

### CITY OF PORTLAND, OREGON



#### **Bureau of Police**

Ted Wheeler, Mayor
Danielle M. Outlaw, Chief of Police
1111 S.W. 2nd Avenue • Portland, OR 97204 • Phone: 503-823-0000

Integrity • Compassion • Accountability • Respect • Excellence • Service

## **Directive 345.00, Employee Information System**

### Introduction

In accordance with the 2012 Settlement Agreement, the Bureau is required to conduct an initial sixmonth and subsequent twelve-month reviews of Department of Justice (DOJ)-identified directives after receiving initial DOJ approval on the directive. The DOJ originally approved Directive 345.00, Employee Information System, in October 2016. The Policy Development Team worked in conjunction with internal staff, the DOJ and the Compliance Officer and Community Liaison (COCL) to review and revise the directive. This directive establishes procedures for use of the Bureau system that compiles and tracks data pertaining to members' performance and behavior.

### **Public Comments**

The Bureau received input from one community member over the course of both universal review and public comment periods. The community member commented on several aspects of the directive, including the review of use of force incidents, the timing of a member's EIS review upon transferring to a new unit, the need to define a threshold-related term, and general EIS reporting.

# Supervisor Review of Use of Force Incidents

The commenter expressed concern that the supervisory review of use of force incidents may undermine full administrative investigations of alleged misconduct conducted by Internal Affairs (IA) or the Independent Police Review (IPR). This appears to conflate a supervisor's investigation of an isolated force incident and their after action reporting on that incident, as described in Directive 1010.00, Use of Force, with a supervisor's review of relevant reports or case files, EIS data, and information contained in the Performance Discussion Tracker (PDT) and Alert Management System (AMS) in this context – otherwise stated, a less formal macro-level review of a member's performance and/or behavioral trends. A supervisor's review through the lens of this directive does not in any way subvert an IA and/or IPR investigation of alleged misconduct or the standard investigation procedures for all force events as established in Directive 1010.00, Use of Force.

# Post-Transfer Review

The directive provides guidance regarding the review of a member's EIS data should the member transfer to another unit or serve in a temporary assignment for a prescribed duration. We received an inquiry about the deadline by which a supervisor must review the EIS record of a member who is new to their command, as well as the timing of the review. More specifically, the commenter recommended that supervisors conduct reviews of this nature prior to the completion of the transfer. Although supervisors are informed of incoming members or temporary assignments, staff changes are authorized by the Chief and are typically made to address an operational or strategic need. Given staffing demands, these shifts may need to occur quickly. Furthermore, a supervisor could be reassigned prior to the effective date of a member's transfer or temporary assignment, so allotting 30 days post-transfer affords the existing or new supervisor ample time to acquaint themselves with the member's performance- and/or behavior-related information.

#### Traumatic Incidents

The commenter suggested the directive should include a definition of "traumatic incident," which is a threshold criterion. The Policy Development Team considered this recommendation, but decided not to include a definition in the policy, so as not to generate any confusion with the term "critical incident," which is defined in Directive 416.00, Critical Incident – Temporary Altered Duty and is different in concept than the traumatic incident threshold in this policy. However, the meaning of the term in this context is largely derived from the National Incident-Based Reporting System (NIBRS) coding system, which is a reporting system widely used by law enforcement agencies. Moreover, to ensure that EIS users have a clear understanding of the intent behind this threshold, the term is also described in EIS as "an event, occurring while on duty, which may cause physical, emotional, and/or psychological injury or harm and has the potential to interfere with a member's ability to function either at the scene or later."

## EIS Reporting

The Bureau received a request through the universal review process to make EIS data and information available to the public. While the Bureau does not generate an EIS-specific report, given the confidential nature of the information stored in the system, there are other sources available that include several EIS-related data points, such as the Annual Force Audit and IPR's quarterly and annual reports. As the commenter correctly identifies, the settlement agreement does require that all reports related to the implementation of the agreement be made publicly available; however, as the settlement agreement also states, these requirements do not undermine state and federal confidentiality laws. The Professional Standards Division (PSD), which houses the EIS team, maintains a positive and collaborative working relationship with IPR to ensure that relevant and non-confidential data and information are available for the purpose of promoting transparency and accountability through publicized reports.

We thank every individual who took the time to provide feedback on this directive. All comments received during both review periods are attached at the end of this document. We have removed all personal information to protect the privacy of commenters.

# The Bureau's Revised Policy

In its initial approval of Directive 345.00, Employee Information System, in October 2016, the DOJ noted at the time that the policy complied with the terms of the settlement agreement and relevant professional standards. With that in mind, the Bureau made few significant revisions to the directive, primarily clarifying roles and certain procedural elements. Specifically, the Policy Development Team sought to clearly define the role of the Force Inspector with regard to the review and analysis of groupand supervisor-level force data, as well as the various alert notifications that trigger threshold breaks. Furthermore, the team modified the section regarding the use of the PDT to clarify that the tool may also be used for non-sworn Bureau members.

The Bureau believes that the revised directive provides more clarity and enhanced guidance to its members; however, any suggestions to further improve this policy are welcome during its next review.

This directive will become effective on April 15, 2019.

Published on 4/15/19

## 345.00, Employee Information System

### (EIS) Refer:

- DIR 215.00, Member Performance Evaluations
- DIR 905.00, Non-Force After Action Reporting
- DIR 1010.00. Use of Force
- Professional Standards Division Standard Operating Procedure 44, Employee Information System Alert Processing Guide
- Professional Standards Division Standard Operating Procedure 47, Force Data Analysis at the Group and Supervisor Level
- PPA Labor Agreement

#### **Definitions:**

- Alert: A threshold break notification that is assigned a case number by the Employee Information System Administrator; a Responsibility Unit (RU)-generated request to review a member's performance and/orbehavior; and/or a Force Inspector-generated request to review force trends at the RU level.
- Alert Management System (AMS): A system within EIS that serves as a repository for all case notes associated with any alert.
- Employee Information System (EIS): The EIS consists of a read-only database that collects information from external data sources, the Alert Management System, and the Performance Discussion Tracker.
- Performance Discussion Tracker (PDT): A system within EIS that allows supervisors to record conversations about member performance and/or behavior and any follow up on those conversations. Members may also submit a response within the system.
- Supervisor: A sworn Portland Police Bureau member at the rank of sergeant or above (or anyone acting in those capacities) and non-sworn personnel with oversight responsibility for other sworn members.
- Supervisory Action: A non-disciplinary process designed to give sworn members feedback
  on their performance and promote best practices. Supervisory actions may include
  coaching, commending, debriefing, monitoring, referring to the Employee Assistance
  Program (EAP), requiring training, temporarily re-assigning, or some other form of nondisciplinary action.
- Supervisor Review: A review of information concerning a sworn member's performance and/or behavior.
- Threshold: Pre-programmed criteria established by the Chief of Police, including:
  - Shift Force Ratio: a sworn member's force ratio is greater than or equal to three (3) times their shift's average ratio in the preceding six (6)months;
  - o Force Ratio: a sworn member's force ratio is greater than or equal to 20% of their

- arrests in the preceding six (6) months;
- o Force Count: a sworn member uses force three (3) or more times in the preceding thirty (30) days;
- o Criminal Complaint: a member receives a complaint with an allegation of criminal misconduct;
- o Complaint in Same Category: a member receives two (2) or more complaints with at least one (1) allegation in each complaint being in the same category (such as two (2) complaints that both have conduct allegations) for events in the preceding six months:
- o Complaint Count: a member receives three (3) or more complaints for events in the preceding six (6) months;
- Traumatic Incidents: a member experiences three (3) or more traumatic incidents in the preceding thirty (30) days;
- o Commendations: a member receives two (2) or more commendations for events in the preceding six (6) months.
- Threshold Break: An automatic notification to the EIS Administrator when a member reaches or exceeds a threshold.
- Type I Alert: An alert notification that pertains to a complaint- or commendation-related threshold break.
- Type II Alert: An alert notification that pertains to a force- or traumatic incident-related threshold break.
- Type III Alert: An alert notification that pertains to statistically meaningful deviations from normative behavior, with respect to groups and their respective supervisors, which the Force Inspector has determined places such groups and the respective supervisors at risk of problematic trends.

