation is implemented.
5	Within six months, NYPD should report to DOI whether and how the Department will change remaining forms and databases to record an individual's preferred name in a separate field.	**Unchanged: Accepted in Principle** NYPD reports that it has continued to delay the revision of all relevant forms and databases as recommended pending consultation with relevant community groups. Until a consensus has been reached, a separate field to capture the preferred names of those in custody will not be made universally available. OIG-NYPD will continue to monitor the issue until the recommendation is fulfilled.

6	On a periodic basis, NYPD should make sure that police stations are using updated forms, particularly those documents that are intended to comply with the 2012 revisions.	**Unchanged: Accepted in Principle** According to NYPD, representatives of the Quality Assurance Division (QUAD) conduct audits of precincts on a routine basis to ensure that the sites are compliant with a range of agency directives on subjects including EEO regulations, which capture LGBTQ-related themes. The assessments include the review of the content of posters, bulletins and other distributed resources. However, OIG-NYPD was not provided with information sufficient to determine whether NYPD is auditing police stations' use of the updated forms, as was intended to comply with the 2012 revisions. As such, the status of the recommendation remains unchanged. OIG-NYPD will continue to monitor the issue.
8	NYPD Internal Affairs Bureau's complaint system should be configured to categorize and track all LGBTQ-related allegations that implicate biased conduct, and not just "profiling." LGBTQ-related allegations involving bias would include violations of the 2012 Patrol Guide revisions and "offensive language."	**Unchanged: Rejected** Despite the pending transfer of biased policing investigative authority from NYPD to CCRB, the tracking procedures proposed for LGBTQ-related allegations in the recommendation would still fall within the purview of IAB and its complaint management system. As such, the recommendation remains applicable and its status unchanged. OIG-NYPD will continue to monitor this issue.
9	IAB should report patterns and trends associated with LGBTQ-related complaints to NYPD's LGBT Liaison to the Police Commissioner as well as to DOI pursuant to NYPD's reporting obligations under Local Law 70.	**Changed from Accepted in Principle to Rejected** Although NYPD's Risk Management Bureau tracks LGTBQ-related complaints for its Early Intervention Program, IAB does not analyze LGBTQ-related complaint data for patterns and trends, nor does it send such information to OIG-NYPD. OIG-NYPD maintains that production of this information is required by Local Law 70. OIG-NYPD will continue to monitor this issue.

WHEN UNDOCUMENTED IMMIGRANTS ARE CRIME VICTIMS: AN ASSESSMENT OF NYPD'S HANDLING OF U VISA CERTIFICATION REQUESTS

July 28, 2017 Report

Law enforcement agencies rely on victim cooperation in the investigation and prosecution of crimes. However, for undocumented people who are victims of crimes, fear of deportation can stand in the way of cooperation—a fact that perpetrators readily exploit. The U nonimmigrant status visa (U visa), a special visa provided to undocumented victims of certain qualifying crimes who provide assistance to officials in the investigation and prosecution of those crimes, is intended to address this concern. A certification of cooperation from a local law enforcement agency is required to obtain this visa. In 2017, OIG-NYPD conducted a review of NYPD's U visa certification program to ensure that it was fair and efficient and provided the protection envisioned by the program.

The Office found that NYPD had taken commendable steps to improve its U visa program and to work with, protect, and gain the trust of the undocumented immigrant community. However, the Report identified concerns about the Department's application of certification criteria, its reliance on criminal background checks to deny certification requests, and its practice of referring certification requests to other agencies. The Report contained ten recommendations for strengthening NYPD's U visa certification program. An assessment of NYPD's continued progress on the status of the remaining seven recommendations follows.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has implemented three of the ten recommendations issued in this Report. Those recommendations (2, 5, 8) not listed below were implemented prior to the issuance of this Annual Report, and are listed in Appendix A. The statuses of the outstanding recommendations are as follows.

WHEN UNDOCUMENTED IMMIGRANTS ARE CRIME VICTIMS: AN ASSESSMENT OF NYPD'S HANDLING OF U VISA CERTIFICATION REQUESTS (JULY 2017 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
1	NYPD should develop concrete, written standards on how to conduct an assessment of an applicant's criminal background and on the types of criteria that warrant denial of the certification request.	**Unchanged: Rejected** Since the publication of this Report, NYPD has asserted that this recommendation is addressed by federal guidelines and in Patrol Guide § 212-111 and Administrative Guide § 308-07, which are publicly available. Neither Patrol Guide § 212-111 or A.G. § 308-07 directly address what types of criminal histories will result in a

		certification denial, and federal guidelines do not require local agencies to conduct criminal background checks. OIG-NYPD maintains that written standards regarding criminal background checks are important in ensuring consistency and transparency in how U visa certification decisions are made by NYPD. This recommendation remains rejected.
3	If NYPD's investigative file states that the applicant was not cooperative but the applicant certification request or other information in the investigative file suggests the applicant had a reasonable basis for not helping law enforcement, NYPD should assess whether the non-cooperation was reasonable by contacting both the NYPD personnel who investigated the incident and the party requesting the U visa certification.	**Unchanged: Partially Implemented** NYPD asserts that DVIU investigators assess whether there was a reasonable basis for the applicant's refusal to cooperate when reviewing the application, and that it uses a form to document its outreach to personnel who conducted the investigation at issue. NYPD also asserts that DVIU investigators have an opportunity to clarify any prior reasons for lack of cooperation when the applicant files for a U visa application. However, NYPD does not *require* a record of this contact. OIG-NYPD maintains that it is equally important to contact the party requesting the U visa certification to obtain that individual's explanation for the subsequent non-cooperation. The recommendation is partially implemented.
4	NYPD should provide a written rationale in its internal file when concluding that the applicant was not a victim of a qualifying crime.	**Unchanged: Rejected** The form NYPD uses to explain why the applicant was not the victim of a qualifying crime only provides a non-exhaustive check list of qualifying crimes. It does not *require* NYPD to provide a detailed written rationale explaining the denial of an application for a U visa. Without *requiring* a written explanation, a non-exhaustive checklist may not provide sufficient information for a denial to be clearly supported. OIG-NYPD maintains that NYPD should ensure that the reason that a crime is not qualifying is clearly stated in each applicant's file in writing. This recommendation remains rejected.
6	NYPD should create and publish its complete standards for certification eligibility.	**Unchanged: Partially Implemented** In 2019, NYPD reported that its standards for certification were explained in the federal guidelines and in Patrol Guide § 212-111 and A.G. § 308-07. According

		to NYPD, these provide guidance for reviewing U visa certification requests. Although NYPD stated that criminal background checks were still part of the U visa certification request process, NYPD has provided no updates regarding written policies outlining the need to conduct background checks, or explaining how to assess whether a particular criminal background check constitutes a public safety concern. OIG-NYPD will continue to monitor this issue.
7	NYPD's denial letters should articulate specific reasons for each denial, using the facts of the case to explain the decision.	**Unchanged: Partially Implemented** According to NYPD, DVIU achieves this by providing the letter listing qualifying crimes mentioned above. This form does not, however, *require* DVIU to list specific facts of the case in order to clarify for the applicant why their case does not qualify. OIG-NYPD will continue to monitor this issue.
9	NYPD should develop written materials regarding the U visa program for dissemination at precincts and other locations where victims may encounter police.	**Unchanged: Accepted in Principle** NYPD has stated that DVIU has finalized a flyer, which is not yet approved by NYPD leadership, to be disseminated to each NYPD precinct regarding the U visa program. The flyer will be available to members of the public as well as members of service. OIG-NYPD will continue to monitor this issue until the materials are disseminated.
10	NYPD should develop informational training on U visas for specialized NYPD units that frequently encounter immigrant communities.	**Unchanged: Accepted in Principle** As mentioned above, NYPD has reported working to finalize U visa related materials for dissemination. In the meantime, OIG-NYPD appreciates that DVIU has begun to refer officers to Patrol Guide § 212-111 as a means of providing U visa training. NYPD reports that approximately 3,297 members of service were trained in this way in 2021, focusing on promotional classes, training sergeants, and Domestic Violence officers.

