MEMORANDUM OF AGREEMENT

AGREEMENT NUMBER: [unnumbered]

PARTIES:

METROPOLITAN POLICE DEPARTMENT OF THE DISTRICT OF COLUMBIA

THE UNIVERSITY OF ARIZONA, JAMES E. ROGERS COLLEGE OF LAW

COLUMBIA UNIVERSITY, DEPARTMENT OF POLITICAL SCIENCE

YALE UNIVERSITY, DEPARTMENT OF POLITICAL SCIENCE

GOVERNMENT OF THE DISTRICT OF COLUMBIA , OFFICE OF THE CITY ADMINISTRATOR

TOPIC:

EVALUATION OF THE BODY-WORN CAMERA PROGRAM

I. PARTIES

The Parties to this Memorandum of Agreement ("Agreement") are the University of Arizona, James E. Rogers College of Law ("UA"), Columbia University Department of Political Science ("Columbia"), Yale University Department of Political Science ("Yale"), the District of Columbia Office of the City Administrator ("OCA") — collectively, the "Research Team" — and the Metropolitan Police Department of the District of Columbia ("MPD") — collectively, the "Parties."

II. PURPOSE

The purpose of this Agreement is to outline the general expectations of all Parties during the mutual research and evaluation of the body-worn camera (BWC) program implemented by MPD. It is also intended to govern the exchange, use, safeguarding, and ownership of data exchanged between the MPD and the Research Team to support the purposes of the evaluation.

Specifically, this document is intended to establish an agreement and mechanism to make law enforcement and public safety data collected by MPD in its records management systems (i-LEADS and/or Cobalt), Data Warehouse, Personnel Performance Management System (PPMS), Personnel Resource Tracking System, Time Attendance and Court Information System, Evidence.com, Integrated Justice Information System (IJIS) Outbound 12.1 feed, clinic, and other relevant systems available to the Research Team in a form and manner that facilitates the research and analyses for the purpose of conducting the evaluation of the BWC program.

This Agreement is a statement of intent, and should not be construed as a legally binding contract between the MPD and the Research Team. This agreement outlines the intent of the Parties to share law enforcement and public safety data for the purposes of studying and evaluating the short- and long-term impacts of the use of BWCs by members of the MPD.

It is the intent of all Parties to protect the confidentiality and security of law enforcement and public safety data subject to this Agreement, in accordance with applicable state and federal law, any applicable regulations on privacy and security, and relevant Departmental policies.

III. AUTHORITY

MPD enters this Agreement under authority set forth in 24 D.C. M.R. § 3902.7, which provides: "The Department shall engage academic institutions and organizations to analyze the BWC program; provided that any such relationship shall require the protection of any information or unredacted BWC recordings."

IV. BACKGROUND

The MPD is the primary law enforcement agency for the District of Columbia. Founded in 1861, the MPD is on the forefront of technological crime fighting advances, from highly developed advances in evidence analysis to state-of the-art-information technology.

In 2013, MPD began exploring the use, purchase, and deployment of BWCs for its police officers. The use of BWCs can benefit members of the community and the MPD by improving police services, increasing accountability for individual interactions, and enhancing public safety. MPD worked with law enforcement agencies across the country that have already deployed BWCs, as well as independent oversight agencies, criminal justice partners, and prosecutors. The Department also discussed the program at community meetings throughout the city and with other stakeholders.

MPD launched a six-month, limited trial period on October 1, 2014, for the purposes of determining the camera model that best suits the needs of the Department and city. After evaluating five different models, MPD selected the models that met the needs of the agency and officers.

In Phase Two of the BWC deployment, MPD procured additional cameras and deployed them to patrol officers in the Fifth and Seventh Police Districts on June 29, 2015. With funds allocated in the FY2016 budget, MPD has purchased additional cameras, to be deployed to MPD officers throughout the city.

The Phase Two deployment allowed the Parties to collect and analyze early information to inform the design and implementation of the full-scale evaluation of BWCs. This evaluation will consist of a randomized controlled trial (RCT) to evaluate the impact that use of BWCs may have on patrol operations, police-community interactions, and other possible areas. Randomization will take place at the individual officer level, with half of the eligible officers in each remaining district (1D, 2D, 3D, 4D, 6D) will be randomly assigned to wear BWCs. The trial will conclude in December 2016, at which point all eligible officers will be given BWCs in accordance with MPD's legislative obligations.

V. ROLES AND RESPONSIBILITIES

The team working on the BWC research and evaluation includes individuals from MPD, DC Government, and partnered academic institutions.

Team members from MPD will:

- Provide subject matter expertise in policing policy and practices;

- Lead the installation and deployment of BWCs and relevant infrastructure;
- Provide appropriate training and policy guidance to officers on the use of BWCs;
- Coordinate with the BWC Research Team to design and implement the RCT and analyze the data collected over the course of the RCT.

Team members from the DC Government (Office of the City Administrator and Metropolitan Police Department) and partnered academic institutions (UA, Columbia, and Yale) will:

- Design and guide implementation of the RCT, including conducting the randomized assignment of BWCs to members in each district.
- Analyze the results of the RCT and provide timely updates to MPD.

VI. DATA TO BE SHARED

The MPD agrees to furnish to the Research Team with the necessary data and information related to the BWC project and the relevant metrics and information necessary to evaluate the impact of the BWCs, subject to the following provisions:

- The Research Team agrees to abide by all present rules, policies, and procedures governing the databases and information systems; and any rules, policies, and procedures hereinafter required by the relevant databases and information systems, provided those rules, policies, and procedures are consistent with the charter and regulations governing the respective institutions with which Research Team members are affiliated. The shared data will remain subject to conditions of use, management, and disclosure that are consistent with the policies and practices of the MPD.
- The Research Team shall recognize and acknowledge the need to protect the privacy and confidentiality of the data and information and the necessity for protecting and preserving the integrity of such information by preventing access by unauthorized personnel, and inappropriate use by all user personnel.

VII. INTENDED USE OF THE DATA

The MPD is partnering with the Research Team to conduct a comprehensive study on the impact of the use of BWCs on police operations and activities as well as community implications. The Research Team will provide research guidance and expertise to ensure the study is conducted in a valid and sound manner according to accepted methodologies of scientific research.

The Parties agree that the data will only be used for the purposes of this specific research evaluation of MPD's BWC program. Any use of the data unrelated to or falling outside of this stated purpose is strictly prohibited unless expressly agreed to in writing by both Parties.

VIII. PROTECTION OF DATA

Any stored data will be afforded the same level of protection as it maintains in its original database.

The data shall be accessed or transferred via encrypted network protocols and shall not be exposed either in transport or at rest to the Public Internet, or any other publicly accessible network.

All raw data that is collected or downloaded from MPD systems and provided to the Research Team must be deleted or destroyed upon the conclusion of the research study, expiration or termination of this Agreement, or at the direction of MPD.

IX. LIMITATIONS ON THE DISCLOSURE AND USE OF INFORMATION

The MPD and the Research Team shall respect all controls and limitations placed upon the data with regards to the sharing or disclosure of data and products derived from analysis of the data, with the exception of replication data, which will be made publicly available.

Replication data are defined as the final, cleaned versions of all datasets used in the study analyses. This data will not contain any Personally Identifiable Information (PII) and will be vetted and cleaned through procedures documented in a codebook.