# **Policy**:

- The EIS is an application that compiles information from the Police Bureau and other data sources to enable a comprehensive review of a sworn member's work performance. The use of EIS benefits the Bureau and sworn members alike by facilitating professional growth through a feedback process that reinforces the Bureau's management and accountability systems, standards, and expectations.
- 2. It is the policy of the Bureau to encourage and develop personnel. EIS supports this goal by supplying information to supervisors that will allow them to better develop, manage, and support their sworn members.
- 3. EIS and the information developed therein shall not form the basis for disciplinary action but may be used for non-disciplinary notice purposes, such as development of work performance plans and letters of expectation. The reports from EIS may not be used by the City for disciplinary, transfer or promotion decisions. However, if the underlying data that appears in EIS is maintained separately by the City and is simply reflected in EIS, nothing

in this directive prevents the City from making appropriate use of the underlying data in disciplinary, transfer, or promotion decisions.

4. The AMS and PDT shall be treated as confidential material.

### **Procedure**:

- 1. Performance Discussion Tracker:
  - 1.1. The PDT allows supervisors to record discussions about a member's performance and behavior. Every entry to a member's PDT should be preceded by a discussion with the member.
  - 1.2. Supervisors who observe positive behavior or performance related to a member's job duties as described in the member's personnel evaluation form (ref: Directive 215.00, Member Performance Evaluations) are encouraged to discuss the observation with the member and make an entry to the member's PDT.
  - 1.3. Supervisors who counsel a member or engage in other non-disciplinary corrective action, whether during normal operations; during an after action review in accordance with Directives 905.00, Non-Force After Action Reporting and 1010.00, Use of Force; or as part of another formal process such as a Supervisory Investigation, shall make an entry about the event and the corrective action undertaken in the member's PDT.
  - 1.4. At minimum, any entry made under Section 1.2 or 1.3 shall contain a brief synopsis of the incident, any relevant reference number (case number, CAD number, etc.), and an indication of how additional information may be obtained (e.g., contact the supervisor, review an after action, etc.).
  - 1.5. Upon notification that a sworn member's use of force has resulted in a finding of liability in a civil trial, the EIS Administrator shall make an entry reflecting the event in the member's PDT. In addition, the EIS Administrator shall generate an alert and send it to the sworn member's RU Manager for review.
  - 1.6. EIS automatically generates an e-mail to a member when a supervisor makes an entry in their PDT.
  - 1.7. Members may submit a response to PDT entries by writing a memorandum through their chain of command, to their RU Manager, and sending an electronic copy of the memorandum to the EIS Administrator.
    - 1.7.1. Upon receipt, the RU Manager will forward a copy of the memorandum to the EIS Administrator, retaining the original in theirfile.
    - 1.7.2. The EIS Administrator will enter the response in the sworn member's PDT upon receipt of the copy of the memorandum described in Section 1.7.1.
- 2. Review of Sworn Member Data upon Transfer:
  - 2.1. Supervisors who have sworn members new to their command, whether due to the

transfer of the supervisor or transfer of the sworn members, shall review the sworn members' EIS record and document this review occurred in the sworn members' PDT within thirty (30) days of the transfer.

- 2.1.1. This requirement applies to all temporary assignments (TDY, acting supervisor, etc.) that are in effect for more than thirty (30) continuous days, as well as a return to normal status from a temporary assignment (including all types of leave described in Directive 210.21, Leaves from Service) in effect for more than thirty (30) continuous days.
- 2.2. Prior to completing a sworn member's performance evaluation conducted in accordance with Directive 215.00, Member Performance Evaluations, or Human Resources Administrative Rule 9.02, Performance Management, supervisors will review the information available in EIS, including the various external data sources, PDT, and AMS.
  - 2.2.1. EIS contains aggregate and comparison data that may be useful in completing the evaluation and facilitating a career development conversation.
  - 2.2.2. After concluding the review, the supervisor shall document that the review occurred in the sworn member's PDT.
- 3. Performance Discussion Tracker and After Actions:
  - 3.1. Supervisors who address a sworn member's performance in the Recommendation and Critique Section of an After Action Report written in accordance with Directives 905.00, Non-Force After Action Reporting and 1010.00, Use of Force, shall place an entry in the sworn member's PDT. This requirement applies to the following events/incidents:
    - (a) Vehicle pursuits;
    - (b) Force events;
    - (c) Complaint of improper force;
    - (d) Complaint of injury or physical injury;
    - (e) All critical firearm discharge;
    - (f) Injury to suspect in custody;
    - (g) Police vehicle collision;
    - (h) Damage to or loss of city property; and
    - (i) Destruction of animal(s).
    - 3.1.1. This entry shall be made prior to forwarding the After Action Report to the next level of review unless the supervisor is unable to either personally make the entry or cause the entry to be made within the timelines established in Directives 905.00, Non-Force After Action Reporting and 1010.00, Use of Force. If the entry is not made prior to forwarding the After Action Report to the next level of review, the supervisor shall do the following prior to forwarding the After Action Report:
      - 3.1.1.1. Note the inability to make the entry in the After Action Report;
      - 3.1.1.2. E-mail either the EIS Administrator or a supervisor in the member's RU and request the entry be made; and
      - 3.1.1.3. Request in the After Action Report that the next level of review verify that

- the entry has been made in the sworn member's PDT.
- 3.1.2. Supervisors who receive an After Action Report where an EIS entry has been requested but not made under the procedure described in Section 3.1.1 shall document that the entry has been made in their After Action Report comments.
- 3.1.3. The entry shall include, at a minimum:
  - 3.1.3.1. The case number of the incident,
  - 3.1.3.2. The nature of the incident and, if applicable, the type of force used,
  - 3.1.3.3. Whether the incident was within policy,
  - 3.1.3.4. Any positive performance, and
  - 3.1.3.5. Any training deficiencies, policy deficiencies, or poor tactical decisions identified as well as any non-disciplinary corrective action taken to remedy them.
- 3.2. Pursuant to Directives 905.00, Non-Force After Action Reporting and 1010.00, Use of Force, all After Action Reports must be reviewed by the sworn member's chain of command. A manager (lieutenant or above) who is reviewing an After Action Report prepared by a subordinate shall make an EIS entry under the following circumstances:
  - 3.2.1. When the manager identifies a previously unidentified training deficiency, policy deficiency, or poor tactical decision made by the sworn member, the manager shall make an entry in the sworn member's PDT in accordance with this directive, in addition to ensuring the appropriate corrective action is provided to the sworn member.
  - 3.2.2. When the manager concludes the critique, analysis, or other commentary provided by any subordinate level of review is inadequate, inaccurate, or incomplete, the manager shall, if the matter is not referred to Internal Affairs (IA), provide the appropriate non-disciplinary corrective action and document it in the subordinate's PDT with:
    - 3.2.2.1. The case number of the incident,
    - 3.2.2.2. The nature of the incident,
    - 3.2.2.3. The nature of the deficiency, and
    - 3.2.2.4. The non-disciplinary corrective actiontaken.
  - 3.2.3. Entries made in accordance with Sections 3.2.1 and 3.2.2 may require the manager to make entries in multiple subordinates' PDTs.
  - 3.2.4. The manager shall make any PDT entry required by Section 3.2.1., and 3.2.2., prior to forwarding the investigation to the next level of review.
- 3.3. When a subordinate's performance on an After Action investigation or review exceeds the expectations of the organization, managers and supervisors shall make an entry to the subordinate's PDT documenting the performance.
- 4. Type I and Type II Alerts and Review Process.
  - 4.1. EIS Administrator Alert and Review Process Responsibilities:
    - 4.1.1. If a member has reached a threshold, the EIS Administrator shall generate an alert in the AMS.
      - 4.1.1.1. Every alert is evaluated by the EIS Administrator in accordance with the Professional Standards Division's (PSD) Standard Operating Procedure

