MEMORANDUM

TO: Marty Chakoian
Tina Podlodowski

FROM: Merrick Bobb
Matthew Barge

DATE: March 31, 2014

RE: Business Intelligence System: Overview of Expected Functionalities & Capabilities

---

The Seattle Police Department ("SPD") currently lacks data to assess officer performance; manage constitutional violations; identify misconduct; manage the risk of litigation and liability; hold supervisors and managers accountable; and identify and reward those who are best at community based policing, communication, and constitutional, respectful, and effective law enforcement. The SPD has no accurate and trustworthy data about use of force, *Terry* stops, and litigation. Furthermore, SPD's existing database platforms make data retrieval and analysis time-consuming and frequently unreliable.

As such, the SPD is approximately 20 years behind major law enforcement agencies—including the Los Angeles Police Department ("LASD"), the Los Angeles Sheriff's Department ("LASD"), the Phoenix Police Department, the Miami Police Department, and Washington DC's Metropolitan Police Department—that have computerized, relational databases for tracking, managing, and analyzing officer performance. As the Monitoring Team noted in its Second Semiannual Report, "the Business Intelligence System which will pass muster will be a close first cousin to the LAPD's Teams II and the LASD's PPI in terms of functionality, depth, speed, breadth, flexibility, and ease of use . . . . " (*Id.* at 12.)

The best of these databases permit and facilitate ad hoc queries as well as pre-programmed reports. The ease and transparency of the process for ad hoc queries is essential. SPD will need a research and development unit that uses these ad hoc querying capabilities to conduct longitudinal studies and identify patterns and trends.

Additionally, to ensure data accuracy and integrity, there needs to be a capacity to audit the data after it is entered for completeness and accuracy. The system should prompt the person entering data if there are open fields to be filled in or the lack of a narrative.

This memorandum provides a general overview of the functionalities and capabilities that the Monitoring Team will be expecting to see in a business intelligence system. It is not a comprehensive description of everything that such a system must do or an exhaustive list of the

information and data that must be collected. It is, however, an introduction to the major practices, processes, procedures and objectives that must be served by a comprehensive business intelligence system.

I. FUNCTIONALITY

A robust business intelligence system must accommodate discrete user sets who will use the system differently and will, therefore, require some differing functionality. Specifically, SPD will rely on the business intelligence system to provide the following, broad functionalities:

- **Incident Reporting and Performance Data Tracking.** All officers will use the business intelligence system to report the occurrence of various incidents, including uses of force, stops and detentions, vehicle collisions, and the like. That is, officers will satisfy the Department's basic reporting requirements by entering data about the incident and providing (in almost all instances) a free-text narrative that describes the incident.

  For other classes of performance data, such as tracking an officer's missed court appearances or training attended (or required training not attended), the business intelligence system must store (or otherwise access) that data in a manner that can be queried in real-time.

- **Incident Review.** For the average incident (such as a lower-level use of force or a stop of a citizen), the officer's Chain of Command (e.g., sergeant, lieutenant, captain) conduct the primary investigation and/or review of the incident. Accordingly, the business intelligence system must permit an officer's supervisors to review incidents and forward their reviews up the Chain.

  For some incidents, including uses of force and traffic collisions, a review culminates in consideration of the incident by a centralized Board that convenes to consider the incident for rigor of the investigation below, consideration of officer discipline, and—most importantly—to consider whether the incident has any prospective implications for training, practice, policy, or procedure.

  Regardless of the review process required for specific incident types, the business intelligence system should allow immediate, comprehensive information about the status of a current review—who is reviewing it, how long each step in the chain of review has taken, and the like.

- **Administrative Investigations.** Currently, SPD uses two specialty groups to conduct internal, administrative investigations of incidents.

The first is the Office of Professional Accountability ("OPA"), which conducts investigations of alleged officer misconduct. An incident can be referred to OPA by any officer at any time. For example, if an officer reports a use of force incident and a sergeant, subsequently reviewing the incident, believes that the facts suggest possible officer misconduct, that sergeant will refer the incident to OPA for investigation, review, and ultimate adjudication.

The second is the Force Investigation Team ("FIT"). The FIT team—a specialized, highly trained investigative section—investigates "serious" uses of force, including Type III incidents and officer-involved shootings. (They may investigate Type II incidents if sergeants or others within the Chain of Command so request.) Thus, for lower-level uses of force (Type I and Type II incidents), a sergeant conducts an investigation of the force. For higher-level uses of force (Type III and officer-involved shooting incidents), the FIT team investigates.