Attribution of MPD data used in subsequent publication or academic materials shall include the relevant contextual information on the source of the data and the date the information was accessed. The Research Team will not share or disseminate raw data to other agencies or persons without written permission from MPD.

All Parties shall be provided the opportunity to review and comment on any subsequent report or other written material, generated as part of this evaluation, prior to the material being published. All parties are committed to publicly disseminating the results of the evaluation (in presentations, reports, peer-reviewed journals, social media, and any other related medium as fitting), so that other interested parties may benefit from the knowledge generated by the study.

The Research Team will minimize its use, querying, and storage of Personally Identifiable Information (PII) to only what is necessary for proper analysis. Any PII will

be handled, stored, and destroyed in accordance with Federal law and regulations and laws of the District of Columbia.

The Research Team recognizes that data contained within and accessed from the MPD records management system (i-LEADS and/or Cobalt), PPMS, and Evidence.com is law enforcement sensitive or otherwise protected PII, and its disclosure to unauthorized personnel could hamper ongoing investigations, put innocent persons at risk, or divulge protected PII.

The Research Team will report to MPD any unauthorized disclosures, breaches or inadvertent releases of data or information immediately upon discovery.

X. PERIOD AND TIMING OF AGREEMENT

This Agreement shall remain effective for the period of one year, with a one-year option for renewal, commencing upon the date of the Agreement's signing by all Parties, unless terminated on an earlier date in accordance with the actions outlined in the next section.

The aforementioned MPD data shall be made available to the Research Team in the manner described in this Agreement upon its signing, or as soon as technically feasible thereafter.

XI. MODIFICATION

Modifications to this agreement must be made in writing and signed and dated by authorized officials, prior to any changes being performed.

XII. TERMINATION

Any of the Parties may terminate this Agreement, in whole or in part, by providing thirty (30) days written notice to the other parties.

XIII. FUNDING

This agreement is neither a fiscal nor a funds obligation document. Absent a separate written agreement, the Parties will cover their own costs for any work performed under this Agreement.

XIV. USE OF NAMES

None of the Parties may use the name of the other Parties in any form of advertising or publicity without express written permission. The Parties will seek permission from one another by submitting the proposed use, well in advance of any deadline, to the Contacts listed in XV and XVI below.

XV. CONTACT INFORMATION

The following individuals shall serve as the points of contact for this Agreement.

Heidi Fieselmann
Special Assistant
Executive Office of the Chief of Police
Metropolitan Police Department
300 Indiana Avenue, NW, Rm 5080
Washington, DC 20001
(202) 727-9318
heidi.fieselmann@dc.gov

Katherine Barnes, J.D., Ph.D.
Professor
James E. Rogers College of Law
University of Arizona
1201 E. Speedway Blvd
Tucson, AZ 85721
(520) 621-5513
2-534(a)(2)

Alexander Coppock, Ph.D.
Assistant Professor
Department of Political Science
Yale University
77 Prospect Street, Room D233
Institution for Social and Policy Studies
New Haven, CT 06511
(651) 343-8133
alex.coppock@yale.edu

Donald P. Green, Ph.D.
Professor
Department of Political Science
Columbia University
815 IAB, 420 W. 118th St.
New York, NY 10027
(212) 854-0397
dpg2110@columbia.edu

David Yokum, J.D., Ph.D.
Senior Policy Advisor
Office of the City Administrator | The Lab @ DC
Government of the District of Columbia
1350 Pennsylvania Ave NW
Washington, DC 20004
(202) 430-8858
david.yokum@dc.gov

XVI. OTHER CONTACTS

Anita Ravishankar
Research Fellow
Executive Office of the Chief of Police
Metropolitan Police Department
300 Indiana Avenue, NW, Rm 5080
Washington, DC 20001
anita.ravishankar@dc.gov

XVII. SIGNATURES

The signatories below warrant and represent that they have the requisite authority on behalf of their respective governmental entities to enter into the obligations set forth in this Agreement.

IN WITNESS WHEREOF the parties hereto have caused this agreement to be executed by their duly authorized representatives:

EXECUTIVE OFFICE OF THE CHIEF OF POLICE
METROPOLITAN POLICE DEPARTMENT OF THE DISTRICT OF COLUMBIA

Signature: _____ Date: _____

Peter Newsham
Acting Chief of Police

JAMES E. ROGERS COLLEGE OF LAW
THE UNIVERSITY OF ARIZONA

Signature: _____ Date: _____

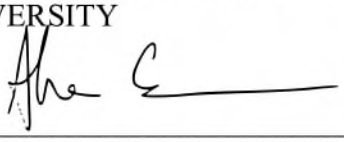
Katherine Barnes, J.D., Ph.D.
Professor

DEPARTMENT OF POLITICAL SCIENCE
COLUMBIA UNIVERSITY

Signature: _____ Date: _____

Donald P. Green, Ph.D.
Professor

DEPARTMENT OF POLITICAL SCIENCE
YALE UNIVERSITY

Signature:  Date: 5/5/17

Alexander Coppock, Ph.D.
Assistant Professor

OFFICE OF THE CITY ADMINISTRATOR | THE LAB @ DC
GOVERNMENT OF THE DISTRICT OF COLUMBIA

Signature: _____ Date: _____

David Yokum, J.D., Ph.D.
Senior Policy Advisor

GOVERNMENT OF THE DISTRICT OF COLUMBIA

OFFICE OF THE CITY ADMINISTRATOR

OCA Approval and Tracking Form

Date submitted: 7/11/17

☐ **For your awareness**

☒ **For your signature**

Document Information

1. Name of OCA Analyst	Sam Quinney	**3. Date document was received**	7/11/17
2. Originating agency	MPD/The Lab @ DC	**4. Date needed**	7/20/17
5. Name/title of document	**Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator**		

6. Brief description of document

This data use agreement governs the exchange, use, safeguarding, and ownership of data shared by MPD with OCA. MPD is sharing this data with OCA in order to allow The Lab @ DC to evaluate MPD's Body-Worn Camera Program; evaluate the Crime Gun Intelligence Center; and conduct data analysis and evaluation to test the effects of changes to MPD's standard processes in order to provide timely, accurate, and objective information to support MPD decision-makers and stakeholders.

7. Recommendation

We recommend that the CA sign off on the data use agreement with MPD as soon as possible.

8. Additional notes (e.g., prior approvers, controversial aspects, etc.)

This document aligns with the new District Data Policy; has been reviewed by both OCA and MPD general counsel, and has been signed by Chief Peter Newsham. It has received the necessary approvals from all involved parties, and its execution will allow the efficient conduct of The Lab @ DC's work supporting MPD.

Additional Clearances

	Jenny Reed	Barry Kreiswirth	Ben Stutz	Tonya Thompson	Rashad Young
Approval required	☒	☒	☒	☐	☒
Reviewer approval	☑ Yes ☐ No	☒ Yes ☐ No	☒ Yes ☐ No	☐ Yes ☐ No	☐ Yes ☐ No
Initials	JR	BK			
Date	7/11/17	7/12/17	7/12/17		

Reviewer Comments (if any)

Reviewer initials	Comment

DATA USE AGREEMENT
BETWEEN THE METROPOLITAN POLICE DEPARTMENT AND
THE OFFICE OF THE CITY ADMINISTRATOR

This DATA USE AGREEMENT ("Agreement") is entered into between the Metropolitan Police Department of the District of Columbia ("MPD") and the Office of the City Administrator ("OCA"), collectively referred to herein as the "Parties" and each individually referred to herein as a "Party."