- (SOP) 44 for individual sworn members and SOP 47 for groups and their respective supervisors.
- 4.1.1.2. If the EIS Administrator determines that the member's supervisor should review the alert, the EIS Administrator shall send the alert to the member's RU Manager with a request for the RU Manager to review the alert.
- 4.1.1.3. If the EIS Administrator does not request an RU Manager Review, the alert is sent to the PSD Lieutenant for review as outlined in Section 4.4.3.
- 4.1.1.4. Any decision made during this process, and the reason(s) for it, shall be documented in the "case notes" section of the alert.
- 4.1.2. The EIS Administrator shall review and process alerts as described in this section within thirty (30) days of EIS creating a system notification of the broken threshold. Exceptions to this requirement may be granted by the PSD Lieutenant for good cause. When the PSD Lieutenant receives a request for an exception, the request, and whether it was granted, the decision and the rationale for it, shall be documented in the "case notes" section of the alert.
  - 4.1.2.1. When an alert that was assigned for RU Manager review, as described in Section 4.2. of this directive is returned to PSD, the EIS Administrator shall review the RU Manager's response to the alert.
  - 4.1.2.2. If the documentation and process requirements of this directive have been fulfilled, the EIS Administrator shall close thealert.
  - 4.1.2.3. If the documentation and process requirements of this directive have not been fulfilled, the EIS Administrator shall return the alert to the RU Manager for correction.
  - 4.1.2.4. Any decision made during this process, and the reason(s) for it, shall be documented in the "case notes" section of the alert.
  - 4.1.2.5. The EIS Administrator shall review and process alerts, as described in this section, within fifteen (15) days of the alert being returned to PSD. Exceptions to this requirement may be granted by the PSD Lieutenant for good cause. Whether this request was granted, and the rationale for the decision, shall be documented in the "case notes" section of the alert.
- 4.2. RU Manager Process and Responsibilities:
  - 4.2.1. Within fifteen (15) days of an alert being assigned to an RU Manager by the EIS Administrator, they shall:
    - 4.2.1.1. Review the content of the alert and make a reasonable determination supported by the facts about whether to require a Supervisor Review as described in Section 4.3.
    - 4.2.1.2. Document the decision made, and the reason(s) for making it, in the "case notes" section of the alert.
  - 4.2.2. Within thirty (30) days of a Supervisor Review being returned to an RU Manager, they shall:
    - 4.2.2.1. Determine whether the Supervisor Review is complete and notify the supervisor if additional information is required.
    - 4.2.2.2. Review, approve, reject, and/or add Supervisory Actions as appropriate.
    - 4.2.2.3. The RU Manager shall not recommend an alert for closure until all Supervisory Actions have been completed.

- 4.2.2.4. Document the actions taken and the reason(s) for the actions in the case notes section of the alert.
- 4.2.3. Exceptions to the timelines required by Sections 4.2.1. and 4.2.2. may be granted by the PSD Commander for good cause. Whether this request was granted, and the rationale for the decision, shall be documented in the "case notes" section of the alert.
- 4.3. Supervisor Review Process and Responsibilities:
  - 4.3.1. When assigned a Supervisor Review, the supervisor will review the sworn member's performance by doing all of the following:
    - 4.3.1.1. Review of relevant information contained in the EIS data sources, the PDT, and the AMS;
    - 4.3.1.2. Review of relevant reports, IA case files, after actions, and other written documentation;
    - 4.3.1.3. Discuss the sworn member's performance with other supervisor(s); and
    - 4.3.1.4. Review other material as appropriate.
  - 4.3.2. At the conclusion of the review, the supervisor shall make a recommendation regarding Supervisory Action(s) to the RU Manager.
    - 4.3.2.1. The Supervisory Action(s) recommended should be based on the information gained during the Supervisor Review process.
    - 4.3.2.2. The supervisor shall document the Supervisory Action(s) recommended and the reason(s) for the Supervisory Action(s) in the "case notes" section of the alert.
  - 4.3.3. Supervisor Reviews shall be completed within thirty (30) days of the alert being assigned to the RU Manager by the EIS Administrator. Exceptions to this requirement may be granted by the PSD Commander for good cause. Whether this request was granted, and the rationale for the decision shall be documented in the "case notes" section of the alert.

# 4.4. Additional PSD Responsibilities:

- 4.4.1. The EIS Administrator is responsible for the following:
  - 4.4.1.1. Maintain EIS,
  - 4.4.1.2. Manage the AMS, including alerts and open reviews,
  - 4.4.1.3. Monitor access and usage of EIS,
  - 4.4.1.4. Assist other members with EIS, including AMS, and PDT, when requested,
  - 4.4.1.5. Solicit and provide feedback on the system and its usage to all Bureau members,
  - 4.4.1.6. Develop and provide on-going training to all Bureau members,
- 4.4.2. Semi-annually and as directed conduct data analysis of units and supervisors to identify and compare patterns of activity in accordance with established PSD SOPs.
  - 4.4.2.1. Semi-annually and as directed select a sample of employees to ensure the review of EIS as described in Section 2.1 of this directive has occurred,
  - 4.4.2.2. Produce an annual report describing EIS usage and trends,
  - 4.4.2.3. Develop and train sufficient alternate EIS Administrators to provide EIS service if the EIS Administrator is unavailable for an extended period,

- 4.4.2.4. Grant temporary additional access to EIS as described in Section 7, and
- 4.4.2.5. Ensure EIS administrative rights granted to Bureau members are consistent with current assignments.
- 4.4.3. The PSD Lieutenant Responsibilities:
  - 4.4.3.1. Ensure the EIS Annual Report and other documents described in Section 4.4.2., are produced in a timely manner.
  - 4.4.3.2. Review alerts recommended for closure by the EIS Administrator and either close or return the alerts to the EIS Administrator for additional work.
  - 4.4.3.3. Review requests for additional review time made by the EIS Administrator and either approving or rejecting the request as described in Section 4.12.
- 4.4.4. The PSD Commander is responsible for the following:
  - 4.4.4.1. The overall administration of the EIS Program, and
  - 4.4.4.2. Reviewing requests for additional review time made by RU Managers and either approving or rejecting the request as described in Sections 4.2.3. and 4.3.3.
- 5. Type III Alert and Review Process.
  - 5.1. Force Inspector ("the Inspector") Responsibilities:
    - 5.1.1. The Inspector shall conduct a quarterly analysis of force data in accordance with PSD SOP 47, Force Data Analysis at the Group and Supervisor Level.
    - 5.1.2. After consultation with RU Manager, if the Inspector has determined that statistically meaningful deviations from normative behavior places groups and their respective supervisors at risk of problematic trends, the Inspector shall notify the EIS Administrator via memorandum. The notification shall prompt the EIS Administrator to generate an alert to the RU Manager with specific instructions and/or recommendations from the Inspector.
    - 5.1.3. Upon notification from the EIS Administrator that the RU Manager has submitted a response to the Type III alert, the Inspector shall complete a review of the response within seven days.
      - 5.1.3.1. If the Inspector determines the RU Manager's response adequately addresses the alert, the Inspector shall document the response in the "case notes" section of the alert and notify the EIS Administrator that the alert can be closed.
      - 5.1.3.2. If the Inspector determines the RU Manager's response is insufficient, the Inspector shall direct the RU Manager to submit a revised response to adequately address the alert and document this direction in the "case notes" section of the alert.

# 5.2. EIS Administrator Responsibilities:

5.2.1. Within seven days of receiving a memorandum from the Inspector that a force use trend has been identified, the EIS Administrator shall generate an alert to the appropriate RU Manager.

- 5.2.2. The EIS Administrator shall notify the Inspector within seven days of receipt (in EIS) of the RU Manager's response to the alert.
- 5.2.3. The EIS Administrator shall close the alert when instructed by the Inspector to do so.

# 5.3. RU Manager Responsibilities:

- 5.3.1. Upon receipt of a Type III alert, the RU Manager shall complete a review of the Inspector's recommendations and provide a response within 30 days.
- 5.3.2. Document the actions taken and reasons for those actions in the "case notes" section of the alert. The RU Manager shall also make an entry into both the identified group's and the respective supervisor's pages of the AMS.
- 5.3.3. If the RU Manager's response is deemed insufficient by the Inspector, they shall submit a revised response to adequately address the recommendation(s) within 15 days of the alerts reassignment with EIS by the EIS Administrator.

# 5.4. Branch Assistant Chief Responsibilities:

5.4.1. If the Inspector and the RU Manager do not agree on a resolution, the Branch Assistant Chief shall consider the Inspector's memo and decide upon the appropriate resolution. The Branch Assistant Chief shall direct implementation of the resolution and the recording of Branch Assistant Chief's determination and the resolution in the "Case Notes."