ADDRESSING INEFFICIENCIES IN NYPD'S HANDLING OF COMPLAINTS: AN INVESTIGATION OF THE "OUTSIDE GUIDELINES" COMPLAINT PROCESS

February 7, 2017 Report

In February 2017, OIG-NYPD released a report detailing NYPD's procedure for handling "Outside Guidelines" (OG) complaints—less severe allegations that fall outside NYPD's Patrol Guide rules. The Report identified inefficiencies and inconsistencies in how NYPD tracks OG complaints as they move from NYPD's Internal Affairs Bureau to the Office of the Chief of Department's (COD) Investigation Review Section (IRS) for handling. These problems included outdated technology incompatible with other NYPD systems, which slowed down the completion of the complaint process.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has implemented three of the six recommendations issued in this Report. Those recommendations (1, 2, 4) not listed below were implemented prior to the issuance of this Annual Report, and are listed in Appendix A. The statuses of the outstanding recommendations are detailed as follows.

ADDRESSING INEFFICIENCIES IN NYPD'S HANDLING OF COMPLAINTS: AN INVESTIGATION OF "OUTSIDE GUIDELINES" COMPLAINT PROCCESS (FEBRUARY 2017 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
3	If an OG investigation has not been completed within 90 days, the assigned supervising investigator should be required to request an extension from COD-IRS in writing, stating the reason for this request.	**Unchanged: Partially Implemented** NYPD's Internal Case Management and Tracking System (ICMT) features automatic notifications that alert commanding officers, executive officers, supervisors and case owners when cases are not assigned within 10 days, after 30 days of inactivity, and when cases are open over 90 days. Additionally, COD-IRS sends daily email reminders for cases that are 75 days or older and 90 days or older. While OIG-NYPD acknowledges the steps NYPD has taken to ensure supervisors are aware of cases open beyond the 90-day deadline, explanation of the reason for investigation extension should be recorded. OIG-NYPD will continue to monitor this issue.
5	NYPD should implement a web-based procedure for communicating the status and results of externally-generated OG	**Unchanged: Partially Implemented** In 2020, NYPD updated its website to include information that instructs community members to

	investigations back to the community members who filed the complaints.	contact IAB in order to inquire about the status of their complaint. This is not the equivalent of providing a web-based procedure to communicate the status of complaints to complainants; therefore, this recommendation remains partially implemented.
6	NYPD should publish quarterly reports on OG complaints.	**Unchanged: Under Consideration** The Department continues to report that it is considering regularly releasing relevant information on OG complaints, as it has since the time of this Report's release in 2017. If NYPD does not make progress by the 2023 Annual Report, the recommendation will be considered rejected.

PUTTING TRAINING INTO PRACTICE: A REVIEW OF NYPD'S APPROACH TO HANDLING INTERACTIONS WITH PEOPLE IN MENTAL CRISIS

January 19, 2017 Report

Reflecting national trends, in 2015, OIG-NYPD began a review of NYPD's approach to the handling of interactions with people in mental health distress. The primary goals of the Crisis Intervention Team (CIT) model, which has been successfully applied in jurisdictions across the country and was adopted by the Department: the improvement of officer-public relations by limiting use of force against those in crisis and reducing instances of incarceration of those with mental health conditions by increasing opportunities for their diversion into publicly facilitated social service networks.

The findings of OIG-NYPD's 2017 Report revealed that while NYPD was following the CIT model in many respects, it was not implementing all aspects of the program. In particular the Department's dispatch system could not direct CIT-trained individuals to all crisis incidents, a practice which OIG-NYPD viewed as likely to minimize use of force by having trained individuals aid people in distress. Instead, whether trained in the CIT approach or not, officers are randomly assigned to encounters with people in crisis. That approach serves to undermine the intention of the training protocols and the program more broadly. Further, OIG-NYPD identified shortfalls in how NYPD managed its CIT efforts, weaknesses in data collection regarding crisis incidents and gaps in the agency's Patrol Guide regarding how officers should approach the mentally vulnerable. As a result, OIG-NYPD made 13 recommendations for procedural or policy improvements.

Since the Report's release, NYPD has accepted in principle or implemented a majority of those proposals. As of October 19, 2021, 16,869 uniformed personnel had completed the CIT curriculum, a number that had not changed since January 2021, due to COVID-19 related limitations, as well as the creation of an MOU with the Department of Health and Mental Hygiene (DOHMH) to aid in the delivery of the course. The Department indicated that the provision of training will resume at an unspecified point in the near future.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has implemented 11 of the 13 recommendations issued in this Report. Those recommendations (1, 4–7, 9–13) not listed below were implemented prior to the issuance of this Annual Report and are listed in Appendix A. The statuses of the outstanding recommendations are as follows.

PUTTING TRAINING INTO PRACTICE: A REVIEW OF NYPD'S APPROACH TO HANDLING INTERACTIONS WITH PEOPLE IN MENTAL CRISIS (JANUARY 2017 REPORT)		
OIG-NYPD'S RECOMMENDATIONS		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
2	NYPD should adjust its dispatch procedures to ensure that officers with CIT training are directed to crisis incidents.	**Unchanged: Partially Implemented** NYPD reports that the development of "Next Generation 911" (NG911) by its contracted vendor may make it possible in the future to direct calls concerning people in crisis to officers trained in CIT. However, according to NYPD, automatic assignment of calls to trained personnel is not currently possible. The integration and testing of the necessary new features into the dispatch system is not anticipated by NYPD until the third quarter of 2024. OIG-NYPD will continue to monitor this issue until NYPD trains all of its uniformed officers in CIT, which would render the recommendation no longer applicable, or until the ICAD system is updated to allow calls to be directed to trained officers.
3	NYPD should create a dedicated mental health unit, or at the very least appoint a CIT coordinator who holds the rank of chief, in order to manage all aspects of a CIT program.	**Changed from Partially Implemented to Implemented** NYPD reports that in December 2019, its Behavioral Health Division (BHD) was established to address the findings of then-Mayor De Blasio's NYC Crisis Prevention and Response Task Force. BHD is responsible for providing management and oversight to NYPD's Co-Response teams that operate citywide to assist those in crisis, coordinating the delivery of the CIT course with the Training Bureau, the assessment of data, the maintenance of NYPD's relationship with DOHMH's Support and Connection centers, and public outreach, among other things. BHD is staffed by five officers including a Chief, a lieutenant, three sergeants, and a detective. The Co-Response Unit, which has been overseen by the Division since October 2021, has 28 assigned personnel including an Assistant Commissioner, 4 sergeants, and 23 uniformed members of service. In fiscal year 2020, the Co-Response teams intervened 7,176 times with individuals in mental crisis.