1. The Parties

   a. OCA directly oversees all executive agencies in the District that report to the Mayor. It is responsible for the day-to-day management of the District government, setting operational goals and implementing the legislative actions and policy decisions of the D.C. Council and the Mayor. As part of its operations, OCA employs The Lab @ DC, which is housed within OCA, to conduct quantitative research to evaluate and inform policy and program decisions. Staff members of The Lab @ DC are applied research scientists with expertise in statistics, experimental design, quantitative research methods, and various social science disciplines.

   b. One of the 10 largest local police agencies in the United States, the MPD is the primary law enforcement agency for the District of Columbia. With a sworn force of approximately 3,700 members, MPD serves a population of over 680,000. Founded in 1861, the MPD of today is on the forefront of technological crime fighting advances, from highly developed advances in evidence analysis to state-of the-art-information technology. These modern techniques are combined with a contemporary community policing philosophy that seeks to bond the police and residents in a working partnership designed to organize and mobilize residents, merchants and professionals to improve the quality of life for all who live, work, and visit the nation's capital.

      Under this agreement, data sharing and use between the Parties encompasses all project work between the Parties, as enumerated in section 2 below.

2. Purpose of the Agreement

   a. The purpose of this agreement is to govern the exchange, use, safeguarding, and ownership of data shared by MPD with OCA. MPD is sharing this particular data with OCA in order to allow The Lab @ DC to evaluate MPD's Body-Worn Camera Program; evaluate the Crime Gun Intelligence Center; and conduct data analysis and evaluation to test the effects of changes to MPD's standard processes in order to provide timely, accurate, and objective information to support MPD decision-makers and stakeholders.

   b. This Agreement encompasses the projects listed below:

i. *Body-Worn Camera ("BWC") Program Evaluation*

1. MPD began its BWC Program in 2014, with the initiation of a trial deployment of BWCs to evaluate various camera models. After selecting a Taser BWC system as best suited to the needs of the MPD and the city, MPD implemented a pilot deployment of BWCs in 2015 to inform the full-scale deployment and evaluation of its BWC program. From June 2015 through December 2016, the Parties conducted a randomized controlled trial ("RCT") to evaluate the effects of BWCs citywide. The treatment period concluded in December 2016, when MPD deployed cameras to all eligible officers on the force.

2. The Lab @ DC led the design and implementation of the study, and will conduct the analyses of the data as set forth in the study pre-analysis plan, available on the Open Science Framework website.[1] Sharing data will allow The Lab @ DC to conduct these analyses and provide MPD, OCA, and The District with insights on how BWCs affect key outcomes of interest in The District, including police use of force, civilian complaints, police activity, and judicial outcomes.

3. Expected work products include the pre-analysis plan, presentation slides on study design and findings, a full written report documenting the study design, analysis, and results, and other content as needed (e.g., press releases, research briefs, web content, etc.).

ii. *Crime Gun Intelligence Center ("CGIC") Evaluation*

1. With a $1 million grant from the Department of Justice Bureau of Justice Assistance, MPD is working with the Department of Forensic Science, Prince George's County Police Department, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") to build out and boost the capacity of the regional crime gun intelligence center. The goal of this effort is to increase partner agency capacity to 1) Quickly recover, analyze, and enter into the National Integrated Ballistic Information Network ("NIBIN")[2] any and all shell-casings/guns recovered; 2) Conduct the analysis/correlations in partnership with the ATF NIBIN National Correlation and Training Center; 3) Conduct the link analysis to connect guns to relevant crimes/perpetrators of those crimes; 4) Provide this investigatory material to detectives for more rapid resolution and closure of cases; and 5) Develop a stronger

[1] The pre-analysis plan is available at https://osf.io/yjyng/.

[2] For more information on NIBIN, please see https://www.nij.gov/topics/law-enforcement/investigations/Pages/nibin.aspx.

evidentiary basis in the interest of successful prosecution. The overall objective is to reduce gun crime by getting both the guns and those who use them off the street.

2. The Lab @ DC will lead the evaluation effort, which will include both process and impact evaluation. By sharing and using the data, the Parties can conduct a robust and comprehensive evaluation of the CGIC and provide information relevant to decision-makers regarding CGIC policy and operations.

3. The data will be used to conduct both process and impact evaluations. The study will incorporate randomized evaluation as well as other modeling techniques (e.g. pre-post analyses, difference-in-difference modeling, synthetic control analyses), to be documented in detail in the pre-analysis plan.

4. Expected work products include the pre-analysis plan; presentation slides on study design and findings; a full written report documenting the study design, analysis; and results, and other content as needed (e.g., press releases, research briefs, web content, grant-mandated reports, etc.).

iii. MPD Recruitment Improvement

1. This project uses behavioral science to redesign the MPD recruitment-related web pages and emails. The aim is to increase the number of qualified applicants that complete the National Testing Network ("NTN") qualifying test, and to thereby help MPD reach its goal of increasing hiring by fifty percent (50%).

2. By sharing data, the Parties can ensure that proposed redesign does, in fact, increase the number of qualified applicants completing the NTN. The Parties can also test different processes, outreach platforms, and content to help inform the selection of the redesign that best optimizes MPD recruitment.

3. The study applies a randomized evaluation approach, in which control applicants proceed through MPD's existing recruitment process, while treated applicants will view the redesigned web and email content. The redesigned content is based on behavioral science research.

4. Expected work products include the pre-analysis plan; presentation slides on study design and findings; a full written report documenting the study design, analysis, and results; and other content as needed (e.g., press releases, research briefs, web content, etc.).

iv. Officer Care and Early Intervention Predictive Analysis and Interventions

1. Modern police departments face considerable human resource challenges: they must recruit and train officers to provide consistently excellent service under what are often stressful and dangerous conditions. Unfortunately, there is little evidence-based research providing objective metrics for recruiting, assigning, and supporting front-line officers. The purpose of the proposed research is to address this gap by conducting rigorous, replicable, and generalizable research into the factors shaping officer performance and wellbeing using data available to most metropolitan police departments.

2. By sharing data, MPD will provide The Lab @ DC with the data necessary to build a machine learning model that estimates two key outcomes of interest: the Probability of an Adverse Event ("PAE"), defined as the probability that an officer will be involved in a serious adverse event such as unauthorized use of force or a sustained citizen complaint; and the Probability of Officer Harm ("POH"), defined as the probability of an officer's criminal victimization, accident, injury, or illness. Using the model predictions, stage two of this project will entail randomized evaluations of three types of officer support. The shared data will allow the Parties to assess the effects of these interventions on PAE and POH.

3. The Parties will use the data to build machine-learning models and conduct randomized evaluations of officer support interventions.

4. Expected work products include the pre-analysis plan, presentation slides on study design and findings, a full written report documenting the study design, analysis, and results, and other content as needed (e.g., press releases, research briefs, grant-mandated content, web content, etc.).

v. Shotspotter Analyses

1. Shotspotter data can be employed as a proxy for a variety of outcomes (and inputs) of interest. For example, Shotspotter alerts can serve as a gauge of more localized measures of violent crime or exposure to crime, and can also be paired with calls for service data to proxy public trust in the police (e.g., what proportion of Shotspotter alerts are also called in by members of the public). By leveraging other administrative data (specified in Appendix A) with Shotspotter data, The Lab @ DC can conduct a variety of data analytic projects to support MPD and OCA decision-makers.