# 6. EIS obtains data from the following outside sources:

- 6.1. Regional Justice Information Network (RegJIN): Arrests, Computer Aided Dispatch (CAD), Investigative Cases, Street Checks, Traumatic Incidents, and Uses of Force.
- 6.2. SAP: Employee Leave, Extra Employment, Leave Summary, Overtime, and Work Hour Summary.
- 6.3. Administrative Investigations Management (AIM): Commendations, Complaints.
- 6.4. Oregon e-Courts: Traffic Citations
- 6.5. Cite Search: Traffic Citations (electronic citations only)

# 7. EIS Data Access:

- 7.1. EIS administrative rights are controlled by the EIS Administrator under the direction of PSD Commander.
- 7.2. All Bureau members will be granted access to their own data in EIS.
- 7.3. A supervisor will be granted access to the EIS data of any subordinate members in their chain of command.
- 7.4. Temporary or additional access may be granted by submitting a written request to the

### EIS Administrator.

- 7.5. The following persons have access to the entire Bureau in EIS:
  - 7.5.1. The Chief of Police, Assistant Chiefs, and their adjutants,
  - 7.5.2. The PSD Commander, PSD Captain, PSD Lieutenant, Inspector, and EIS Administrators,
  - 7.5.3. The Training Division Manager and Field Training Evaluation Program Sergeant,
  - 7.5.4. Information Technology Division employees tasked with supporting EIS, and
  - 7.5.5. Other members as directed by the PSD Commander or PSD Lieutenant.

#### 8. EIS Data Retention:

- 8.1. Retention of EIS data pertain to entries in the PDT, as well as the AMS. Data from outside sources (RegJIN, SAP, etc.) are obtained each night, discarding prior data as new data are acquired.
- 8.2. EIS data will be retained for no less than ten years from the date of separation.
- 8.3. Questions regarding the retention of EIS data should be directed to the City Attorney's Office.

# **History:**

- Originating Directive Effective: 06/11/11
- Last Revision Signed: 04/15/19
  - o Effective Date: 05/15/19
- Next Review Date: 05/15/20

## 345.00, Employee Information System

#### (EIS) Refer:

- DIR 215.00, Sworn Represented Member Performance Evaluations
- DIR 940905.00, Non-Force After Action Reports Reporting
- DIR 1010.00, Use of Force
- Professional Standards Division Standard Operating Procedure 44, Employee
   Information System Alert Processing Guide
- Professional Standards Division Standard Operating Procedure 47, Force Data Analysis at the Group and Supervisor Level
- PPA Labor Agreement

### **Definitions:**

- Alert: Automatic A threshold break notification to that is assigned a case number by the Employee Information System Administrator that a sworn member has reached a preestablished threshold, or; a Responsibility Unit-(RU)-generated request to review a sworn member's performance and/or behavior; and/or a Force Inspector-generated request to review force trends at the RU level.
- Alert Management System (AMS): The AMS generates and processes electronic alerts. A system within EIS that serves as a repository for all case notes associated with any alert.
- Employee Information System (EIS): The EIS consists of a read-only database that collects information from external data sources, the Alert Management System, and the Performance Discussion Tracker.
- Performance Discussion Tracker (PDT): A system within EIS whichthat allows supervisors to record conversations about sworn member performance and/or behavior and any follow up on those conversations. Sworn members Members may also submit a response within the system.
- Supervisor: <u>aA</u> sworn Portland Police Bureau member at the rank of sergeant or above (or anyone acting in those capacities) and non-sworn personnel with oversight responsibility for other sworn members.
- Supervisory Action: A non-disciplinary process designed to give sworn members feedback on their performance and promote best practices. Supervisory actions may include coaching, commending, debriefing, monitoring, referring to the Employee Assistance Program, (EAP), requiring training, temporarily re-assigning, or some other form of non-disciplinary action.
- Supervisor Review: A review of information concerning a sworn member's performance and/or behavior.
- Threshold: Pre-programmed criteria established by the Chief of Police, including:
  - o Shift Force Ratio: a sworn member's force ratio is greater than or equal to three (3)

- times their shift's average ratio in the preceding six (6)months;
- o Force Ratio: a sworn member's force ratio is greater than or equal to 20% of his or hertheir arrests in the preceding six (6) months;
- o Force Count: a sworn member uses force three (3) or more times in the preceding thirty (30) days;
- Criminal Complaint: a member receives a complaint with an allegation of criminal misconduct;
- •—Complaint in Same Category: a member receives two (2) or more complaints with
- \_at least one (1) allegation in each complaint being in the same category (such as two (2) complaints that both have conduct allegations) for events in the preceding six months:
- o Complaint Count: a member receives three (3) or more complaints for events in the preceding six (6) months;
- Traumatic Incidents: a member experiences three (3) or more traumatic incidents in the preceding thirty (30) days;
- o Commendations: a member receives two (2) or more commendations for events in the preceding six (6) months.
- Threshold Break: An automatic notification to the EIS Administrator when a member reaches or exceeds a threshold.
- Type I Alert: An alert notification that pertains to a complaint- or commendation-related threshold break.
- Type II Alert: An alert notification that pertains to a force- or traumatic incident-related threshold break.
- Type III Alert: An alert notification that pertains to statistically meaningful deviations from normative behavior, with respect to groups and their respective supervisors, which the Force Inspector has determined places such groups and the respective supervisors at risk of problematic trends.

#### **Policy**:

- 1. The Employee Information System (EIS) is an application that compiles information from the Police Bureau and other data sources to enable a comprehensive review of a sworn member's work performance. The use of EIS benefits the Bureau and sworn members alike by facilitating professional growth through a feedback process that reinforces the Bureau's management and accountability systems, standards, and expectations.
- 2. It is the policy of the Bureau to encourage and develop personnel. EIS supports this goal by supplying information to supervisors that will allow them to better develop, manage, and support their sworn members.
- 3. EIS and the information developed therein shall not form the basis <u>for</u> disciplinary action but may be used for non-disciplinary notice purposes, such as development of work performance plans and letters of expectation. The reports from EIS may not be used by the

City for disciplinary, transfer or promotion decisions. However, if the underlying data that appears in EIS is maintained separately by the City and is simply reflected in EIS, nothing in this directive prevents the <a href="mailto:cityCity">city City</a> from making appropriate use of the underlying data in disciplinary, transfer, or promotion decisions.

4. The Alert Management System AMS and Performance Discussion Tracker PDT shall be treated as confidential material.

#### Procedure:

- 1. Performance Discussion Tracker (PDT)::
  - 1.1. The PDT allows supervisors to record discussions about a sworn-member's performance and behavior. Every entry to a sworn-member's PDT should be preceded by a discussion with the sworn-member.
  - 1.2. Supervisors who observe positive behavior or performance related to a sworn member's job duties as described in the sworn member's personnel evaluation form (ref: Directive 215.00, Sworn Represented Member Performance Evaluations) are encouraged to discuss the observation with the sworn member and make an entry to the sworn member's PDT.
  - 1.3. Supervisors who counsel a member or engage in other non-disciplinary corrective action, whether during normal operations; during an after action review in accordance with <a href="https://doi.org/10.00/">Directive 940</a>Directives 905.00, <a href="https://doi.org/10.00/">Non-Force</a> After Action <a href="https://doi.org/10.00/">Reports</a> Reporting and <a href="https://doi.org/10.00/">1010.00/</a>, <a href="https://doi.org/10.00/">Use of Force</a>; or as part of another formal process such as a <a href="https://doi.org/10.00/">Service</a> Improvement Opportunity</a> Supervisory <a href="https://doi.org/10.00/">Investigation</a>, shall make an entry about the event and the corrective action undertaken in the <a href="https://doi.org/10.00/">Sworn</a> member's PDT.
  - 1.4. At minimum, any entry made under Section 1.2 or 1.3 shall contain a brief synopsis of the incident, any relevant reference number (case number, CAD number, etc.), and an indication of how additional information may be obtained (e.g., contact the supervisor, review an after action, etc.).
  - 1.5. Upon notification that a sworn member's use of force has resulted in a finding of liability in a civil trial, the EIS Administrator shall make an entry reflecting the event in the member's PDT. In addition, the EIS Administrator shall generate an alert and send it to the sworn member's RU Manager for review.
  - 1.6. EIS automatically generates an e-mail to a sworn member when a supervisor makes an entry in their PDT.
  - 1.7. Sworn members Members may submit a response to PDT entries by writing a memorandum through their chain of command, to their RU Manager, and sending an electronic copy of the memorandum to the EIS Administrator.
    - 1.7.1. Upon receipt, the RU Manager will forward a copy of the memorandum to the EIS Administrator, retaining the original in their file.
    - 1.7.2. The EIS Administrator will enter the response in the sworn member's PDT

upon receipt of the copy of the memorandum described in Section 1.7.1.

