



U.S. DEPARTMENT OF JUSTICE  
OFFICE OF COMMUNITY ORIENTED POLICING SERVICES  
145 N Street NE, Washington, DC 20530

**COPS**

**DATA SHARING AGREEMENT**  
**between**  
**U.S. DEPARTMENT OF JUSTICE,**  
**OFFICE OF COMMUNITY ORIENTED POLICING SERVICES**  
**and**  
**SAINT ANTHONY, MINNESOTA POLICE DEPARTMENT**  
**for**  
**COLLABORATIVE REFORM INITIATIVE FOR TECHNICAL ASSISTANCE**

This Agreement is made by and between the United States Department of Justice, Office of Community Oriented Policing Services (the "COPS Office"), and the Saint Anthony, Minnesota Police Department.

1. As part of the COPS Office engagement with the Saint Anthony Police Department to administer Collaborative Reform Initiative for Technical Assistance (CRI-TA), Hillard Heintze, LLC ("the Contractor") pursuant to the U.S. Department of Justice (DOJ) Contract Number DJJ15-C-2614 is charged with collecting, accessing and securely maintaining the Police Department's records/data for review and analysis. This Agreement sets forth the terms and conditions below for the transfer of data between the Police Department and the Contractor to advance the Collaborative Reform process.
2. For purposes of this Agreement, the data being collected and accessed by the Contractor for the CRI-TA project may contain, but is not limited to, the following types of information:
  - a. "Personally Identifiable Information" ("PII"), is any information about an individual including, but not limited to, information related to education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, or other personal information linkable to a specific individual.
  - b. "Individually Identifiable Information," is information collected about human subjects during research and statistical activities that is either labelled by name or other personal identifiers, or can, by virtue of sample size or other factors, be reasonably interpreted as referring to a particular private person.
  - c. "Sensitive Law Enforcement Data" which may include, but is not limited to:
    - i. Departmental policies, manuals, SOPs, and other written memos or directives

- ii. Training lesson plans, curriculum, schedules, records, and other training materials
- iii. Department strategic plans, audits, and inspection reports
- iv. Any collective bargaining agreements
- v. Use of force and any other internal review board policies, reports and related data
- vi. Criminal and administrative investigation files
- vii. Aggregate and detailed data regarding crime reporting, traffic and pedestrian stops, related data collection and reporting, and other reports generated by employees of the Department including:
  - Documents prepared by officers when they encounter an individual and believe it is important to make a record of the contact, such as field interview cards
  - Felony and misdemeanor arrest, citation, and summons data
  - Data collected to identify race, ethnicity, or protected class during police contact
  - Video or audio recordings of community member encounters, stops, and arrests
- viii. Dispatch and CAD data
- ix. Aggregate employee demographic data
- x. Disciplinary investigations and findings
- xi. Data required to study bias
- xii. Internal review records and reports, including use of force review board policies and data
- xiii. Other departmental documents, reports and data as deemed appropriate during this CRI-TA process

3. To ensure the CRI-TA process is successful, the Police Department will:

- a. Provide to the Contractor the data identified in paragraph 2 of this Agreement, and any other data deemed necessary to support the CRI-TA project, as requested by the Contractor in writing.

- b. Facilitate access and coordination for all data sources used by the Police Department, and to the extent possible, provide the data in the formats requested by the Contractor, including, but not limited to, meta-data, Excel spread sheet data, scanned PDF files, Word documents, or text files. Delivery of the data will be by a secure method such as Secure File Transfer Protocol (SFTP), encrypted CD-ROM, or Virtual Private Network (VPN).
- 4. To protect the confidentiality and maintain the security of the data provided by the Police Department for the CRI-TA project, the COPS Office established the following protocols which apply to the Contractor and its employees (to include contractors, subcontractors, and subject matter experts):
  - a. Prior to working on this CRI-TA project the Contractor's employees signed a Non-Disclosure Agreement with the COPS Office that restricts the Contractor's employees from revealing, divulging or publicizing any matters dealt with under this project unless specifically authorized in writing by the COPS Office.
  - b. Only the Contractor's employees with subject matter expertise and a need to know as part of the Collaborative Reform process will have access to the Police Department data.
  - c. The Contractor understands that the access granted to data containing individually identifiable information and PII may only be used for the purposes identified in the CRI-TA work plans, and by the Contractor's employees authorized to participate in the CRI-TA project. All such use of the data must comply with applicable federal regulations.
  - d. The Contractor will submit, upon request, the appropriate approved segments of the CRI-TA work plans for review by the Police Department when requesting Police Department data or research support.
  - e. The Contractor will use the data file(s) for generating statistical or technical reports, briefings and manuscripts, scientific presentations, and publications, including demographic and situational information generated by the data listed in paragraph 2 of this Agreement. All Contractor's employees with access to data provided by the Police Department will follow the terms of this Agreement.
  - f. The Contractor will treat all data generated and supplied by Police Department as confidential information and retain strict control standards over the data while under review.

- g. The Contractor will not make any disclosure of any data or aggregations of data from the file(s) provided by the Police Department in any form, including, but not limited to, presentations, reports, articles or other publications.
- h. The Contractor may securely retain data file(s) and/or any derivative file(s) on the Contractor's network drives for purposes of completing the CRI-TA project pursuant to the contract with the COPS Office, DOJ Contract Number DJJ15-C-2614. At the conclusion of the contract period with the COPS Office, the Contractor will sanitize all media which has been used in connection with the CRI-TA project, such as PC hard drives and memory, network server hard drives and memory according to DOJ approved procedures. In the event that the Contractor is unable to sanitize the media according to DOJ approved procedures, then the Contractor must turn over the media to the DOJ for destruction.
- i. The Contractor will ensure that sensitive information does not remain on the storage media, including hard disks and floppy disks, when the PC is removed from the Contractor's area for maintenance or other use. Maintenance personnel must be escorted and monitored by the COPS Office or Contractor personnel when allowed to perform on-site maintenance for the equipment. The storage media must be removed from the PC prior to removal of the PC from the area for maintenance.
- j. Any and all removable storage media will be appropriately marked with the classification level.
- k. The Contractor will ensure appropriate administrative, technical, procedural, and physical safeguards are established to protect the confidentiality of the data and to prevent unauthorized access to it. The safeguards shall provide a level of security for any PII as required by state and federal law.
- l. The Contractor will ensure the proper safeguarding and disposition of all copies (in any format) of project-related information during and after the CRI-TA project to protect against the unauthorized access to or disclosure of such information pursuant to the contract with the COPS Office.

- m. Unauthorized disclosure of the data may result in immediate termination of the Contractor's involvement in CRI-TA project activities, and any other remedies available by law.
- 5. This Agreement may be formally modified by the COPS Office, as needed, to facilitate the success of the CRI-TA process.
- 6. This document constitutes the entire agreement of the parties concerning the subject matter hereof, and shall become effective when signed by an authorized representative of each party.

RECC for DATE: 12/2/16  
Ronald L. Davis, Director, The COPS Office  
Rob. F. Chapman, Deputy Director, COPS office

Jon Mangseth DATE: 11-29-16  
Jon Mangseth, Chief, Saint Anthony, Minnesota Police Department