2. The Lab @ DC's role in this effort is to use the data to conduct analysis per OCA and MPD needs/requests.

3. Expected work products include the pre-analysis plan for each data analytic project involving Shotspotter data; presentation slides on research design and findings, a full written report documenting the research design, analysis, and results, and other content as needed (e.g., press releases, research briefs, web content, etc.).

3. Data to be Shared by MPD

a. Within five (5) business days after the effective date of this agreement, MPD shall provide the data specified in Appendix A (hereinafter referred to as "Data") to OCA.

i. MPD shall provide periodically updated pulls of the datasets listed in Appendix A to OCA based on individual project needs. These requests will be communicated to MPD's liaison to The Lab @ DC in writing, to be processed within ten (10) business days of receipt of the request.

b. If the Data are pulled from a database, MPD shall provide the exact query used to pull the Data.

c. If, during the term of this Agreement, the Parties identify additional information needed by or useful to OCA to carry out the purposes of this Agreement, the Parties may revise Appendix A by a written agreement signed by the agency representatives listed in section 15 of this Agreement.

4. Authorized Uses of Data by OCA

a. OCA shall use the Data only for the purposes described in section 2 of this Agreement.

5. Protection of Data

a. OCA shall follow the standards set forth in Appendix C in storing, accessing, and using the Data to protect the security and confidentiality of the Data.

6. Authorized Disclosures of Data

a. OCA shall disclose or provide Level 1, 2, 3, or 4 Data only to authorized users (as described in subsection b. of this section) and only to carry out the purposes of this Agreement. In addition, OCA shall only disclose or provide as much Data to an authorized user as is necessary or useful for the authorized user to carry out his or her work in fulfilling the purposes of this Agreement.

b. Authorized users are OCA employees, contractors, and agents and other employees of the government of the District of Columbia whose services OCA determines are necessary or useful to fulfill the purposes of this Agreement.

c. Before an authorized user may receive or be provided access to Level 1, 2, 3, or 4 Data:

i. OCA must submit a written notification to MPD to authorize the user;

ii. The authorized user must execute and provide to the Data Custodian a Data Confidentiality Agreement (in the form provided in Appendix B); and

iii. The Data Custodian must submit a copy of the executed Data Confidentiality Agreement to MPD within five (5) business days of receipt from the authorized user.

d. There are no restrictions on the disclosure or provision of Level 0 Data.

7. Sharing of Data for Replication Purposes

a. Notwithstanding section 6 of this Agreement, OCA may share the Data with a party outside the District government who is not an authorized user under section 6.b. if such sharing is for the purpose of validating the accuracy of analyses conducted by OCA under the Agreement (this purpose is hereinafter referred to as "replication purposes"). Level 0 data may be shared for replication purposes without restriction. In sharing Level 1, 2, 3, or 4 Data for replication purposes, OCA shall ensure that the Data is de-identified to the extent that identification is not needed for replication purposes and shall ensure that other Level 1, 2, 3, and 4 confidential or sensitive information unnecessary for replication purposes is not shared, to the extent that such sharing is not necessary for replication purposes. OCA shall also take appropriate measures to ensure that the outside party protects the Data and disposes of the Data after the Data is no longer needed for replication purposes. The sharing of Level 3 and 4 Data for replication purposes shall be approved by MPD in writing. In addition, the scope of the Level 2, 3, and 4 Data shared with the outside party for replication purposes shall be approved by MPD in writing to ensure that the Data will be de-identified to the extent that identification is not needed for replication purposes and to ensure that confidential or sensitive information unnecessary for replication purposes will not be shared, to the extent that such sharing is not necessary for replication purposes.

8. Required Disclosures of Data

a. Nothing in this Agreement shall prohibit OCA from disclosing any Data if OCA is legally required to do so by judicial or governmental order or in a judicial or governmental proceeding; provided that OCA shall:

i. Notify MPD of the requirement to make the disclosure within forty-eight (48) hours after it becomes aware of such requirement; and

ii. Cooperate with MPD if MPD elects to contest the requirement to make the disclosure or to seek a protective order.

9. Publication of Results of Data Analysis

a. Notwithstanding section 6 of this Agreement, OCA may publish and present the results and conclusions of its analyses under this Agreement to individuals and entities outside of the OCA; provided, that:

i. The publication or presentation shall not include personally identifiable information; and

ii. The publication or presentation shall not include Level 1, 2, 3, or 4 confidential or sensitive information, unless the publication or presentation of such information is allowed under Appendix C.

b. MPD will be given the opportunity to review and comment on the analysis plan. The analysis plan will be posted to the Open Science Framework (https://osf.io) prior to analysis of the outcome data.

c. OCA shall provide a draft of each planned publication or presentation to MPD for MPD's review at least five (5) days before publishing or presenting the results or conclusions of OCA's analyses under this Agreement. The purpose of MPD's review is only to ensure conformity with paragraphs a.i. and a.ii. of this section.

10. OCA Data Custodian

a. OCA designates David Yokum, Director of The Lab @ DC, as the Data Custodian under this Agreement.

b. The Data Custodian is the OCA employee or agent who is responsible for initially receiving the Data from MPD.

c. Once the Data is received from MPD by the Data Custodian, the Data Custodian is responsible for providing the Data to authorized users and ensuring that authorized users receive access to the Data only in conformity with this Agreement (including by ensuring that a signed Data Confidentiality Agreement is signed before the Data Custodian provides access to the Data to an authorized user); maintaining a record of all Data requested and received; ensuring that the Data is disposed in accordance with section 11 of this Agreement; and providing notice of such disposition as set forth in section 11 of this Agreement.

d. Before MPD supplies any data to the Data Custodian, the Data Custodian shall execute and deliver to MPD a Data Confidentiality Agreement in the form set forth in Appendix B.

11. Disposition of Data at Termination of the Project

a. OCA shall delete Level 2, 3, and 4 Data from all places where it is stored and provide verification, in writing, to MPD of the manner and date of deletion within ninety (90) days after the later of the following occurrences:

i. MPD and OCA determine that the purpose of this Agreement has been fulfilled; or

ii. The OCA issues a final report, or other terminal work product, based on the Data.

b. The Parties may, for good cause shown, extend such ninety (90) day period in increments of ninety (90) days. Such extension must be in writing, executed by the Parties' representatives listed in section 13 of this Agreement.

c. Notwithstanding paragraph a. of this section, OCA may maintain datasets developed from the Data so long as OCA removes any personally identifiable information and other Level 2, 3, or 4 confidential or sensitive information from such datasets.

12. Reporting of Unauthorized Disclosures or Misuse of Information

a. If the OCA discovers any actual or suspected use, access, or disclosure of Data not authorized by this Agreement, OCA shall promptly notify MPD in writing. Such notification shall include the following information (to the extent known by OCA):

i. The nature of the unauthorized use, access, or disclosure;

ii. The Data used, accessed, or disclosed;

iii. The individual who made the unauthorized use or access or received the unauthorized disclosure;

iv. OCA's actions to mitigate any negative impact of the unauthorized use, access, or disclosure; and

v. The corrective action OCA has taken or will take to prevent future similar unauthorized use, access, or disclosure.

b. OCA shall be responsible for making reasonable efforts to eliminate or mitigate the negative impact of any unauthorized access, use, or disclosure of Data. OCA shall inform all unauthorized individuals who received or accessed Data that such Data was disclosed or accessed in error and of the steps the individual must take to mitigate any negative impacts of the error.