- 2. Review of Sworn Member Data Uponupon Transfer:
  - 2.1. Supervisors who have sworn members new to their command, whether due to the transfer of the supervisor or transfer of the sworn members, shall review the sworn members' Employee Information System (EIS) record and document this review occurred in the sworn members' Performance Discussion Tracker (PDT) within thirty (30) days of the transfer.
    - 2.1.1. This requirement applies to all temporary assignments (TDY, acting supervisor, etc.) that are in-effect for more than thirty (30) continuous days, as well as a return to normal status from a temporary assignment (including all types of leave described in Directive 210.21, Leaves of Service) in effect for more than thirty (30) continuous days.
    - 2.1.2. This requirement also applies to all transfers that occur within a Responsibility Unit (RU), such as an officer changing detail sergeants while remaining on the same shift.
  - 2.2. Prior to completing a sworn member's performance evaluation conducted in accordance with Directive 215.00, <a href="Sworn Represented">Sworn Represented</a> Member Performance Evaluations, or— Human Resources Administrative Rule 9.02, Performance Management, supervisors will review the information available in EIS, including the various external data sources, PDT, and AMS.
    - 2.2.1. EIS contains aggregate and comparison data that may be useful in completing the evaluation and facilitating a career development conversation.
    - 2.2.2. After concluding the review, the supervisor shall document that the review occurred in the sworn member's PDT.
- 3. Performance Discussion Tracker (PDT) and After Actions:
  - 3.1. Supervisors who address a sworn member's performance in the Recommendation and Critique Section of an After Action Report written in accordance with Directive 940 Directives 905.00, Non-Force After Action Reports Reporting and 1010.00, Use of Force, shall place an entry in the sworn member's PDT. This requirement does not applyapplies to After Action Reports written pursuant to Sections 1.6, 1.7. 1.11, 1.12, and 1.14, as written in Directive 940.00, After Action Reports. the following events/incidents:
    - (a) Vehicle pursuits;
    - (b) Force events;
    - (c) Complaint of improper force;
    - (d) Complaint of injury or physical injury;
    - (e) All critical firearm discharge;
    - (f) Injury to suspect in custody;
    - (g) Police vehicle collision;
    - (h) Damage to or loss of city property; and
    - (i) Destruction of animal(s).
    - 3.1.1. This entry shall be made prior to forwarding the After Action Report to the next

level of review unless the supervisor is unable to either personally make the entry or cause the entry to be made within the timelines established in Directive 940Directives 905.00, Non-Force After Action Reports. Reporting and 1010.00, Use of Force. If the entry is not made prior to forwarding the After Action Report to the next level of review, the supervisor shall do the following prior to forwarding the After Action Report:

- 3.1.1.1. Note the inability to make the entry in the After Action Report;
- 3.1.1.2. E-mail either the EIS Administrator or a supervisor in the member's RU and request the entry be made; and
- 3.1.1.3. Request in the After Action Report that the next level of review verify that the entry has been made in the sworn member's PDT.
- 3.1.2. Supervisors who receive an After Action Report where an EIS entry has been requested but not made under the procedure described in Section 3.1.1 shall document that the entry has been made in their After Action Report comments.
- 3.1.3. The entry shall include, at a minimum:
  - 3.1.3.1. The case number of the incident,
  - 3.1.3.2. The nature of the incident and, if applicable, the type of force used,
  - 3.1.3.3. Whether the incident was within policy,
  - 3.1.3.4. Any positive performance, and
  - 3.1.3.5. Any training deficiencies, policy deficiencies, or poor tactical decisions identified as well as any non-disciplinary corrective action taken to remedy them.
- 3.2. Pursuant to <u>Directive 940 Directives 905.00</u>, <u>Non-Force</u> After Action <u>ReportsReporting</u> and 1010.00, <u>Use of Force</u>, all After Action Reports must be reviewed by the sworn member's chain of command. A manager (lieutenant or above) who is reviewing an After Action Report prepared by a subordinate shall make an EIS entry under the following circumstances:
  - 3.2.1. When the manager identifies a previously unidentified training deficiency, policy deficiency, or poor tactical decision made by the sworn member, the manager shall make an entry in the sworn member's PDT in accordance with this <a href="Directivedirective">Directivedirective</a>, in addition to ensuring the appropriate corrective action is provided to the sworn member.
  - 3.2.2. When the manager concludes the critique, analysis, or other commentary provided by any subordinate level of review is inadequate, inaccurate, or incomplete, the manager shall, if the matter is not referred to the Internal Affairs Division, (IA), provide the appropriate non-disciplinary corrective action and document it in the subordinate's PDT with:
    - 3.2.2.1. The case number of the incident.
    - 3.2.2.2. The nature of the incident,
    - 3.2.2.3. The nature of the deficiency, and
    - 3.2.2.4. The non-disciplinary corrective actiontaken.
  - 3.2.3. Entries made in accordance with Sections 3.2.1 and 3.2.2 may require the manager to make entries in multiple subordinates' PDTs.
  - 3.2.4. The manager shall make any PDT entry required by Section 3.2.1., and 3.2.2., prior to forwarding the investigation to the next level of review.

- 3.3. When a subordinate's performance on an After Action investigation or review exceeds the expectations of the organization, managers and supervisors shall make an entry to the subordinate's PDT documenting the performance.
- 4. Type I and Type II Alerts and Review Process.
  - 3.4.4.1. EIS Administrator Alert and Review Process Responsibilities:
    - 3.4.1.4.1.1. If a member has reached a threshold, the EIS Administrator shall generate an alert is automatically generated in the Alert Management System (AMS).
      - 3.4.1.1.4.1.1.1. Every alert is evaluated by the EIS Administrator in accordance with the Professional Standards Division's (PSD) Standard Operating Procedure (SOP) 44 for individual sworn members and SOP 47 for groups and their respective supervisors.
      - 3.4.1.2.4.1.1.2. If the EIS Administrator determines that the member's supervisor should review the alert, the EIS Administrator shall send the alert to the member's RU Manager with a request for the RU Manager to review the alert.
      - 3.4.1.3. If the EIS Administrator does not request an RU Manager Review, the alert is sent to the Professional Standards Division (PSD) Lieutenant for review as outlined in Section 7.24.4.3.
      - 3.4.1.4.4.1.1.4. Any decision made during this process, and the reason(s) for it, shall be documented in the "case notes" section of the alert.
    - 3.4.2.4.1.2. The EIS Administrator shall review and process alerts as described in this section within thirty (30) days of EIS creating a system notification of the broken threshold. Exceptions to this requirement may be granted by the PSD Lieutenant for good cause. When the PSD Lieutenant receives a request for an exception, the request, and whether it was granted, the decision and the rationale for it, shall be documented in the "case notes" section of the alert.
      - 3.4.2.1.4.1.2.1. When an alert that was assigned for RU Manager review, as described in Section 34.2. of this directive is returned to PSD, the EIS Administrator shall review the RU Manager's response to the alert.
      - 3.4.2.2.4.1.2.2. If the documentation and process requirements of this directive have been fulfilled, the EIS Administrator shall close the alert.
      - 3.4.2.3. If the documentation and process requirements of this directive have not been fulfilled, the EIS Administrator shall return the alert to the RU Manager for correction.
      - 3.4.2.4.4.1.2.4. Any decision made during this process, and the reason(s) for it, shall be documented in the "case notes" section of the alert.
      - 3.4.2.5.4.1.2.5. The EIS Administrator shall review and process alerts, as described in this section, within fifteen (15) days of EIS creating a system notification of the broken threshold.the alert being returned to PSD. Exceptions to this requirement may be granted by the PSD Lieutenant for good cause. Whether this request was granted, and the rationale for the decision, shall be documented in the "case notes" section of the alert.