Both OPA and FIT are likely to use the business intelligence system as a case management platform. (Currently, OPA and FIT are both transitioning their case management platforms from SPD legacy platforms to IAPro, the interim database solution.) Accordingly, the business intelligence system should allow OPA and FIT to either manage investigations within the system or allow for seamless integration with any alternative platforms that they may use (e.g., IAPro). The Monitoring Team believes that SPD may be better served over the long-term by having a case management platform built into the end-product business intelligence system.

- **Early Intervention** (also referred to as "Performance Mentoring"). Law enforcement agencies nationwide use so-called "early intervention" or "early warning" systems to identify performance trends among officers that may warrant supervisor review, behavioral intervention, mentoring, specialized training or re-training, and the like. The idea is for the Department to identify and assist officers with less optimal performance trends and intervene appropriately to prevent future occurrences of problematic behavior or performance.

  SPD's Performance Mentoring Program, which is what it calls its early intervention policy, was recently approved. It is attached as Exhibit A.

  One provision provides specific threshold levels of activity across defined indicator criteria that, upon an officer meeting those levels, sets the occasion for a performance mentoring assessment. For instance, with respect to vehicle pursuits, an officer having engaged in two (2) vehicle pursuits with a rolling, 24-month period will "trigger" a performance mentoring assessment.

Categories of data that serve as "indicator criteria," for which the policy also defines threshold levels of activity that will trigger a performance assessment, include: uses of force; vehicle collisions; receipt of OPA complaints (e.g., complaints of officer misconduct); receipt of Equal Employment Opportunity ("EEO") complaints (e.g., employment-related complaints such as sexual harassment or discrimination); being named in actions, claims, or lawsuits against the City; vehicle pursuits; unexcused failures to appear in mandatory training; K9 apprehension/bite ratios; and officer-involved shootings. Accordingly, the business intelligence system must be able to rigorously track of these classes of data.

The performance mentoring assessment involves a comprehensive review of performance data across the universe of performance that the business intelligence system tracks. That is, meeting a threshold of behavior in one area "triggers" a comprehensive review of an officer's performance data. Accordingly, the business intelligence system must provide command staff with the ability to easily query a summary of the officer's performance data across his or her career.

It should also be noted that SPD's policy requires that sergeants and commanders review the performance mentoring criteria thresholds of employees that they supervise at least monthly. Again, the business intelligence must, therefore, allow officers to quickly retrieve an officer's performance summary—a report that must be configured to provide officers with clear, accurate information in an easily understandable format.

- **Data-Driven Management and Data Analytics.** The Monitor's Second Semiannual Report observed:

> The active use of data and statistical analysis has improved the way that police conduct law enforcement and measure performance trends. Indeed, the days of police management needing to rely on hunches or gut intuition alone . . . are over . . . . Modern policing is, in short, a scientific and data-driven enterprise . . . . [T]oday's business intelligence systems permit tremendous amounts of data to be retained, sorted, and mined for research, insight, and a more comprehensive picture of officer performance, department-wide practices, and both systemic and officer-specific trends.

(*Id.* at 6.)

Thus, a business intelligence system must allow for command staff as well as a dedicated data analytics group within SPD to conduct real-time, in-depth analyses of officer performance. The Department must be able to use the system to proactively and

affirmatively manage the risk of unconstitutional, biased, or otherwise problematic performance.

II. SPECIFIC CAPABILITIES

The Monitoring Team's recommends that a business intelligence system include the following elements or "modules":

A. Use of Force

The SPD divides force into Types I, II, and III, with Type I uses of force constituting the deployment of less serious, severe, or injurious force and Type II constituting more serious, severe, or injurious force. (Officer-involved shootings are a separate, fourth category.) By SPD policy, a use of force module should record every reportable instance when an SPD officer uses more force than unresisted handcuffing. The data should be reported uniformly.

Basic information may be recorded via "checkboxes" or selecting an appropriate response from a drop-down "pick list." For example, on the Department's current use of force reporting form—which officers must complete following the use of force at any level—officers are asked to select a "reason for [the] use of force." Options that they can select include: arrest, defense of others, defense of self, non-compliance, protection of property, or response to disturbance/trespass. Attached as Exhibit B are the use of force reporting forms to be used by the SPD in its stopgap database, IAPro. Attached as Exhibit C are the SPD policies governing the reporting and review of use of force incidents.