13. Data Levels

a. The Data levels (i.e., Level 0, Level 1, Level 2, Level 3, and Level 4) referenced in this Agreement refer to the data levels described in Appendix C of this Agreement.

14. Applicable Laws

a. The following statutes and regulations are applicable to this agreement and the Parties make the following affirmations:

i. D.C. Official Code § 16–2333, pursuant to which law enforcement records and files concerning a child shall not be open to public inspection nor shall their contents or existence be disclosed to the public unless the person or entity inspecting the records falls into an articulated exception. MPD affirms that for the purposes of this agreement, OCA is not considered to be a public entity; rather, MPD considers OCA for the purposes of this agreement to be an authorized representative of MPD.

ii. D.C. Official Code § 5-113.01(3), pursuant to which MPD must keep a personnel record of each member of the Metropolitan Police force. The parties agree that there is an implicit requirement imposed by this statute for MPD and its authorized representatives to create reasonable measures to protect such records and prevent its disclosure to unauthorized entities and the parties further agree that the data safeguards and procedures contained in this agreement fulfill that implicit protection requirement.

iii. D.C. Official Code § 5-113.06(a), pursuant to which general complaint files, records of lost, missing, or stolen property, and arrest books must be open to the public when not in actual use by MPD. MPD affirms that such records will be available to the public, even when in use by OCA, as such records are now digitized.

iv. 6B DCMR §§ 3100, 3101.2, 3106.2, and 3106.3, pursuant to which:

1. All official personnel records of the District Government shall be established, maintained, and disposed of in a manner designed to ensure the greatest degree of applicant or employee privacy while providing adequate, necessary, and complete information for the District to carry out its responsibilities under the District of Columbia;

2. All Federal personnel records (which include personnel records of District employees whose positions were subject to Federal civil service rules and regulations, for the entire period of service during which such rules and regulations applied) in the custody of the District Government shall be subject to the Federal laws and regulations regarding personnel records, availability of official information, protection of privacy and personnel records, freedom of information, and other pertinent subjects, as set forth in Title 5 of the Code of Federal Regulations;

3. Agency employees whose official duties involve personnel records shall be sensitive to individual rights to personal privacy and shall not disclose information from any personnel record unless disclosure is part of their official duties or required by regulation or statute; and

4. Any agency employee who makes a disclosure of personnel records knowing that such disclosure is unauthorized, or who otherwise knowingly violates these regulations, shall be subject to disciplinary action and may also be subject to criminal penalties where the records are Federal records subject to the Privacy Act.

MPD affirms that these statutes do not impose any further obligations or requirements on OCA than those contained in this agreement and that the data safeguards and procedures contained in this agreement fulfill that implicit protection requirement. OCA affirms that it understands the consequences of improper disclosure enforced by these statutes.

b. Data sharing and use pertaining to any analyses for the Body-Worn Camera (BWC) program pursuant to section 2.b.i. of this agreement is specifically authorized by 24 DCMR 3902.7, which provides: "The [Metropolitan Police] Department shall engage academic institutions and organizations to analyze the BWC program; provided that any such relationship shall require the protection of any information or unredacted BWC recordings." The parties agree that the data safeguards and procedures contained in this agreement fulfill the data protection requirement imposed by 24 DCMR 3902.7.

15. Parties' Representatives

a. The following individuals are the Parties' representatives under this Agreement:

MPD
Matthew Bromeland, Chief of Staff, Executive Office of the Chief of Police
300 Indiana Avenue, N.W.
Washington, D.C. 20001
Email: matthew.bromeland@dc.gov
Phone: (202) 438-8453

OCA
David Yokum, Director, The Lab @ DC
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
Email: david.yokum@dc.gov
Phone: (202) 308-7888

b. All writings and notices delivered under this Agreement shall be provided to the Parties' representatives by mail, by electronic mail, or by hand.

16. Duration

a. The period of this Agreement is from its date of execution through the date by which OCA has deleted the Data under section 10 of this Agreement (the "Termination Date"); provided, that sections 4, 5, 6, 7, 8, 10, and 11 shall survive beyond the Termination Date.

17. Modifications

a. The terms and conditions of this Agreement may be modified only upon the agreement of the Parties. A modification must be in writing and signed by the duly authorized signatories of OCA and MPD.

18. Counterparts

a. This Agreement may be executed in counterparts, each of which shall be deemed an original and all of which shall be taken together and deemed to be one instrument.

The Office of the City Administrator and the Metropolitan Police Department of the District of Columbia, by the signatures of the authorized representatives below, hereby acknowledge and agree to the terms and conditions of this Agreement.

IN WITNESS WHEREOF, this Agreement has been executed by the Parties as of the dates set forth below.

METROPOLITAN POLICE DEPARTMENT

By: Peter Newsham
Title: Chief of Police

Date: 7/10/2017

OFFICE OF THE CITY ADMINISTRATOR

By: Rashad Young
Title: City Administrator

Date: 7/18/17

APPENDIX A

Dataset #	Dataset	General Description	Dataset Security Level
1	De-identified Personnel Performance Management System (PPMS)	Personnel performance records as described in GO-PER-120-28.	3
2	Personnel Resource Tracking (PRT)	Personnel records.	3
3	Arrests	Records of all arrests made by MPD.	2
4	Crime	Records of all crimes reported and documented by MPD.	2
5	Calls for Service	Records of calls for service, including responding officers, event type and disposition.	2
6	Traffic Tickets	All traffic tickets issued by MPD members.	2
7	Traffic Warnings	All traffic warnings issued by MPD members.	2
8	Evidence.com	Cloud system containing all BWC videos; includes video categorization information and audit logs.	3
9	Time, Attendance, and Court Information System (TACIS)	Tracks officer time; include home assignment as well as specific assignment each day.	3
10	De-identified Clinic data	Data on officer injuries sustained while on duty, including injury cause and nature of injury, as well as relevant case number and incident date.	3
11	Integrated Justice Information System 12.1 feed	Data on court outcomes at the arrest level.	3
12	File on Q	MPD evidence tracking system.	3
13	Shotspotter	Documents all Shotspotter alerts, including number of shots fired, date, time, and geographic coordinates of shots fired.	2

Note Regarding Personally Identifiable Information

If personally identifiable information—or other Level 2, 3, or 4 confidential or sensitive information—does not need to be included in the Data in order to allow OCA to fulfill the purpose of this Agreement, MPD shall, if possible, separate or otherwise mask such information in the Data provided to OCA. For the purposes of this paragraph, the term "personally identifiable information" is defined as information that can be used to identify, contact, or locate a specific individual (such as a name, address, social security number, driver's license number, taxpayer identification number, email address, telephone number, financial records, educational records, health records, criminal records, or biometric information and indirect identifiers, such as an individual's date of birth, place of birth, or mother's maiden name) or information for which there is a reasonable basis to believe that the information can be used to identify an individual in combination with other reasonably available information.

APPENDIX B

Data Confidentiality Agreement

Pursuant to the Data Use Agreement between the Office of the City Administrator ("OCA") and the Metropolitan Police Department ("Data-Sharing Agency"), signed by the City Administrator on [redacted], 2017 and regarding the sharing of data to support evaluation and analytic projects conducted by MPD and The Lab @ DC ("Data Use Agreement"), OCA will be given access to data which includes confidential or sensitive information, such as personally identifiable information. As an authorized user of such data, I make the following affirmations:

I have carefully read and completely understand the data security guidelines outlined in The Lab @ DC Data Security Policy (the "Data Security Policy").