- 3.5.4.2. Responsibility UnitRU Manager Process and Responsibilities:
  - 3.5.1.4.2.1. Within fifteen (15) days of an alert being assigned to an RU Manager by the EIS Administrator, they shall:
    - 3.5.1.1.4.2.1.1. Review the content of the alert and make a reasonable determination supported by the facts about whether to require a Supervisor Review as described in Section 4.3.
    - 3.5.1.2.4.2.1.2. Document the decision made, and the reason(s) for making it, in the "case notes" section of the alert.
  - 3.5.2.4.2.2. Within thirty (30) days of a Supervisor Review being returned to an RU Manager, they shall:
    - 3.5.2.1.4.2.2.1. Determine whether the Supervisor Review is complete and notify the supervisor if additional information is required.
    - 3.5.2.2.4.2.2. Review, approve, reject, and/or add Supervisory Actions as appropriate.
    - 3.5.2.3.4.2.2.3. The RU Manager shall not recommend an alert for closure until all Supervisory Actions have been completed.
    - 3.5.2.4.4.2.2.4. Document the actions taken and the reason(s) for the actions in the case notes section of the alert.
  - be granted by the PSD <u>CaptainCommander</u> for good cause. Whether this request was granted, and the rationale for the decision, shall be documented in the "case notes" section of the alert.
- 3.6.4.3. Supervisor Review Process and Responsibilities:
  - 3.6.1.4.3.1. When assigned a Supervisor Review, the supervisor will review the sworn member's performance by doing all of the following:
    - 3.6.1.1.4.3.1.1. Review of relevant information contained in the EIS data sources, the PDT, and the AMS;
    - 3.6.1.2.4.3.1.2. Review of relevant reports, <u>IADIA</u> case files, after actions, and other written documentation;
    - 3.6.1.3.4.3.1.3. Discuss the sworn member's performance with other supervisor(s); and
    - 3.6.1.4.4.3.1.4. Review other material as appropriate.
  - 3.6.2.4.3.2. At the conclusion of the review, the supervisor shall make a recommendation regarding Supervisory Action(s) to the RU Manager.
    - 3.6.2.1.4.3.2.1. The Supervisory Action(s) recommended should be based on the information gained during the Supervisor Review process.
    - 3.6.2.2.4.3.2.2. The supervisor shall document the Supervisory Action(s) recommended and the reason(s) for the Supervisory Action(s) in the "case notes" section of the alert.
  - 3.6.3.4.3.3. Supervisor Reviews shall be completed within thirty (30) days of the

alert being assigned to the RU Manager by the EIS Administrator. Exceptions to this requirement may be granted by the PSD <u>CaptainCommander</u> for good cause. Whether this request was granted, and the rationale for the decision shall be documented in the "case notes" section of the alert.

```
3.7.4.4. Professional Standards Division (Additional PSD) Responsibilities:
   3.7.1.4.4.1. The EIS Administrator is responsible for the following:
       3.7.1.1.4.4.1.1. Maintain EIS,
       3.7.1.2.4.4.1.2. Manage the AMS, including alerts and open reviews,
       3.7.1.3.4.4.1.3. Monitor access and usage of EIS,
       3.7.1.4.4.4.1.4. Assist other members with EIS, including AMS, and PDT, when
               requested,
       3.7.1.5.4.4.1.5. Solicit and provide feedback on the system and its usage to all
               Bureau members,
       3.7.1.6.4.4.1.6. Develop and provide on-going training to all Bureau members,
    3.7.2. Semiannually Semi-annually and as directed conduct data analysis of units and
            supervisors to
   3.7.3.4.4.2. identify and compare patterns of activity in accordance with established
          PSD Standard Operating Procedures SOPs,
       3.7.3.1.4.4.2.1. Semiannually Semi-annually and as directed select a sample of
               employees to ensure the review of EIS as described in Section 2.1 of this
               Directive directive has occurred,
       <del>3.7.3.2.</del>4.4.2.2.
                         Produce an annual report describing EIS usage and trends,
                         Develop and train sufficient alternate EIS Administrators to
       <del>3.7.3.3.</del>4.4.2.3.
               provide EIS service if the EIS Administrator is unavailable for an extended
               period,
       <del>3.7.3.4.</del>4.4.2.4.
                         Grant temporary additional access to EIS as described in Section
               97, and
       <del>3.7.3.5.</del>4.4.2.5.
                         Ensure EIS administrative rights granted to Bureau members
               are consistent with current assignments.
                  The PSD Lieutenant is responsible for the following Responsibilities:
   <del>3.7.4.</del>4.4.3.
       3.7.4.1.4.4.3.1. Ensuring Ensure the EIS Annual Report and other documents
               described in Section 7.1,4.4.2., are produced in a timely manner.
       3.7.4.2.4.4.3.2. Reviewing Review alerts recommended for closure by the EIS
               Administrator and either close or return the alerts to the EIS
               Administrator for additional work.
       3.7.4.3.4.4.3.3. <u>ReviewingReview</u> requests for additional review time made by
               the EIS Administrator and either approving or rejecting the request as
               described in Section 4.12.
   3.7.5.4.4.4. The PSD CaptainCommander is responsible for the following:
       3.7.5.1.4.4.4.1. The overall administration of the EIS Program, and
       3.7.5.2.4.4.4.2. Reviewing requests for additional review time made by RU
               Managers and either approving or rejecting the request as described in
               Sections 54.2.3. and 64.3.3.
```

- 5. Type III Alert and Review Process.
  - 5.1. Force Inspector ("the Inspector") Responsibilities:
    - 5.1.1. The Inspector shall conduct a quarterly analysis of force data in accordance with PSD SOP 47, Force Data Analysis at the Group and Supervisor Level.
    - 5.1.2. After consultation with RU Manager, if the Inspector has determined that statistically meaningful deviations from normative behavior places groups and their respective supervisors at risk of problematic trends, the Inspector shall notify the EIS Administrator via memorandum. The notification shall prompt the EIS Administrator to generate an alert to the RU Manager with specific instructions and/or recommendations from the Inspector.
    - 5.1.3. Upon notification from the EIS Administrator that the RU Manager has submitted a response to the Type III alert, the Inspector shall complete a review of the response within seven days.
      - 5.1.3.1. If the Inspector determines the RU Manager's response adequately addresses the alert, the Inspector shall document the response in the "case notes" section of the alert and notify the EIS Administrator that the alert can be closed.
      - 5.1.3.2. If the Inspector determines the RU Manager's response is insufficient, the
        Inspector shall direct the RU Manager to submit a revised response to
        adequately address the alert and document this direction in the "case notes" section of the alert.

# 5.2. EIS Administrator Responsibilities:

- 5.2.1. Within seven days of receiving a memorandum from the Inspector that a force use trend has been identified, the EIS Administrator shall generate an alert to the appropriate RU Manager.
- 5.2.2. The EIS Administrator shall notify the Inspector within seven days of receipt (in EIS) of the RU Manager's response to the alert.
- 5.2.3. The EIS Administrator shall close the alert when instructed by the Inspector to do so.

# 5.3. RU Manager Responsibilities:

- 5.3.1. Upon receipt of a Type III alert, the RU Manager shall complete a review of the Inspector's recommendations and provide a response within 30 days.
- 5.3.2. Document the actions taken and reasons for those actions in the "case notes" section of the alert. The RU Manager shall also make an entry into both the identified group's and the respective supervisor's pages of the AMS.
- 5.3.3. If the RU Manager's response is deemed insufficient by the Inspector, they shall submit a revised response to adequately address the recommendation(s) within 15 days of the alerts reassignment with EIS by the EIS Administrator.

## 5.4. Branch Assistant Chief Responsibilities:

5.4.1. If the Inspector and the RU Manager do not agree on a resolution, the Branch

Assistant Chief shall consider the Inspector's memo and decide upon the appropriate resolution. The Branch Assistant Chief shall direct implementation of the resolution and the recording of Branch Assistant Chief's determination and the resolution in the "Case Notes."