		Since July 2021, the BHD has been working with various City agencies to support the Behavioral Health Assistance Emergency Response Division (B-HEARD) pilot program, which is pairing EMS providers with social workers to respond to low-level 911 calls involving those in mental distress as an alternative to officer involvement.[12] This approach has been successful in other jurisdictions and seeks to minimize police involvement with individuals in mental crisis. Given the creation and existence of BHD, this recommendation can be considered implemented. OIG-NYPD may reevaluate this recommendation should the Department make substantial operational changes.
8	NYPD should analyze data regarding mental crisis incidents.	**Changed from Accepted in Principle to Partially Implemented** NYPD maintains that it evaluates data related to interactions with people in mental distress using 911 call details, incident reports, and other forms. In addition, data is collected and assessed for the Co-Response Unit, which provides short-term assistance and connects individuals with resources. Quarterly and annual cumulative data regarding the Co-Response Unit and B-HEARD program are available on the Mayor's office of Community Mental Health (OCMH) website. The Department states it has an active role in maintaining and assessing this data. OIG-NYPD will continue to monitor the issue until the Department demonstrates that information related to interactions with individuals in crisis has been analyzed and considered for the purposes of policy development or program improvement.

[12] For more information about the B-HEARD program, please visit the following site: https://mentalhealth.cityofnewyork.us/b-heard

AN INVESTIGATION OF NYPD'S COMPLIANCE WITH RULES GOVERNING INVESTIGATIONS OF POLITICAL ACTIVITY

August 23, 2016

On August 23, 2016, OIG-NYPD released a Report on NYPD's compliance with court-mandated rules governing the investigation of political activity known as the Handschu Guidelines.[13] The Guidelines require, in part, that NYPD document the basis for an investigation, secure specific approvals from senior NYPD officials, and complete the investigation within an approved time-frame.

After a comprehensive review, OIG-NYPD found that documents seeking to extend investigations or to include undercover officers or confidential informants in investigations usually did not have the required information, and that in more than half the cases, investigations continued after the expiration of the approved time frame.

In 2017, the Court monitoring the Handschu Guidelines approved a proposal for modifications. A central element of those resulting Guideline changes was to install a Civilian Representative on NYPD's "Handschu Committee," empowered to report violations of the Handschu Guidelines to the applicable federal court, and to publish reports on NYPD's compliance with the rules.

For more information about the findings and recommendations, a full copy of the Report can be found here.

The six recommendations (1-3, 5, 8, 9) not listed below were implemented prior to the issuance of this Annual Report and are listed in Appendix A; NYPD has not made progress with respect to implementing the remaining five recommendations in this Report. The statuses of the outstanding recommendations are as follows.

AN INVESTIGATION OF NYPD'S COMPLIANCE WITH RULES GOVERNING INVESTIGATIONS OF POLITICAL ACTIVITY (AUGUST 2016 REPORT)		
OIG-NYPD'S RECCOMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
4	For requests to extend a Preliminary Inquiry, NYPD should ensure that Investigative Statements capture fact-specific reasons why further investigative steps are warranted.	**Unchanged: Rejected** NYPD continues to disagree with the Report's finding, asserting that requests to extend Preliminary Inquiries include a full and detailed recitation of the key facts justifying further investigation. NYPD has made no changes relevant to this recommendation since the publication of this Report in 2016.

[13]The Handschu Guidelines were established pursuant to a 1971 federal lawsuit and are codified in NYPD Patrol Guide § 212-72.

6	NYPD's Human Source Authorization Form should require members of NYPD's Intelligence Bureau to specify the role of the undercover officer or confidential informant.	**Unchanged: Rejected** NYPD last provided updates on its Human Source Authorization forms in 2017. When OIG-NYPD reviewed those updates, it determined that the section on the role of the human source included a handful of very broad, generic categories that did not meaningfully describe the anticipated investigative role of the undercover officer or confidential informant, as opposed to specific content specifying the role of the human source. NYPD has made no additional changes relevant to this recommendation.
7	NYPD should specify, when extending use of an undercover or confidential informant, the reason for the extension.	**Unchanged: Accepted in Principle** When OIG-NYPD last reviewed NYPD's updated Human Source Extension memos in 2017, it found that those forms needed to be revised to include more detailed, fact-based reasons for the extensions. OIG-NYPD has no reason to believe that any changes have been made since that time. Despite requests, NYPD has provided no further update. If NYPD does not make progress by the 2023 Annual Report, the recommendation will be considered rejected.
10	NYPD should consolidate its policies and procedures for investigations involving political activity into a unified handbook.	**Unchanged: Accepted in Principle** In preparation for OIG-NYPD's Annual Report released in 2020, NYPD stated "the Intelligence Bureau has finalized the policy guide." Two years later, however, the Department has still not provided a copy of the finalized policy guide or provided any updates. As a result, the status of the recommendation remains unchanged.
11	NYPD should develop written guidelines concerning informational standards for Preliminary Inquiries, Full Investigations, and Terrorism Enterprise Investigations.	**Unchanged: Rejected** NYPD has made no changes relevant to this recommendation since the publication of this Report in 2016.

AN ANALYSIS OF QUALITY-OF-LIFE SUMMONSES, QUALITY-OF-LIFE MISDEMEANOR ARRESTS, AND FELONY CRIME IN NEW YORK CITY, 2010-2015

June 22, 2016 Report

In June 2016, OIG-NYPD issued a Report that examined whether quality-of-life criminal summonses (also known as "C-summonses") and misdemeanor arrests contributed to reductions in the occurrence of felony crimes, as had been long asserted by NYPD in publications such as "Broken Windows and Quality-of-Life Policing in New York City."[14] The OIG-NYPD Report found that dramatic declines in C-summons activity over the period of 2010-2015 did not correlate with elevations in the seven major categories of felony crimes. It was also observed that C-summons enforcement was not evenly distributed across the five boroughs. High rates of such activity by officers were found to be concentrated in precincts with larger proportions of Black and Hispanic residents, among New York City Housing Authority residents, and males aged 15–20. In contrast, precincts with significant numbers of White residents had lower rates of such policing.

As a result of those observations, OIG-NYPD issued seven recommendations to the Department, including support for the introduction of data-driven approaches to assessing its quality-of-life enforcement tactics and policies. Over the nearly six-year period since the report's release, NYPD has increased the information available for public analysis on its website and the City's Open Data Portal, and the rates of quality-of-life enforcement have remained low.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has implemented four of the seven recommendations made in this Report. Those recommendations (4-7) not cited below were implemented prior to the issuance of this Annual Report and are outlined in Appendix A. The statuses of the outstanding recommendations are as follows.