I understand that I must, and affirm that I will, comply with all data security requirements specified in the Data Security Policy.

I have carefully read, completely understand, and will comply with the terms and conditions of the Data Use Agreement, including the restrictions on the use and disclosure of the data provided to OCA pursuant to the Data Use Agreement.

I understand that it is my responsibility to know the level(s) of data exchanged under the Data Use Agreement (as reported by the Data-Sharing Agency in the Data Use Agreement), and the security protections in place and necessary to ensure the protection of the data.

I will not disclose, and will take all necessary and reasonable precautions to prevent others from disclosing, any confidential or sensitive data provided pursuant to the Data Use Agreement, unless such disclosure is authorized by the Data Use Agreement.

I will not use, and will take all necessary and reasonable precautions to prevent others from using, the data provided pursuant to the Data Use Agreement for any purpose not authorized by the Data Use Agreement.

I will not attempt to use, and will take all necessary and reasonable precautions to prevent others from using, the data provided pursuant to the Data Use Agreement to contact any persons in the data for any purpose unless such contact is authorized by the Data Use Agreement.

I understand that my disclosure of confidential or sensitive information in violation of the Data Use Agreement, or my failure to abide by this Data Confidentiality Agreement or the Data Security Policy may subject me to disciplinary action, up to and including termination of employment.

I agree to report the violation or apparent violation of any term of this Data Confidentiality Agreement or the Data Use Agreement to the Data Custodian without unreasonable delay.

I acknowledge and affirm that I am personally responsible for compliance with the terms of this Data Confidentiality Agreement and the Data Use Agreement.

Signature: _____

Printed Name: _____

Date: _____

APPENDIX C

The Lab @ DC Data Security Policy

The work of The Lab @ DC ("the Lab") often involves confidential or sensitive information. This document outlines the Lab's procedures for working with data at all different levels of confidentiality and sensitivity and ensuring the protection of data.

General Security Controls Employed by All Lab Staff

- All data analysis must be conducted on District-issued computers.
- All District-issued computers on which data analysis is conducted must:
    - Run Windows 10 to facilitate encryption;
    - Use full disk encryption (using Check Point endpoint security);
    - Be password-protected; and
    - Have the computer screen set to automatically lock and require a password to re-open after 5 minutes of inactivity.
- All users must use a password that is not used elsewhere by the user and a password manager to access other analytic tools.
- All users must lock their computer screens and require a password to re-open whenever they leave a District-issued laptop unattended outside of a District government facility.
- When using a Wi-Fi connection (other than the secure Wi-Fi connection operated by the District government), all users shall comply with the following guidelines:
    - The user shall not use an unsecured public Wi-Fi connection unless such use is absolutely necessary (for example, the user's hotel only provides an unsecured Wi-Fi connection and it is necessary for the user to perform work while at the hotel);
    - The user shall immediately connect to the DC VPN (regardless of whether the Wi-Fi connection is secure or unsecure);
    - To the extent feasible, the user shall avoid accessing or analyzing Level 3 or Level 4 data when connected to a public Wi-Fi connection, even if the user is connected to the DC VPN and even if the Wi-Fi connection is secured; and
    - The user shall ensure that his or her home network uses WPA2 authentication.

Level 0: Open Data

Description: Level 0 data refers to all datasets not designated by an agency as being level 1 to level 4.

Example: Certificates of occupancy are determinations by the Department of Consumer and Regulatory Affairs (DCRA) that the use of a building, structure, or land in the District conforms to zoning regulations and building codes. This dataset would not be designated by DCRA as Level 1, 2, 3, or 4 and therefore would be considered Level 0. Moreover, any dataset regularly published in machine-readable format on opendata.dc.gov or another dc.gov website prior to this Order is considered "Level 0, Open" unless an agency makes a proactive determination to raise the classification.

Protections: The Lab will not provide any protections for Level 0 data.

Publication: There are no restrictions on the publication of Level 0 data.

Sharing: There are no restrictions on sharing Level 0 data.

Disposal: There are no requirements to dispose of Level 0 data.

Level 1: Public, Not Proactively Released

Description: Level 1 data refers to a dataset that is not protected from public disclosure or subject to withholding under any law (including the Freedom of Information Act ("FOIA")), regulation, or contract. Nevertheless, publication of the dataset on the public Internet and exposure to search engines would:

1. Have the potential to jeopardize the safety, privacy, or security of residents, agency workforce members, clients, partners, or anyone else identified in the information;
2. Require subjective redaction;
3. Impose an undue financial or administrative burden on the agency; or
4. Expose the District to litigation or legal liability.

Example: The Board of Elections (BOE) maintains a voter file, which traditionally is public data, and in fact the BOE is required by law to "publish and display on its website ... a searchable copy of the list of qualified voters." The law does not state that the entire file, including voter history, must be posted. Under this policy, BOE could declare the voter history to be "public but not proactively released."

Protections: Level 1 datasets may be transferred by District government email, flash drive, or the Lab's secure upload facility. No other protections are required for Level 1 data. Level 1 datasets may be printed, but the printouts will be shredded when they are no longer needed.

Publication: If Level 1 datasets are used in a published document, the data may be made available with the document, but will be made anonymous and any data described in paragraphs 1-4 of the Description section above will be removed before being published.

Sharing: Level 1 data may be shared freely within the District government. Level 1 data will not be actively shared outside the District government directly or otherwise (e.g., by posting the data online), except as described in the Publication section above and as described in this section for replication purposes. If OCA receives a request for Level 1 data from a party outside the government, OCA will inform the data owner of the request and refer the requesting party to the data owner to request the data. If, despite the referral, the requesting party continues to request that OCA provide the data, OCA will confer with the data owner to ensure that appropriate precautions are taken (for example, subjective redactions) before the data is shared. OCA may share Level 1 data with an outside party for replication purposes. When Level 1 data is shared for replication purposes, OCA shall take appropriate steps to ensure that sensitive or confidential data is not unnecessarily shared and to ensure that the outside party appropriately protects and disposes of the data.

Disposal: There are no requirements for OCA to dispose of Level 1 data unless specified by the data owner in a data use agreement with OCA.

Level 2: For District Government Use

Description: Level 2 data refers to a dataset that the originating agency determines is subject to one or more FOIA exemptions, is not highly sensitive, and may be distributed within the District government without restriction by law, regulation, or contract.

Example: OCTO licenses commercial data on businesses operating in the District. The license prohibits the public distribution of the data, and proprietary restrictions qualify as a FOIA exemption. Nevertheless, the data has widespread utility within the government, including for economic development and emergency management, and therefore would be classified as Level 2.

Protections: Unless otherwise specified by the data owner in a data use agreement with OCA, Lab staff may transfer Level 2 datasets or any derivatives of Level 2 datasets by District government email, flash drive, or the Lab's secure upload facility. However, some contracts have additional provisions that may apply (for example, the contract may require that the data must be accessed through certain interfaces). The data owner is responsible for notifying the Lab if any such restrictions exist (although the Lab intends to actively solicit this information as well) and for including those restrictions in the data use agreement with OCA. If Level 2 data is transferred via flash drive, the data will be deleted immediately from the flash drive after the transfer is complete and the deletion will be confirmed by ensuring that the data does not appear in the trash or recycle bin of the flash drive. Any Level 2 data that is printed will be stored in a locked file cabinet when the data is not in use and will be shredded when it is no longer needed.