- 4.<u>6.</u>EIS obtains data from the following outside sources:
  - 4.1.6.1. Regional Justice Information Network (RegJIN): Arrests, Computer Aided Dispatch (CAD), Investigative Cases, Street Checks, Traumatic Incidents, and Uses of Force.
  - 4.2.6.2. SAP: Employee Leave, Extra Employment, Leave Summary, Overtime, and Work Hour Summary.
  - 4.3.6.3. Administrative Investigations Management (AIM): Commendations, Complaints.
  - 4.4.6.4. Oregon e-Courts: Traffic Citations
  - 4.5.6.5. Cite Search: Traffic Citations (electronic citations only)
- 5.7. Employee Information System (EIS) Data Access:
  - 5.1.7.1. EIS administrative rights are controlled by the EIS Administrator under the direction of PSD CaptainCommander.
  - 5.2.7.2. All Bureau members will be granted access to their own data in EIS.
  - 5.3.7.3. A supervisor will be granted access to the EIS data of any subordinate members in their chain of command.
  - 5.4.7.4. Temporary or additional access may be granted by submitting a written request to the EIS Administrator.
  - 5.5.7.5. The following persons have access to the entire Bureau in EIS:
    - 5.5.1.7.5.1. The Chief of Police, Assistant Chiefs, and their adjutants,
    - 5.5.2.7.5.2. The PSD Commander, PSD Captain, PSD Lieutenant, Inspector, and EIS Administrators,
    - 5.5.3.7.5.3. The Training Division Manager and Field Training Evaluation Program Sergeant,
    - 5.5.4.7.5.4. Information Technology Division employees tasked with supporting EIS, and
    - 5.5.5.7.5.5. Other members as directed by the PSD Captain Commander or PSD Lieutenant.
- 6.8. Employee Information System (EIS) Data Retention:
  - 6.1.8.1. Retention of EIS data pertain to entries in the PDT, as well as the AMS. Data from outside sources (RegJIN, SAP, etc.) are obtained each night, discarding prior data as new data are acquired.

- 6.2.8.2. EIS data will be retained for no less than ten (10) years from the date of separation.
- 6.3.8.3. Questions regarding the retention of EIS data should be directed to the City Attorney's Office.

#1 1st Universal Review: 2/15/18-3/17/18

COMPLETE

Collector: Web Link 1 (Web Link)

 Started:
 Tuesday, March 13, 2018 12:52:02 PM

 Last Modified:
 Tuesday, March 13, 2018 12:53:19 PM

**Time Spent:** 00:01:16

## Page 1

### Q1 Please provide feedback for this directive

Comments on Copwatching and Employee Information System Directives, March 2018

To Chief Outlaw, Capt. Bell, Lieutenant Morgan, PPB Policy Analysts, Compliance Officer/Community Liaison Team, Community Oversight Advisory Board staff, US Dept. of Justice, Citizen Review Committee and the Portland Police Bureau:

Below are our comments on some of the Directives posted for review in February 2018 (at <a href="http://www.portlandoregon.gov/police/59757">http://www.portlandoregon.gov/police/59757</a>). We turned in our comments on the Training Directive before the March 2 deadline, and will send our comments on Crowd Control separately as they are quite extensive.

Portland Copwatch (PCW) spoke directly with Chief Outlaw about the timeline issue for examining policies. We are glad to see that the "Directives Directive" 010.00 now gives 30 days to comment on the proposed changes from the Bureau. However, this comes at the expense of cutting the first comment period down from 30 to 15 days. For groups like ours, the Citizen Review Committee and others who only meet once a month it is still a very short time to examine lengthy policies in a meaningful way. We remind the Bureau that once the Portland Committee on Community Engaged Policing (PCCEP) is up and running, even if they meet twice a month it is unlikely they can meet 15-day turnarounds, much less 30 day ones.

PCW continues to believe the Bureau should add letters to section headings (Definitions, Policy, Procedure) to avoid having multiple sections with the same numbers, and return to its earlier practice of numbering each Definition, for easier cross-referencing.

Our comments below refer to the Procedure section unless otherwise noted.

#### DIRECTIVE 345.00 EMPLOYEE INFORMATION SYSTEM

When the Directive on the Employee Information System (EIS) was last published in April 2015, it had been extensively reorganized and rewritten. The current version that has been posted underwent further reorganizing and rewriting, making comparisons very complex. Entire sections were moved around, and some of them were re-named. Many changes were minor and not worth noting, but some changes we recommended were not made and other changes are of concern.

For example, we asked that the Bureau make it clear that Supervisory review of Use of Force incidents does not replace the need for Independent Police Review/Internal Affairs investigations (Section 3, previously Section 5: "Performance Discussion Tracker and After Actions"). Here is what we wrote about the language in that section:

"This is related to the Use of Force investigations required by the DOJ Agreement. We've noted elsewhere that we believe civilian investigators from IPR should be sent to the scene of Use of Force incidents to conduct such investigations (or, at minimum, to observe the procedures as at Deadly Force incidents). The Directive indicates that a Supervisor can record 'training deficiencies, policy deficiencies or poor tactical decisions' [3.1.2.5] and non-disciplinary corrective action taken [3.2.2]. It seems this entire process bypasses IPR and could lead to an officer claiming double jeopardy if a community member files a complaint later." This concern was recently affirmed as the Citizen Review Committee found an Internal Affairs investigation hinted that a supervisory investigation finding

#### Directive 345.00 Feedback

no misconduct should mean the officers were within policy, even though IA's job was to conduct an independent investigation.

While the Directive calls for annual reports to be prepared [7.1.9], we noted DOJ Agreement paragraph 158 calls for all reports related to the Agreement to be made public. As the community has been promised repeatedly since at least the year 2000 that the EIS (and the previous Early Warning System) are working just fine, releasing such a report could help clarify whether the system is finally operating as promised and desired. A previous section (8) extensively stating that EIS documentation is not public record has been cut and mostly replaced by a mention in Policy Section 4. PCW continues to believe cumulative data that do not identify individual officers should not only be considered non-confidential but should be willingly and regularly shared with the public.

One of the most concerning changes that was made is also related to the After Action Reports. Section 3.1 says Supervisors do not have to place entries into the Performance Discussion Tracker if After Action Reports are created (a) where incident operation orders are written (old Dir. 940/1.12) -- implying crowd control is not subject to review, (b) in cases of officer injury (old Dir. 940/1.7) -- implying the officer's behavior is excused if they are injured, or (c) for major incidents (old Dir. 940/1.6)-- implying no corrective action in deadly force situations.

In our previous comments, we wondered why the Supervisor of an officer transferring into his/her unit would be given 30 days to look at that officer's Performance history in the EIS (old Section 1.1, current Section 2.1). It seems, we said, that Supervisor should know that information before the transfer takes place. A few new subsections were added clarifying which employees are considered transfers, but the timeline for supervisory review remains at a lengthy 30 days.

We made other comments in August 2014, repeated in 2015, which have not been dealt with, updated here:

- --There is still no definition for "traumatic incidents" (itself in the definition of "Threshold"). While the Threshold definition now outlines specific "triggers" such as three uses of force in 30 days, it still does not say what constitutes a "traumatic incident." If it means officer involved shootings, it is highly unlikely any officer will meet the threshold of three traumatic incidents in 30 days (at least we hope not). We note that the term was changed in Directive 416.00 to "critical incident," but the definition that in that policy is still vague. It states: "Critical Incident: An atypically traumatic event that may cause physical, emotional, and/or psychological injury or harm." What is "atypical"? Does the harm include harm to the civilian or only to the officer? This is a good start but still needs a lot of clarification.
- --It is still not clear what rank the EIS manager holds, which is important given the extraordinary authority he/she is given in Section 7 (formerly Section 6), though it is noted that the EIS administrator's decisions are overseen by the Professional Standards Division Captain in 9.1;

and

--Serious issues such as DUIIs, sustained complaints and use of deadly force will apparently, misguidedly be purged. This is no longer clear as the guideline to get rid of data after 5 years disappeared (former section 7.6) and the new data retention section (10) doesn't give a timeline except for 10 years after an employee leaves the PPB. It is confusing, and concerning, that new data is imported "nightly," leading to purging of old data (10.1). While this provision was in the previous iteration, without a timeline for retention in general it appears some information will be lost rather guickly.

PCW did find a few paragraphs that seem to be in line with the DOJ Agreement which were added, including that the EIS administrator must send alerts of civil liability to officers' supervisor (1.5), review triggered alerts within 30 days (4.1.5), and process alerts sent back from supervisors to Processional Standards within 15 days (4.2.4).

One final and minor observation: The definition of "Intervention" was rewritten and re-named as "Supervisory Action." Perhaps "Intervention" sounded too much like it only applied to officers with substance abuse issues.

#### CONCLUSION

Portland Copwatch appreciates the ability to comment but continues to believe that more progress can be made if there is more of a

# Directive 345.00 Feedback

dialogue rather than a one-way filtered system of comments going to the police. Since other people's comments are not published until the stage when community input is no longer solicited, the Bureau gets to pick and choose what it thinks are the most important or relevant changes. Community members seeing each others' ideas can lead to more of a sense of what matters outside the four walls of Central Precinct. One day, perhaps such discussions will take place at PCCEP meetings, but that process still seems months away from development.