AN ANALYSIS OF QUALITY-OF-LIFE SUMMONSES, QUALITY-OF-LIFE MISDEMEANOR ARRESTS, AND FELONY CRIME IN NEW YORK CITY, 2010-2015 (JUNE 2016 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
1	NYPD should assess the relative effectiveness of quality-of-life summonses, quality-of-life misdemeanor arrests, and other disorder reduction strategies in reducing felony crime,	**Unchanged: Rejected** Since 2016, NYPD has not completed an assessment of the relationship between criminal summons issuance, misdemeanor arrests and the occurrence of felony crimes

[14] Bratton, W.J. (2015). Broken windows and Quality-of-Life policing in New York City. *New York City Police Department*. http://www.nyc.gov/html/nypd/downloads/pdf/analysis_and_planning/qol.pdf.

	demonstrating whether statistically significant relationships exist between these particular disorder reduction tactics and specific felony crimes.	due to a decrease in these enforcement actions following the adoption of the Criminal Justice Report Act (CJRA). On March 23, 2022, NYPD Commissioner Sewell announced that Neighborhood Safety Teams will expand their focus to include enforcement of quality-of-life related offenses. NYPD's justification for this policy and procedural shift is grounded in a hallmark of the "Broken Windows" policing era rhetoric that quality-of-life violations precede acts of violence.[15] This return to earlier practices creates the potential for the recurrence of the same disparate impact issues that were captured by the 2016 report. As such, OIG-NYPD will continue to monitor the issue and encourages the Department to consider the relationship between the policing of low-level offenses and the occurrence of felony crimes.
2	NYPD should conduct an analysis to determine whether quality-of-life enforcement disproportionately impacts black and Hispanic residents, males aged 15-20, and NYCHA residents.	**Unchanged: Rejected** In the past, NYPD asserted that the completion of a disproportionality effect analysis of its quality-of-life policing data is unnecessary due to the diminished state of enforcement regarding the related offenses. With the March 23, 2022 announcement by the NYPD Police Commissioner that quality-of-life enforcement will resume, this recommendation is highly relevant. There is no indication from the Department, however, that it intends to adopt this recommendation at any point in the future. OIG-NYPD will continue to monitor the issue and maintains that internal evaluation of the impact of Department policies and protocols, which are suspected of having a disparate impact on groups across the city, should occur regularly.
3	NYPD should expand consideration regarding quality-of-life	**Unchanged: Rejected** In the past, NYPD argued that this recommendation was no longer applicable as it had wound down its

[15] The announcement regarding the reintroduction of the quality-of-life policing initiative was made by the Department on March 23, 2022 in a press release entitled "NYPD Announces Citywide Crime and Quality-of-Life Enforcement Initiative," which was referenced on the agency website at: https://www1.nyc.gov/site/nypd/news/p00040/nypd-citywide-crime-quality-of-life-enforcement-initiative.

	enforcement beyond short-term real-time conditions.	enforcement of quality-of-life offenses. With the March 23, 2022 announcement by the NYPD Police Commissioner that quality-of-life enforcement will resume, this recommendation is highly relevant. There is no indication from the Department that it intends to implement this recommendation. OIG-NYPD stands by its recommendation. NYPD should consider the long-term, adverse implications for vulnerable populations of quality-of-life enforcement, particularly considering the recent announcement of a returned focus on low level violations.

POLICE USE OF FORCE IN NEW YORK CITY: FINDINGS AND RECOMMENDATIONS ON NYPD'S POLICIES AND PRACTICES

October 1, 2015 Report

Police officers are empowered and at times obligated to use force against members of the public when appropriate. In 2015, OIG-NYPD released this Report following an investigation of NYPD's policies on force, how force incidents are reported, how NYPD trains officers regarding the use of force, and the disciplinary process for substantiated cases of excessive force.

OIG-NYPD found that NYPD's use-of-force policy provided little guidance to individual officers on what actions constitute force and provided insufficient instruction on de-escalation. Further, it concluded that NYPD's documentation and reporting processes left the Department unable to accurately and comprehensively capture data on how frequently officers use force. The Office also found that NYPD frequently failed to impose discipline even when provided with evidence of excessive force.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has implemented 12 of the 15 recommendations issued in this Report—an increase from last year's Annual Report where 11 of 15 recommendations were implemented. There was no movement, however, on the three recommendations that remain unimplemented. Those recommendations (1-3, 5-10, 12, 14) not listed below were implemented prior to this Annual Report, and are listed in Appendix A. The statuses of the outstanding recommendations are as follows.

POLICE USE OF FORCE IN NEW YORK CITY: FINDINGS AND RECOMMENDATIONS ON NYPD'S POLICIES AND PRACTICES (OCTOBER 2015 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
4	With respect to the newly created form, NYPD should require all officers—whether the subject of a force investigation or a witness to a use of force—to document and report all force incidents. When completing this document, officers should use descriptive language to articulate the events leading up to the use of force in encounters with the public, the reason why the force was used, and the level and type of force used.	**Unchanged: Partially Implemented** The only outstanding portion of this recommendation is that NYPD require witnesses to document and report all force incidents. NYPD provided no update towards implementation of this final outstanding portion. Therefore, this recommendation remains partially implemented.

11	NYPD should review use-of-force trends to identify which categories of officers (e.g., by years of service and/or duty assignments) are most in need of de-escalation and use-of-force in-service training, and then implement such instruction.	**Changed from Accepted in Principle to Implemented** Building on the progress identified in last year's Annual Report, NYPD implemented new policies and procedures involving NYPD Risk Management Bureau's implementation of the Early Warning System. This sufficiently addresses the concern that while progress towards implementation was being made, it was not formally documented. This recommendation is implemented.
13	NYPD should collect, review, and compare data regarding disciplinary penalties imposed in use-of-force cases and report on the effects of disciplinary penalties on the frequency of incidents of excessive force. NYPD should publish data in the previously mentioned annual report (Recommendation #6) on the number and percentage of cases in which the Police Commissioner reduces or declines discipline.	**Unchanged: Accepted in Principle** NYPD published disciplinary data in its 2020 "Discipline in the NYPD" report.[16] While the Department informed OIG-NYPD in 2019 that it anticipated future public disciplinary reports will include information on the number of downward departures made by the Police Commissioner, this has not occurred. There was no information in the 2020 report regarding downward departures. OIG-NYPD will continue to monitor this issue to ensure full implementation.
15	NYPD should share a subject officer's force monitoring history with CCRB's Administrative Prosecution Unit (APU) since this information is a critical element that must be taken into consideration when CCRB recommends penalties.	**Unchanged: Partially Implemented** NYPD reports that it has made "no changes as of this time." Without NYPD taking any further steps towards implementation, this recommendation remains partially implemented.

[16] *Discipline in the NYPD*, N.Y.P.D., https://www1.nyc.gov/site/nypd/stats/reports-analysis/discipline.page (last visited Mar. 30, 2021).