Publication: The aggregate results and conclusions from OCA's analysis of Level 2 data may be published or presented to the general public. However raw data from Level 2 datasets will not be used in a published document or a presentation unless the publication or presentation of such information is agreed to by the data owner.

Sharing: Unless prohibited by a contract, Level 2 data may be shared with other District government employees, contractors, and agents, but it may not be shared with an individual outside the District government either directly or otherwise (for example, by posting the data online). If OCA receives a request for Level 2 data from a party outside the government, OCA will inform the data owner of the request and refer the requesting party to the data owner. OCA will not share the data with the outside party upon such a request. If OCA seeks to share the data with an outside party (for example, for replication purposes) the sharing of the data must be approved in writing by the data owner before the data may be shared by OCA, unless such sharing is authorized by the data use agreement between the data owner and OCA. When Level 2 data is shared with an outside party, OCA shall take appropriate steps to ensure that sensitive or confidential is not unnecessarily shared and to ensure that the outside party appropriately protects and disposes of the data.

Disposal: There are no requirements for OCA to dispose of Level 2 data unless specified by the data owner in a data use agreement with OCA.

Level 3: Confidential

Description: Level 3 data refers to a dataset that the originating agency has determined is protected from disclosure by law, including FOIA, regulation, or contract and that is either highly sensitive or is restricted by law, by regulation, or by contract from disclosure to other public bodies. Such datasets generally include datasets that contain data that qualifies for designation by a federal agency or District agency as:

1. Attorney-Client Privileged;
2. Criminal Justice Information;
3. Critical Infrastructure Information;
4. Family Educational Rights and Privacy Act (FERPA);
5. Federal Tax Information (FTI);
6. For Official Use Only (FOUO);
7. Law Enforcement Sensitive;
8. Legally privileged;
9. Payment Card Information (PCI); or
10. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA);
11. Sensitive but Unclassified.

Examples: "Personally identifiable information" (PII) would generally be designated as Level 3, but not always. For example, property records contain owner names and addresses but are traditionally public data and not protected from disclosure under FOIA. On the other hand, the public library tracks the books and materials borrowed by patrons so that it can ensure the return of those assets. Disclosure of what material was borrowed by which patron(s) would violate the personal privacy of the patron and is therefore exempted from mandatory disclosure by FOIA.

Protections: Level 3 data will only be stored and accessed on an encrypted computer. Lab staff will not email, post online, or otherwise make Level 3 data available through unencrypted channels. Level 3 data will be transferred between computers by using an encrypted flash drive or the Lab's secure upload facility. If Level 3 data is transferred via flash drive, the data will be deleted immediately from the flash drive after the transfer is complete and the deletion will be confirmed by ensuring that the data does not appear in the trash or recycle bin of the flash drive. Any data that is printed will be stored in a locked file cabinet and shredded when it is no longer needed.

Publication: Unless otherwise specified in a data use agreement with the data owner, the Lab may publish and present the aggregate results and conclusions of its analyses of Level 3 data to the general public; provided that:

1. The publication or presentation of results and conclusions shall not include personally identifiable information;

2. The publication or presentation of results and conclusions shall not include raw Level 2, 3, or 4 confidential or sensitive information, unless the publication or presentation of such information is agreed to by the data owner; and

3. The publication or presentation has been reviewed by the data owner as specified by the data use agreement with between the data owner and OCA.

Sharing: Level 3 data may only be shared with other Lab staff; OCA staff, contractors, and agents; and any individuals who are authorized to receive the data by the data use agreement between the data owner and OCA. If OCA receives a request for Level 3 data from a party outside the government, OCA will inform the data owner of the request and refer the requesting party to the data owner. OCA will not share the data with the outside party upon such a request. If OCA seeks to share the data with an outside party (for example, for replication purposes) the sharing of the data must be approved in writing by the data owner before the dataset may be shared by OCA, unless such sharing is authorized by the data use agreement between the data owner and OCA. When Level 3 data is shared by OCA, OCA shall take appropriate steps to ensure that sensitive or confidential is not unnecessarily shared and to ensure that the outside party appropriately protects and disposes of the data.

Disposal: Upon finishing the Lab's work with Level 3 datasets, Lab staff will dispose of the data as specified by the data use agreement with the data owner.

Level 4: Restricted Confidential

Description: Level 4 data refers to datasets for which the originating agency has determined that unauthorized disclosure could potentially cause major damage or injury, including death, to residents, agency workforce members, clients, partners, stakeholders, or others identified in the information, or otherwise significantly impair the ability of the agency to perform its statutory functions. Includes any dataset designated by a federal agency to be at the level of "Confidential" or higher under the federal government's system for marking classified information.

Protections: If Level 4 data is shared pursuant to a data use agreement between the data owner and OCA, specific security protocols to ensure the protection of the data will be included in the Agreement.

Publication: Level 4 data may be published only if specifically authorized by the data use agreement with the data owner.

Sharing: Level 4 data may be shared only if specifically authorized by the data use agreement with the data owner.

Disposal: Level 4 data shall be disposed of in the manner specified in the data use agreement with the data owner.

Notes:

1. The term "data owner", as used in this policy, refers to the District agency that shared the data with the Office of the City Administrator.

2. This policy is intended only for the internal use of the Office of the City Administrator. No person or entity is intended to be a beneficiary of this policy and no person or entity shall have any right, interest, or claim under this policy or be entitled to any benefit under or on account of this policy as a third party beneficiary or otherwise.

FOURTH AMENDMENT TO THE
DATA USE AGREEMENT
BETWEEN
THE METROPOLITAN POLICE DEPARTMENT
AND
THE OFFICE OF THE CITY ADMINISTRATOR

The Metropolitan Police Department ("MPD") and the Office of the City Administrator ("OCA"), collectively referred to herein as the "Parties", hereby enter into this Fourth Amendment to the Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator ("Agreement").

I. WHEREAS, the Parties entered into the Agreement on July 18, 2017;

II. WHEREAS, the Agreement governs the exchange, use, safeguarding, and ownership of data shared by MPD with OCA to allow OCA to evaluate MPD's Body-Worn Camera Program; Crime Gun Intelligence Center; and changes to MPD's standard processes;

III. WHEREAS, the Parties now wish to modify the Agreement in order to expand the purpose of the Agreement and evaluations to be conducted by the Parties; and

IV. WHEREAS, the Agreement was modified by the First Amendment to the Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator on February 1, 2018 to add the evaluation of the Community Based Crime Reduction Initiative as a purpose of the Agreement;

V. WHEREAS, the Agreement was further modified by the Second Amendment to the Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator on February 1, 2018 to add the evaluation of the National Museum of African American History and Culture Training Program as a purpose the Agreement;

VI. WHEREAS, the Agreement was further modified by the Third Amendment to the Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator on June 7, 2018 to add the Streetlight and Crime Analysis as a purpose of the Agreement;

VII. WHEREAS, sections 3 and 17 of the Agreement allow the Agreement and its Appendix A to be modified upon a signed, written agreement of the Parties;

VIII. NOW, THEREFORE, the Parties agree to further modify the Agreement as follows:

A. Section 2 of the Agreement ("Purpose of the Agreement") is amended by adding a new subsection ix. to read as follows:

"ix. Stop Data Analysis and Policy Evaluation

1. This project aims to understand how police contacts, stops, frisks, and arrests are conducted in the District by the MPD (e.g., what triggers these interactions, factors that determine how an interaction might progress from one type to another, and where these interactions are taking place); address any areas for improvement to ensure fair and equal treatment under the law; and update data collection policies and procedures in accordance with Title II, Subtitle G of the Neighborhood Engagement Achieves Results Amendment Act of 2016, effective June 30, 2016 (D.C. Law 21-125; D.C. Official Code §§ 7-2411 *et seq.*).