Thank you for the opportunity to comment

Portland Copwatch

**Q2** Contact Information (optional)

Name Portland Copwatch

Email Address copwatch@portlandcopwatch.org

**#1** 2nd Universal Review: 9/15/18-10/15/18

COMPLETE

Collector: Web Link 1 (Web Link)

Started:Wednesday, September 26, 2018 2:33:02 PMLast Modified:Wednesday, September 26, 2018 2:33:53 PM

**Time Spent:** 00:00:51

## Page 1

### Q1 Please provide feedback for this directive

Comments on Camping, Trespass Agreement and Employee Information System Directives, September 2018

To Chief Outlaw, Capt. Bell, Lieutenant Morgan, PPB Policy Analysts, Compliance Officer/Community Liaison Team, Community Oversight Advisory Board staff, US Dept. of Justice, Independent Police Review, Citizen Review Committee and the Portland Police Bureau:

Below are comments from Portland Copwatch (PCW) on the Directives posted for review in mid-September 2018 (at http://www.portlandoregon.gov/police/59757). While we are glad to have been given 30 days to review the Employee Information System Directive, we are including comments in the shorter 15 day window since we had to use that truncated timeline to examine the other two posted policies anyway. We still believe the timeline should be a minimum of 30 days each time a Directive is posted for comment, and as noted in our last feedback, those deadlines should be flexible based on factors such as holidays.

A general comment along ones we have made before: Our suggestions on how to make improvements to these policies does not mean we agree with the underlying premises that allow police to, for instance, take houseless people's belongings when those people have nowhere else to go. As long as those underlying laws and policies are in place, we hope to make police aware of the possible harms that come with enforcing them, and find ways to mitigate that harm.

PCW continues to believe the Bureau should add letters to the Definitions, Policy, Procedure and other Sections to avoid having multiple areas with the same numbers (ie, multiple items called "Section 1"), and return to its earlier practice of numbering each Definition, as is done in City Code and State law.

The two Directives with short turnaround time were last released in 2014 and 2015. It is interesting that our then-comments were directed to Chief Mike Reese, and that we are on our fifth (or perhaps sixth, if you count when Assistant Chief Davis filled in while Chief Marshman was under investigation) Chief since then.\*

Our comments below refer to the Procedure section unless otherwise noted.

### DIRECTIVE 345.00 EMPLOYEE INFORMATION SYSTEM (previous comments February 2018)

There are very few substantive changes being proposed to the Employee Information System (EIS) Directive, despite this tracking system's importance to flagging possible problem officers and the extensive comments PCW made in February. Most of the changes are technical (because After Action Reports are now included in Directive 1010 on Use of Force, rather than 940.00) and clerical. In that department, PCW strongly recommends that the Bureau not use acronyms by themselves in the Section headings (like "PDT" in Section 3, "PSD" in Section 7 and "EIS" in Section 9) as the alphabet soup is confusing enough without having to flip around to see what those mean.

Substantively, we continue to be concerned that Supervisory review of Use of Force incidents are able to be used to undermine full

#### Directive 345.00 Feedback

administrative investigations of alleged misconduct. We cited a case in which "the Citizen Review Committee found an Internal Affairs investigation hinted that a Supervisory investigation finding no misconduct should mean the officers were within policy, even though IA's iob was to conduct an independent investigation."

Our concern remains mostly focused on Section 3, "Performance Discussion Tracker and After Actions." As we wrote before, we have long objected to the idea that Sergeants are sent out to investigate their officers' Use of Force since a person who feels they have been mistreated will be reluctant to talk to police, and perhaps even intimidated. We continue to believe civilian investigators from the Independent Police Review should be opening such on-scene investigations (or, we wrote, "at minimum, to observe the procedures as [they do] at Deadly Force incidents)."

The proposed new language makes the overall timeline of the data entry into the EIS more confusing. Section 3.1 directs Supervisors to make an entry in the Performance Discussion Tracker (PDT) following force events (3.1b) and complaints of improper force (3.1c) or complaints of injury (3.1d). This underscores our concern that the person subjected to force might be looked at as putting the officer in double jeopardy of having their force investigated twice-- once by the Sergeant and once by IA. Similarly, it is confusing that Supervisors might have already taken corrective action prior to a complaint being filed and investigated (3.2.2.4) and made note of "training deficiencies, policy deficiencies or poor tactical decisions" (3.1.3.5). It must be acknowledged that preliminary comments made after the on-scene investigation do not preclude further comments being made after a full investigation.

A good development, though, is that Section 3.1 used to have a list of reasons Supervisors did \_not\_ have to make entries in the PDT. Those included (a) where incident operation orders are written -- implying crowd control was not subject to review, (b) in cases of officer injury-- implying the officer's behavior is excused if they are injured, or (c) for major incidents-- implying no corrective action in deadly force situations. That said, the new list's description of "Force events" should be very clear whether they mean deadly force and crowd control, since those uses of force (inappropriately) get tracked separately by the Force Inspector. It should also be clear if the complaint of injury includes an officer being injured.

We also noted that we have not seen (or been informed about) the publication of the annual reports described in Section 7.1.9. The DOJ Agreement (paragraph 158) says all reports related to the Settlement Agreement should be public. Then again, it also calls for the PPB to produce annual reports and hold public forums on those, and the only year we know of where that happened (2016) we were not alerted to the reports being published or the times and locations of the forums.\*\* We are not asking for individual officers to be named (Policy Section 4 makes it clear that is confidential), but rather for a general report on how often officers cross the various thresholds and whether they are being counseled as envisioned by the Agreement. Right now there are occasional data on such matters in the Compliance Officer / Community Liaison's reports, which is not the same as the Bureau publishing its own. As we wrote earlier, "PCW continues to believe cumulative data that do not identify individual officers should not only be considered non-confidential but should be willingly and regularly shared with the public."

In previous sets of comments, we wondered why the Supervisor of an officer transferring into his/her unit would be given 30 days to look at that officer's Performance history in the EIS (Section 2.1). It seems, we said, the Supervisor should know that information before the transfer takes place.

We made other comments in August 2014, repeated in 2015 and in February, which have not been dealt with, updated here:

- --There is still no definition for "traumatic incidents" (itself in the definition of "Threshold"). While the Threshold definition outlines specific "triggers" such as three uses of force in 30 days, it still does not say what constitutes a "traumatic incident." If it means officer involved shootings, it is highly unlikely any officer will meet the threshold of three traumatic incidents in 30 days (at least we hope not). We noted that the term was changed in Directive 416.00 to "critical incident," but the definition in that policy is still vague. It states: "Critical Incident: An atypically traumatic event that may cause physical, emotional, and/or psychological injury or harm." What is "atypical"? Does the harm include harm to the civilian or only to the officer? This is a good start but still needs a lot of clarification.
- --It is still not clear what rank the EIS manager holds, which is important given the extraordinary authority he/she is given in Section 7.1, though it is noted that the EIS administrator's decisions are overseen to some extent by the Professional Standards Division Lieutenant in 7.2 and the PSD Captain in 7.3 and 9.1;

### Directive 345.00 Feedback

and

--Serious issues such as DUIIs, sustained complaints and use of deadly force will apparently, misguidedly be purged. It is confusing, and concerning, that new data is imported "nightly," leading to purging of old data (10.1). Thus it is unclear what data are to be retained for 10 years under Section 10.2, since it seems much of the older data will get pushed out by new entries.

#### CONCLUSION

Portland Copwatch continues to appreciate the Bureau asking for community input, but still thinks having more interactive discussions could lead to a set of policies even more likely to ensure Portland has a Bureau free from corruption, brutality and racism. This is our first set of comments to be submitted following the naming of members for the Portland Committee for Community Engaged Policing (PCCEP). Nonetheless, the PCCEP is not expected to have its first public meeting until November and it is highly unlikely they will be ready to lead community discussions on Directives for a few months after that.

Thank you for the opportunity to comment

**Portland Copwatch** 

- \* The five Chiefs since Reese are O'Dea, Henderson, Marshman, Uehara, and Outlaw.
- \*\* PCW recently found the "combined 2015/2016" report signed by Chief O'Dea on the PPB's website, with a publication date of August 15, 2018. https://www.portlandoregon.gov/police/article/695363

# **Q2** Contact Information (optional)

Name

**Portland Copwatch** 

**Email Address** 

copwatch@portlandcopwatch.org