BODY-WORN CAMERAS IN NEW YORK CITY: AN ASSESSMENT OF NYPD'S PILOT PROGRAM AND RECOMMENDATIONS TO PROMOTE ACCOUNTABILITY

July 30, 2015 Report

In September 2014, NYPD launched a small pilot program to evaluate the use of body-worn cameras (BWCs) by members of the force. OIG-NYPD conducted a comprehensive review of the program, with a particular focus on the policies and practices developed by the Department concerning usage and preservation of BWC footage. Data collected from participants in the program revealed disparate and inconsistent practices concerning camera activation despite NYPD policies. In its July 2015 report, OIG-NYPD made 23 recommendations to improve the use of the technology. Many of those proposals were implemented.

Of the three remaining recommendations that the Department has yet to implement, NYPD has maintained its objection to the proposal that officers named as subjects or witnesses in misconduct inquiries not be permitted to view their BWC footage until they have submitted formal statements outlining the details of the incidents during which the problematic behavior or activities occurred. Over the nearly seven year period that has elapsed since the 2015 report publication, a number of other jurisdictions, including Atlanta, Baltimore, and San Francisco, have implemented policies that have placed some limits on officer access to footage while under scrutiny for improper conduct.[17] OIG-NYPD believes that NYPD should likewise restrict viewing of BWC footage by its officers before they have provided their initial statements, to preserve investigative integrity. Failure to do so could potentially lead to lessened public trust in law enforcement.

For more information about the findings and recommendations, a full copy of the Report can be found here.

NYPD has implemented 20 of the 23 recommendations issued in this Report. Those recommendations (1.1-3.4, 4.1, 4.3, 5.1, 5.2, 5.3, 6.2, 7.1, 8.1, 8.2, 9) not listed below were implemented prior to the issuance of this Annual Report, and are listed in Appendix A.

[17] The data that were examined to make the comparative statement with relation to the privileges possessed by officers in other jurisdictions to view body worn camera footage in situations when they are beneath evaluation for misconduct was derived from a joint effort by The Leadership Conference on Civil and Human Rights and Upturn. Police Body Worn Cameras: A Policy Scorecard. (November 2017). https://www.bwcscorecard.org/.

BODY-WORN CAMERAS IN NEW YORK CITY: AN ASSESSMENT OF NYPD'S PILOT PROGRAM AND RECOMMENDATIONS TO PROMOTE ACCOUNTABILITY (JULY 2015 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
4.2	NYPD should integrate BWC footage review into NYPD's field training program.	**Unchanged: Accepted in Principle** The Department's position is that by encouraging Field Training Officers (FTOs) and training sergeants to use BWC footage in trainings, and including this encouragement in the FTO program guide, this recommendation is satisfied. The Department states that the 24,000 members of the force "regularly assigned to patrol duties throughout the city are equipped with body worn cameras," with training provided by Police Academy personnel.[18] A related memo #31-18 entitled "Body Worn Cameras: Supervisor Responsibilities" available to patrol commanders, training sergeants, and Integrity Control Officers (ICOs) instructs them to "periodically review BWC footage to provide positive feedback and address any performance or tactical deficiencies observed." OIG-NYPD will continue to monitor this recommendation until BWC footage review is included as a standard part of the FTO program.
6.1	Access to BWC recordings should be limited where officers are under investigation or are witnesses in misconduct investigations.	**Unchanged: Rejected** NYPD has maintained that access to body-worn camera footage related to an active investigation is restricted with respect to most parties, including officers. NYPD's Force Investigation Division (FID) and Internal Affairs Bureau (IAB) use BWC footage regularly in their operations. FID determines who can access footage relevant to an investigation, while IAB imposes access limitations on a case by case basis ensuring that officers under investigation are not alerted to such activity until relevant information is collected. NYPD notes that it maintains BWC access logs, which is intended to serve as a deterrent to misconduct.

[18] The figure of 24,000 police officers, detectives, sergeants and lieutenants comprising the members of the force who are regularly assigned to patrol duties was drawn from NYPD's description of the Body-Worn Camera program provided on the agency website at: https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/body-worn-cameras.page.

		However, any officer who is subject to an internal investigation can view BWC footage relevant to their case, when deemed appropriate by the supervising investigator, prior to providing an official statement, in direct contrast with OIG-NYPD's recommendation. The Department believes that advanced review of BWC footage allows officers to provide statements which are as accurate as possible. OIG-NYPD maintains that officers should be required to submit statements before viewing BWC footage. Viewing privileges should assist with providing supplemental reports when "their initial testimony diverges from the relevant video, and NYPD should not discipline officers solely on the basis of discrepancies absent evidence of intent to mislead." OIG-NYPD will continue to monitor this issue.
7.2	NYPD should ensure fairness between citizens' and officers' rights to view BWC footage.	**Unchanged: Accepted in Principle** OIG-NYPD's recommendation urges the Department to prevent a member of the public or an officer from having access to BWC footage until the individual has provided a statement about an incident. NYPD reports that it permits members of the public who have witnessed incidents/encounters of concern to view footage over the course of criminal investigations, if doing so does not violate legal and policy restrictions. The Patrol Guide requires members of service to confer with a prosecutor before showing a witness BWC footage. However, OIG-NYPD holds that that practice does not address viewing rights for the public in officer misconduct investigations conducted by IAB. In that context, access to footage should be as convenient as possible for participant witnesses, which is not the current situation. Additionally, NYPD reports that after BWC footage is provided to CCRB, the decision to share it with complainants lies with that agency. The Department also reports that it responds to FOIL requests from the public pursuant to the New York State Public Officers Law § 87 and § 89. OIG-NYPD will continue to monitor this issue until the recommendation is adopted as written.

USING DATA FROM LAWSUITS AND LEGAL CLAIMS INVOLVING NYPD TO IMPROVE POLICING

April 21, 2015 Report

Noting the rising number of costly civil claims and lawsuits against NYPD, along with the substantial financial burden on City taxpayers, in April 2015, OIG-NYPD released a Report on how NYPD can better collect and use police litigation data to improve officer performance, identify trends, and make important process improvements. The Report recommended NYPD track more qualitative data, including details about the nature of the claims, the core allegations, information about the subject police officer, the location of the alleged incident, and the home address of the plaintiff. OIG-NYPD also recommended NYPD create an interagency working group with the Law Department and the Comptroller's Office to coordinate the collection and exchange of litigation data.

For more information about the findings and recommendations, a full copy of the Report can be found here.

This Report issued five recommendations, of which three have been implemented by NYPD. NYPD has not implemented any additional recommendations since last year's Annual Report. Those recommendations (1.1, 1.2, 2) not listed below were implemented prior to the issuance of this Annual Report, and are listed in Appendix A. The statuses of the outstanding recommendations are as follows.