2. The Lab @ DC will conduct analyses to help MPD understand the current state of the implementation of police contacts, stops, frisks, and arrests, the current state of data collection on such interactions, and identify areas for improvement.

3. Expected work products include analyses of police contacts, stops, frisks, and arrest data; a pre-analysis plan for the evaluation of current police stop policy implementation; presentation slides on research design and findings; and a written report documenting the designs, analyses, and results of the analyses; and other content as needed."

B. Section 16 of the Agreement ("Duration") is amended by removing paragraph (a) in its entirety and replacing it with the following:

"a. The period of this Agreement is from its date of execution through the date by which OCA has deleted the Data under section 11 of this Agreement (the "Termination Date"); provided that, sections 4, 5, 6, 7, 8, 9, 11, and 12 shall survive beyond the Termination Date."

C. Appendix A of the Agreement is amended by adding a new row to the table of datasets to be shared pursuant to this Agreement, to read as follows:

Dataset #	**Dataset**	**General Description**	**Dataset Security Level**
14	Contacts, Stops, and Frisks	Records of all police contacts, stops, and frisks made by MPD	3

D. This Amendment shall be effective as of the date the last Party signs it.

E. Except as modified by the First Amendment, Second Amendment, Third Amendment, and this Fourth Amendment to the Agreement, all other terms and conditions of the Agreement shall continue in full force and effect.

IN WITNESS WHEREOF, the Parties have executed this Fourth Amendment to the Agreement as of the dates set forth below.

For the Metropolitan Police Department:

Peter Newsham
Chief of Police

Date: June 20, 2018

For the Office of the City Administrator:

Rashad M. Young
City Administrator

Date: 6/28/18

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE CITY ADMINISTRATOR

OCA Approval and Tracking Form

Date submitted: 6/18/19

☐ **For your awareness**
☒ **For your signature**

Document Information

1. Name of OCA Analyst	Vicky Mei	**3. Date document was received**	6/18/2019
2. Originating agency	The Lab @ DC, OCA	**4. Date needed**	ASAP
5. Name/title of document	**Fifth Amendment to the DUA between MPD and OCA**		

6. Brief description of document
This amendment to the MPD/OCA DUA does the following: **1)** updates data custodian from David Yokum to Vicky Mei, Data Scientist, **2)** allows for future data custodian changes to be made via email, **3)** updates the Party Representative in Section 15 to Sam Quinney, **4)** allows for future Party Representative changes to be made via email

It has already been signed by Peter Newsham, the Chief of Police for MPD.

7. Recommendation

I recommend signing the document.

8. Additional notes (e.g., prior approvers, controversial aspects, etc.)

Additional Clearances

	Jenny Reed	Barry Kreiswirth	Ben Stutz	Christina Murphy	Rashad Young
Approval required	☒	☒	☒	☐	☒
Reviewer approval	☑ Yes ☐ No	☑ Yes ☐ No	☒ Yes ☐ No	☐ Yes ☐ No	☒ Yes ☐ No
Initials	JR	BK	BS		
Date	6/24/19	6/25/19	6/25/19		6/25/19

Yes to sign

Reviewer Comments (if any)

Reviewer initials	Comment

FIFTH AMENDMENT TO THE
DATA USE AGREEMENT
BETWEEN
THE METROPOLITAN POLICE DEPARTMENT
AND
THE OFFICE OF THE CITY ADMINISTRATOR

The Metropolitan Police Department ("MPD") and the Office of the City Administrator ("OCA"), collectively referred to herein as the "Parties", hereby enter into this Fifth Amendment to the Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator ("Agreement").

I. **WHEREAS**, the Parties entered into the Agreement on July 18, 2017;

II. **WHEREAS**, the Agreement governs the exchange, use, safeguarding, and ownership of data shared by MPD with OCA to allow OCA to evaluate MPD's Body-Worn Camera Program; Crime Gun Intelligence Center; and changes to MPD's standard processes;

III. **WHEREAS**, the Parties now wish to modify the Agreement in order to update the Data Custodian of the Agreement and OCA's representative; and

IV. **WHEREAS**, the Agreement was modified by the First Amendment to the Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator on February 1, 2018 to add the evaluation of the Community Based Crime Reduction Initiative as a purpose of the Agreement;

V. **WHEREAS**, the Agreement was further modified by the Second Amendment to the Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator on February 1, 2018 to add the evaluation of the National Museum of African American History and Culture Training Program as a purpose the Agreement;

VI. **WHEREAS**, the Agreement was further modified by the Third Amendment to the Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator on June 7, 2018 to add the Streetlight and Crime Analysis as a purpose of the Agreement;

VII. **WHEREAS**, the Agreement was further modified by the Fourth Amendment to the Data Use Agreement Between the Metropolitan Police Department and the Office of the City Administrator on June 28, 2018 to add the evaluation of police stop data as a purpose of the Agreement and add a data variable to Appendix A.

VIII. **WHEREAS**, sections 3 and 17 of the Agreement allow the Agreement to be modified upon a signed, written agreement of the Parties;

IX. **NOW, THEREFORE**, the Parties agree to further modify the Agreement as follows:

A. Section 10 of the Agreement ("OCA Data Custodian") is amended by removing paragraph (a) in its entirety and replacing it with the following:

> "a. OCA designates Vicky Mei, Data Scientist, as the Data Custodian under this Agreement. OCA may change the person designated as the Data Custodian at any time by giving MPD notice by email of the new Data Custodian's name, title, and contact information."

B. Section 15 of the Agreement ("Parties' Representatives") is amended by removing paragraph (a) in its entirety and replacing it with the following:

> "a. The following individuals are the Parties' representatives under this Agreement:
>
> MPD
> Matthew Bromeland
> Chief of Staff, Executive Office of the Chief of Police
> 300 Indiana Avenue, N.W.
> Washington, D.C. 20001
> Email: matthew.bromeland@dc.gov
> Phone: (202) 438-8453
>
> OCA
> Sam Quinney
> Interim Director of The Lab @ DC
> 1350 Pennsylvania Avenue, N.W.
> Washington, D.C. 20004
> Email: sam.quinney@dc.gov
> Phone: (202) 394-4468
>
> The representatives identified above may be changed by the Parties through notice by email to the other Party of the new representative's name, address, email address, and phone number, and without amendment to this Agreement."

C. This Amendment shall be effective as of the date the last Party signs it.

D. Except as modified by the First Amendment, Second Amendment, Third Amendment, Fourth Amendment, and this Fifth Amendment to the Agreement, all other terms and conditions of the Agreement shall continue in full force and effect.

IN WITNESS WHEREOF, the Parties have executed this Fourth Amendment to the Agreement as of the dates set forth below.

For the Metropolitan Police Department:

Peter Newsham
Chief of Police

Date: JUN 1 8 2019

For the Office of the City Administrator:

Rashad M. Young
City Administrator

Date: 6/25/19