The module must also allow for officers to write and include a free-text incident narrative. The narratives should explore all key decisions made by an officer from the time of dispatch or self-initiated activity until the suspect against whom force was used is booked, given medical attention, or let go. The officers should explore why alternatives to force—de-escalation, calling for backup, summing persons skilled in crisis intervention, stepping back—were not reasonable in the circumstances. The business intelligence system should be capable of converting to text all narrative portions of the use of force form.

The Monitoring Team favors officer-based entry of use of force, and other incidents, into the business intelligence system so that responses to questions and data entered reflects the officer's perspective, which is the appropriate perspective within Fourth Amendment jurisprudence. Thus, in the interim IAPro system, officers themselves will enter information (through a web-based interface that feeds data into the flagship IAPro software solution) about use of force incidents. In the context of the business intelligence system, decisions will likewise need to be made about whether officers will enter data themselves in the field into the system or, instead, will send information to a central location for inputting.

The data retention and governance policies applied to the business intelligence system must permit that records are maintained for the entire career of the officer in question plus five or more years so as to be available to subsequent employers.

The business intelligence system must provide the ability for the chain of command to review use of force incidents and the Department's Use of Force Review Board ("UOFRB")—the central hub of review, learning, and change when it comes to department practice, policy, and procedure—to conduct comprehensive assessments of such incidents. Accordingly, the system must provide the ability for investigators to attach documents, audio, and video; to track investigative actions and progress; and to access performance records (such as with respect to training) on involved and witness officers.

By way of just a few examples of the analytical functionality that the business intelligence system should have with respect to use of force, the database should permit a qualified user to sort by an officer's name or badge number and collect, for example, all reported use of a Taser. The user could ask for all uses of pepper spray between midnight and 6 AM in X sector of Y precinct from July through October of a given year. One could sort and rank all gang enforcement officers by numbers of uses of force by precinct. One could determine every instance in which an African-American officer used force on a white subject and each instance were a white officer use force on an African-American suspect. The qualified user should be able to compare like officers in like assignments to determine variances in use of force patterns.

Likewise, the module should attach the use of force package produced in each case, including the investigator's file as well as reviews up the chain of command.

B. Officer-Involved Shootings, In-Custody Deaths, or Other Fatal Incidents

It is best practice to have a separate module for officer-involved shootings, and there should be a separate module for inputting relevant information about them. Attached as Exhibit D is a model of a paper-based form that reflects the classes of information and analysis of an officer-involved shooting that should be captured and conducted. It should be noted that an officer-involved shooting is a use of force, and the officer-involved shooting modules should be able to interface directly with the use of force module such that summary statistics about an officer's, precinct's, or the Department's overall uses of force reflect and include such shootings. Despite this need, utilizing a separate module for shootings will likely allow for a more finely tuned and customized inquiry.

C. Complaints

The business intelligence system should track all complaints of possible policy violations, criminal activity, or other misconduct by SPD personnel from the newest police officer to the Chief of Police, regardless whether the complaints are from the general public or from inside the department. All litigation and all claims should be considered complaints and investigated

internally. The OPA should have the ability to open an investigation of any possible misconduct that comes to its attention or by being proactive.

The guiding principle on public and internal complaints of officer misconduct is that the Constitution guarantees the public the right to petition the government for redress of grievances. It is a fundamental right and one of the hallmarks of a free, open, and democratic society. It channels public dissatisfaction and anger into constructive pathways leading to investigation, resolution, and, if called for, correction or remediation. Law enforcement agencies are an arm of government. The right to petition law enforcement by filing complaints should be untrammeled, and impediments should not be strewn in the path of complainants.

Accordingly, the widest possible net should be thrown open at intake to receive all complaints from all possible sources of complaint. While the procedures for investigation and resolution of these complaints may differ depending upon their nature, it is a recommended practice to take in all complaints. Moreover, complaints as a whole provide the law enforcement agency with insight as to how it is perceived by the public. Law enforcement is not doing its job if the public as a whole or in part believes the police are not effective, ethical, and respectful.

The complaints module should be based upon a form that captures all relevant facts, including the identification of the officer and of the complainant, contact information, witnesses, and a log of all investigative steps. Reminders should be built in to alert investigators and their supervisors, managers, and executives of deadlines for the review and resolution of complaints.