USING DATA FROM LAWSUITS AND LEGAL CLAIMS INVOLVING NYPD TO IMPROVE POLICING (APRIL 2015 REPORT)		
OIG-NYPD'S RECOMMENDATION		**NYPD RESPONSE AND OIG-NYPD ASSESSMENT**
1.3	NYPD should perform a qualitative review of the most relevant data contained within legal claims and lawsuits against NYPD. Specifically: the location of the alleged incident and address of the plaintiff(s).	**Unchanged: Partially Implemented** NYPD has not made any progress towards implementing this recommendation since 2018, when it began reviewing the location of alleged incidents in its analysis of claims/core allegations. NYPD continues to decline to collect and analyze the available data regarding plaintiff addresses, maintaining that such information is not valuable and could instead open up the Department to lawsuits. OIG-NYPD will continue to monitor this issue.
3	NYPD should provide the public with details about NYPD's Early Intervention System and its litigation data analysis team and	**Unchanged: Partially Implemented** NYPD has published details about the early intervention system on its public-facing website, along with responses to court filings, responses to various OIG-NYPD reports, a yearly report to the City Council,

	solicit suggestion for further development.	several quarterly aggregate data reports, and Administrative Guides 320-22 and 320-54. However, NYPD has not published information in a similarly transparent manner regarding its litigation data analysis team. Additionally, NYPD has not solicited suggestions for further development of early intervention system or the litigat-ion data analysis team from the public. Therefore, OIG-NYPD has deemed this recommendation partially implemented. OIG-NYPD will continue to monitor this issue.

OBSERVATIONS ON ACCOUNTABILITY AND TRANSPARENCY IN TEN NYPD CHOKEHOLD CASES

January 12, 2015 Report

OIG-NYPD's issued its first Report on January 12, 2015, assessing NYPD's disciplinary process for officers who were found to have improperly used chokeholds. As part of the investigation, OIG-NYPD reviewed ten chokehold cases substantiated by the Civilian Complaint Review Board and subsequently handled by the Department Advocate's Office records. OIG-NYPD found that in nine of the ten cases reviewed, although CCRB recommended Administrative Charges, the highest level of discipline, NYPD departed from CCRB's recommendation every time and recommended lesser penalties or no discipline at all.

OIG-NYPD's Report made four recommendations that have all been implemented by NYPD. Those recommendations are listed in Appendix A.

For more information about the findings and recommendations, a full copy of the Report can be found here.

IV. *APPENDIX A: RECOMMENDATIONS IMPLEMENTED OR NO LONGER APPLICABLE PRIOR TO 2022*

The following recommendations were IMPLEMENTED by NYPD prior to the April 2022 Annual Report. As a result, no further update is required.

AN INVESTIGATION OF NYPD'S OFFICER WELLNESS AND SAFETY SERVICES (SEPTEMBER 2019 REPORT)	
1	To guide the Department's efforts and memorialize the Department's commitments, NYPD should develop an overarching Mental Health and Wellness policy that articulates goals, establishes standards, and outlines relevant programs and resources. This policy would encompass the recommendations in this Report, the work of the Mental Health and Wellness Coordinator, and the efforts of the Mental Health and Wellness Task Force and the Health and Wellness Section.
4	NYPD's Health and Wellness Section should have access to specific internal data that would assist the Section with identifying behavioral themes or trends in the conduct of NYPD personnel so as to inform the work of the Section.
5	NYPD should retain outside mental health experts to review and audit the current range of Department-wide health and wellness trainings provided by NYPD to personnel, many of which are new, and ask these experts to recommend to NYPD what additional training, if any, should be developed and delivered.
8	NYPD should establish clear written procedures on debriefing NYPD personnel in the wake of critical incidents and follow up with these officers after the debriefing sessions.
9	According to NYPD, its Mental Health and Wellness Coordinator has collaborated with numerous external groups and counterparts that are experts on resilience. Some examples include: Columbia University Medical Center, Police Executive Research Forum (PERF), and the national Fraternal Order of Police.
10	NYPD should establish a mandatory program that provides NYPD personnel approaching retirement with helpful information on the availability of support services following separation, adjusting to life as a member of the public, financial advisement, and medical and retirement benefits.
COMPLAINTS OF BIASED POLICING IN NEW YORK CITY: AN ASSESSMENT OF NYPD'S INVESTIGATIONS, POLICIES, AND TRAINING (JUNE 2019 REPORT)	
4	Consistent with NYPD's investigative training, NYPD should amend its *written* investigative procedures to document the number of attempts that investigators must make to contact complainants for interviews when investigating biased policing complaints before the case is closed.
5	NYPD should amend its *written* investigative procedures to require investigators to attempt to interview incarcerated complainants when such complainants are being held at a jail located within the five boroughs of New York City (regardless of whether the jail is managed by NYC Department of Correction, NYS Department of Corrections and Community Supervision, or the federal Bureau of Prisons).
6	Consistent with NYPD's investigative training, NYPD should amend its *written* investigative procedures to state that a guilty status, plea, or conviction does not resolve the issue of whether an officer or a non-uniformed employee engaged in discriminatory conduct, even if

	the criminal matter and the complaint of biased policing arise from the same set of underlying facts.
7	NYPD should amend its *written* investigative procedures to state that a complainant's previous criminal history should not be dispositive of whether a biased policing allegation is substantiated. Where NYPD does regard the complainant's previous criminal history as a factor in a non-substantiation decision, the investigator should articulate how the criminal history impacted the decision and the investigator must still complete a full investigation of the allegation.
8	Consistent with NYPD's investigative training, the Department should amend its *written* investigative procedures to state that a subject officer's race/ethnicity or other protected status should not be determinative in deciding whether to substantiate a biased policing allegation, even when the officer (or non-uniformed employee) and complainant identify as members of the same race/ethnicity or other protected group.
10	NYPD investigators should not be assigned investigations of biased policing allegations until they complete the formal "Profiling and Bias-Based Policing" training for investigating such complaints.
13	Deputy Chiefs should receive training and reminders emphasizing that biased policing investigations can only be closed when proper investigative protocols have been followed, unless such protocols were impossible to implement or inapplicable to the particular case.
22	City agencies that handle biased policing complaints (NYPD, CCRB, CCHR) should convene within the next four months to address the findings and recommendations in OIG-NYPD's investigation. This would, for example, include developing standard categories and definitions for how these complaints are grouped and sub-classified.
ONGOING EXAMINATION OF LITIGATION DATA INVOLVING NYPD (APRIL 2018 REPORT)	
3	NYPD should regularly enter data about claims naming individual officers into its new Risk Assessment Information Liability System (RAILS), or comparable early intervention system, so that NYPD is aware of at-risk officers who may require assistance.
AN INVESTIGATION OF NYPD'S SPECIAL VICTIMS DIVISION—ADULT SEX CRIMES (MARCH 2018 REPORT)	
1	NYPD should immediately increase the staffing level in SVD's adult sex crime units to meet the minimum investigative capacity required by an evidence-backed and nationally-accepted staffing analysis model. To appropriately handle a caseload as seen in 2017, that model would require an additional 21 detectives in Manhattan SVS, 11 detectives in Bronx SVS, 16 detectives in Queens SVS, 21 detectives in Brooklyn SVS, and four detectives in Staten Island SVS.
6	To the extent that it is inevitable that patrol officers may be the first to respond to sexual assaults in exigent circumstances, NYPD should expand existing training, both in-service and at the academy, to include trauma-informed care and best practices regarding sexual assault.
7	NYPD should formally end the "triaging" process for sex crimes—instead, all sex crimes should be investigated and enhanced by SVD detectives, including patrol arrests for "domestic rape" and "acquaintance rape." The implementation of this recommendation will

	have staffing implications that are not accounted for in Recommendation 1 above, and NYPD should, therefore, include appropriate staffing increases in implementing this recommendation.
11	NYPD should review the use of CompStat as the oversight mechanism for SVD.
12	NYPD should increase and publicize existing efforts to encourage victims of sex crimes to come forward and report these crimes to law enforcement. At the same time, NYPD should take new steps to advise policy makers and the public that success in this area will result in an apparent rise in the "index crime numbers" for sexual assault cases, even if the "true" rate of sex crimes remains unchanged.
AN INVESTIGATION OF NYPD'S NEW FORCE REPORTING SYSTEM (FEBRUARY 2018 REPORT)	
1	NYPD should add a field to the "Force Used" section of the arrest report for officers to note the associated T.R.I. incident number(s).
3	NYPD should add a narrative section to the T.R.I. and require officers to provide a full account of the force incident, including specific details on the force used by the officer and/or members of the public, the chronology of the force encounter, as well as any injuries sustained by either.
7	NYPD should require desk officers to question the involved officers about any force used during arrest processing so that the command log accurately reflects the force incident.
11	NYPD should dedicate well-trained and knowledgeable personnel to be available by phone during all shifts to answer questions from command supervisors regarding T.R.I. worksheets and approval. NYPD should consider removing this function from the Internal Affairs Bureau.
12	NYPD should include in Patrol Guide series 221 a clear and unambiguous definition of "reportable force" by officers. The current policy provides a definition of force when used against officers and defines three levels of force by officers, but a lack of clarity still exists for many officers regarding whether certain actions constitute reportable force.
13	NYPD should establish a clear policy that requires arresting officers to select "Yes" on the arrest report in response to the "Force Used" section if any officer used reportable force during the encounter.
14	NYPD should impose appropriate discipline against arresting officers who fail to select "Force Used: Yes" on the arrest report when reportable force is found to have been used.
16	NYPD should provide officers with more training and formal reminders on (a) when and how to complete a T.R.I. form and the importance of submitting the T.R.I. form, and (b) how to write a detailed account of a force encounter (should a narrative section is added to the T.R.I. form).
17	NYPD should provide more training for desk officers, integrity control officers, precinct training sergeants, and other supervisors to (a) ensure T.R.I. compliance and proper supervisory review of completed T.R.I. worksheets, and (b) closely examine the arrest report narratives and the "Force Used" section on the arrest reports to ensure that officers are selecting "Yes" for "Force Used" when force was used.
19	NYPD's Force Review process should include quality-control procedures that seek to improve the accuracy of force reporting not only on T.R.I. forms, but also on arrest reports and other arrest-related documentation.

21	B) Types of interactions leading to injuries;
21	C) Officer use of force based on job tenure and experience;
21	E) Demographic characteristics of members of the public and officers involved in force incidents; • Are there disparities in the types or amount of force used based on age, gender, race, national origin, precinct, or other factors? • What are the reasons for such disparities?
REVIEW OF NYPD'S IMPLEMENTATION OF PATROL GUIDE PROCEDURES CONCERNING TRANSGENDER AND GENDER NONCONFORMING PEOPLE (NOVEMBER 2017 REPORT)	
2	NYPD should create a memo book insert for officers with a summary of the revised LGBTQ protocols. Officers can use this for reference as needed.
3	Community input should be carefully considered and incorporated as appropriate into the curriculum of officer training on LGBTQ issues.
4	All handouts and additional resource materials provided during LGBTQ trainings should be consistent, as appropriate, ensuring that officers receive the same information.
7	NYPD should consult with its LGBT Advisory Committee and re-examine whether and how to record gender identity information of TGNC people on NYPD forms and databases. The collection of this information is a sensitive matter for some members of the LGBTQ community. Any changes in how such information is recorded must not interfere with NYPD's ability to describe and circulate descriptions of suspects and persons of interest for purposes of apprehension.
WHEN UNDOCUMENTED IMMIGRANTS ARE CRIME VICTIMS: AN ASSESSMENT OF NYPD'S HANDLING OF U VISA CERTIFICATION REQUESTS (JULY 2017 REPORT)	
2	When denying a U visa certification request based on the applicant's criminal history, NYPD should articulate, in its internal file, the reasons why the criminal history presents an ongoing public safety concern and warrants denial.
5	If an arrest has been made on the underlying crime, NYPD should evaluate U visa certification requests if the criminal case has closed.
8	NYPD should publish contact information for its reviewers and certifying officials.
ADDRESSING INEFFICIENCIES IN NYPD'S HANDLING OF COMPLAINTS: AN INVESTIGATION OF "OUTSIDE GUIDELINES" COMPLAINT PROCCESS (FEBRUARY 2017 REPORT)	
1	NYPD should update and unify the computer systems it uses to track and manage OG cases by upgrading OCD IRS from BCATS to ICIS (or an ICIS - compatible system).
2	NYPD should establish a uniform timeframe for completing OG investigations and a uniform system of tracking due dates.
4	NYPD should revise the current OG Disposition and Penalty Form to include a box denoting the case's due date as well as a date section for each stage of the investigation.
PUTTING TRAINING INTO PRACTICE: A REVIEW OF NYPD'S APPROACH TO HANDLING INTERACTIONS WITH PEOPLE IN MENTAL CRISIS (JANUARY 2017 REPORT)	

1	NYPD should commit to creating timelines for any changes to its CIT initiative within 90 days of the publication of this Report.
4	NYPD should revise its Patrol Guide to explicitly authorize CIT-trained officers to use the skills learned in CIT training during crisis situations.
5	NYPD should revise its Patrol Guide to require that CIT-trained officers respond to all crisis incidents whenever possible.
6	NYPD should revise its Patrol Guide to allow all officers to use their discretion to refer individuals to officially approved and vetted outside community resources in appropriate incidents.
7	NYPD should either substantially revise one of its current forms or develop a new permanent form to capture more useful data on incidents involving persons in crisis.
9	NYPD should consider training more officers in CIT.
10	NYPD should begin training 911 call takers and dispatchers in at least some aspects of CIT.
11	In every CIT training, NYPD should ensure that its officers interact with people living with mental illnesses.
12	In every CIT training, NYPD should assess the retention of officers' skills.
13	NYPD should provide a manual or reference guide to officers who undergo CIT training.
AN INVESTIGATION OF NYPD'S COMPLIANCE WITH RULES GOVERNING INVESTIGATIONS OF POLITICAL ACTIVITY (AUGUST 2016 REPORT)	
1	For investigations of political activity, NYPD should use a formal mechanism for tracking investigative deadlines and should ensure that, where needed, extensions are approved prior to required deadlines.
2	NYPD should use a formal case tracking mechanism that identifies when investigations advance to the next investigative level.
3	For the use of confidential informants and undercover officers in investigations of political activity, NYPD should use a formal mechanism for tracking expiration deadlines and ensure that extensions are approved prior to the expiration of an authorization.
5	For authorizations and renewals of investigations, NYPD should create controls to ensure that authorizations to renew or extend investigations properly capture the date, signature, and approval of the authorizing officials.
8	NYPD should create controls to ensure that authorizations to use or extend the use of human sources properly capture the date, signature, and approval of the appropriate supervisor.
9	NYPD's Human Source Authorization Form should include the number of the extension request and the date of the last extension.
AN ANALYSIS OF QUALITY-OF-LIFE SUMMONSES, QUALITY-OF-LIFE MISDEMEANOR ARRESTS, AND FELONY CRIME IN NEW YORK CITY, 2010-2015 (JUNE 2016 REPORT)	
4	NYPD should release incident-level and geographically coded data on summonses and misdemeanor arrests.
5	NYPD should release historical incident-level and geographic data.