D. Litigation

The SPD lacks data about litigation generated from its activity. A litigation module should track all open cases and all closed cases involving the SPD. On open cases, complete information as to all plaintiffs and all defendants should be recorded. Likewise, one should record the court number of the case, when it was opened, the status of the case updated regularly, the amount of the demand, and counsel's informed judgment about exposure. All counsel of record should be noted. The litigation record should also summarize all claims and causes of action and whether the underlying event was the subject of use of force review or a complaint. It should also note whether a given case is on appeal along with its case number and identification of the appellate court in which it is pending.

Closed cases should contain all the foregoing information along with the ultimate result, including whether the case was dismissed, abandoned, settled, tried or appealed. If there was a settlement or judgment, the dollar amount should be stated as well as legal fees generated or otherwise imputed. The litigation result should be compared to the use of force investigation or OPA investigations of the same incident to determine possible deficiencies.

The business intelligence system should be capable of identifying which individual officers generate the most litigation, complaints, and claims. The litigation module should also track discovery requests and relevant dates.

E. Administrative Investigations

As noted above, the business intelligence system should track all administrative investigations of possible employee misconduct, including all FIT administrative investigations as well as OPA investigations. All the claims and charges should be listed on an employee by employee basis as well as the results of the investigation. If the investigation is sustained, the specific discipline initially recommended and ultimately imposed should be tracked.

Thus, in addition to assisting FIT and OPA in conducting investigations and managing cases, the incidence of administrative investigations and their outcomes must be part of individual officer's performance summaries so that the Department and its command staff can consider such investigations as a performance metric.

F. Criminal Investigations

All criminal investigations should be tracked. For purposes of secrecy and privacy, the existence of a criminal investigation should be known only by the Chief of Police, the Assistant Chief of Compliance, the Director of OPA, and the unit commander and investigators specifically involved, assuming there is no conflict.

G. Stops, Searches, and Arrests

A *Terry* stop module should be able to track information about stops and detentions of civilians that includes:

a. The date, time, and location of the stop;
b. The name and serial numbers of all officers, from any agency, present at any time during the stop
c. Whether there is any in car video/audio of the stop and if not, why not.
d. the individual's apparent race/ethnicity (including Latino as a separate category), color, or national origin; gender; and apparent age;
e. the reason for the stop, including a description of the facts creating reasonable suspicion and/or probable cause;
f. the disposition of the stop, including whether a citation was issued or an arrest made of any individual;

g. whether a frisk was conducted as a result of the stop, and if so, a description of the facts justifying the frisk
h. the result of any frisk, including whether any physical evidence was seized, whether the search led to an arrest, and a description of the facts creating probable cause for the arrest.
i. Whether a person was moved or transported from the location of the initial stop and if so, why.
j. Whether the person stopped was specifically directed to assume any posture or position and if so, what posture or position and why.
k. The duration of the stop and an explanation of the factors justifying the length of the stop.

Attached as Exhibit E, is a memorandum from Matthew Barge and Ian Warner setting forth parameters for use of stop data. (It should be noted that this "Data Analysis Plan" is preliminary only and subject to modification through mid-May 2014.)

H. Integrity Module

The business intelligence system should collect data reflecting upon the integrity and honesty of police officers. It should capture any instance in which evidence is suppressed by a court because of constitutional violations. It should also capture any instance in which a trier of fact disbelieves the testimony of a police officer. It should contain a *Brady* list of police officers whose integrity has been successfully challenged. It should record all instances in which a "contempt of cop" charge is made by a police officer without any other crime being charged. "Contempt of cop" includes resisting arrest, obstruction, and battery on a police officer without injury.

I. Traffic Collisions

Preventable traffic accidents by police officers result in substantial settlements or judgments. Accordingly, police departments frequently track traffic collisions and the identity of officers who are involved in them more than others. The business intelligence system should feature a mechanism for tracking traffic collisions and automobile accidents involving patrol cars.

J. Training

Thorough and complete records of an officer's complete training history are vital to the Department's risk management strategy and should be collected by the business intelligence system.

III. CONCLUSION

With experiencing with both building, modifying, and using business intelligence systems in many other cities and departments, the Monitor and Monitoring Team look forward to partnering closely with the Department, City, Department of Justice, and outside vendors and experts to develop a high-quality business intelligence system that SPD can use to assess, analyze, and manage officer and departmental performance.