6	NYPD should ensure that data currently released in yearly formats also include more granular temporal data, including month-to-month formats and incident-level data.
7	All incident-level crime data, from felony arrests and complaints to misdemeanor arrests and summonses, should be released in the same accessible spreadsheet file format (.csv or similar file format).
POLICE USE OF FORCE IN NEW YORK CITY: FINDINGS AND RECOMMENDATIONS ON NYPD'S POLICIES AND PRACTICES (OCTOBER 2015 REPORT)	
1	The NYPD Patrol Guide should include definitional language that provides officers and the public with greater clarity regarding what is meant by "force," "excessive force," and "deadly physical force."
2	NYPD should update Patrol Guide § 203-11 governing use of force and require officers to de-escalate all encounters where appropriate.
3	NYPD should create a separate, uniform use-of-force reporting form.
5	NYPD should create a database to track comprehensive Department-wide information on use of force, including data compiled from the use-of-force forms.
6	NYPD should compile data and publish, on an annual basis, a report addressing Department-wide metrics on use of force, including but not limited to information from the new use-of-force reporting form. This report would track and collect various components related to the issue of use of force, including those addressed in this Report, such as officer tenure, assignments, age, type of force used, pertinent information regarding members of the public subjected to force, as well as officer injuries, disciplinary trends and outcomes, and other data deemed necessary for a comprehensive understanding of the issue.
7	NYPD training should place a stronger and more thorough emphasis on de-escalation tactics, by adding specific Police Academy and in-service courses on de-escalation that incorporate both classroom and scenario-based training.
8	NYPD should incorporate a formal evaluation system for all scenario-based trainings concerning the use of force.
9	NYPD should increase funding and personnel at the Police Academy with respect to training for both recruits and in-service officers.
10	NYPD should implement training to instruct officers to intervene in situations where other officers escalate encounters, use excessive force, and/or commit other misconduct.
12	In disciplinary cases where there are multiple disciplinary counts, each count should have an accompanying distinct penalty, as opposed to an aggregated penalty for all counts.
14	NYPD should set forth, in writing, in its disciplinary paperwork, the extent to which an officer's placement on force monitoring has or has not impacted the penalty imposed.
BODY-WORN CAMERAS IN NEW YORK CITY: AN ASSESSMENT OF NYPD'S PILOT PROGRAM AND RECOMMENDATIONS TO PROMOTE ACCOUNTABILITY (JULY 2015 REPORT)	
1.1	NYPD should broaden and illustrate the standard for the mandatory activation of BWCs during street or investigative encounters.
1.2	NYPD should redefine the safety exception for recording.
1.3	NYPD should consider stricter limitations on recording vulnerable populations.
1.4	NYPD should expand BWC training for officers using the BWCs.

2.1	NYPD should provide an example notification phrase to advise members of the public that they are being recorded.
2.2	NYPD should redefine the safety exception for notifications.
3.1	NYPD should require supervisors to review footage related to documented incidents.
3.2	NYPD should address discipline when the BWC program is more established and formalized.
3.3	NYPD should computerize the random selection of officers for review.
3.4	NYPD should establish a system for high-level and periodic review.
4.1	NYPD should grant supervisors general access to BWC footage with restrictions on arbitrary review.
4.3	NYPD should solicit feedback and suggestions for improvement from supervisors performing quality assurance reviews and officers participating in the Volunteer BWC Pilot Program.
5.1	NYPD should develop policies to guide supervisors when officer infractions are observed on BWC footage.
5.2	NYPD should institute mandatory reporting procedures.
5.3	NYPD should integrate BWC recordings into NYPD's existing force monitoring programs.
6.2	In all other instances, access to recordings prior to making statements should be noted in those statements.
7.1	If and when disclosing BWC video, NYPD should provide privacy and safety protections for vulnerable populations.
8.1	NYPD should establish a minimum retention period of at least 18 months.
8.2	NYPD should ensure expeditious purging of archived BWC footage that no longer holds evidentiary value.
9	NYPD should incorporate government and public input in continuing to develop the BWC program.
USING DATA FROM LAWSUITS AND LEGAL CLAIMS INVOLVING NYPD TO IMPROVE POLICING (APRIL 2015 REPORT)	
1.1	NYPD should perform a qualitative review of the most relevant data contained within legal claims and lawsuits against NYPD. Specifically: Nature of the claims/core allegations.
1.2	NYPD should perform a qualitative review of the most relevant data contained within legal claims and lawsuits against NYPD. Specifically: Information about the subject police officer(s).
2	NYPD should create an interagency working group between NYPD, the Comptroller's Office, and the Law Department to improve their police-involved litigation data collection, coordination, and exchange.
OBSERVATIONS ON ACCOUNTABILITY AND TRANSPARENCY IN TEN NYPD CHOKEHOLD CASES (JANUARY 2015 REPORT)	
1	NYPD should increase coordination and collaboration with CCRB to refine the disciplinary system for improper use of force.
2	NYPD should provide transparency with respect to the Police Commissioner's Disciplinary decisions.

3	NYPD should expand IAB's access to newly-filed complaints and substantive information on Use-of-Force cases filed with CCRB.
4	NYPD should improve information sharing and case tracking for cases that are outsourced to Borough and Precinct Investigators via the Office of the Chief of Department and the Investigative Review Section.

The following recommendations are **NO LONGER APPLICABLE** to NYPD due to a Department technology or procedure change prior to the April 2022 Annual Report.

AN INVESTIGATION OF NYPD'S NEW FORCE REPORTING SYSTEM (FEBRUARY 2018 REPORT)		
OIG-NYPD RECOMMENDATION		REASON NO LONGER APPLICABLE
20	NYPD should standardize the quarterly reporting mechanism for bureau and patrol borough commanders and ensure that their quarterly T.R.I. reports are submitted to the First Deputy Commissioner in a timely fashion.	The Department has repealed the underlying policy for this recommendation and replaced it with T.R.I 2.0, a system that can aggregate reports for any time period based on the ForceStat Process.