MARICOPA COUNTY SHERIFF'S OFFICE POLICY AND PROCEDURES

Subject	Policy Number
EARLY IDENTIFICATION SYSTEM (EIS)	**GH-5**
	Effective Date **03-24-17**

Related Information	Supersedes
CP-2, *Code of Conduct*, EB-1, *Traffic Enforcement, Violator Contacts, and Citation Issuance*, EB-2, *Traffic Stop Data Collection*, GB-2, *Command Responsibility*, GC-13, *Awards*, GC-16, *Employee Grievance Procedures*, GC-17, *Employee Disciplinary Procedure*, GG-1, *Peace Officer Training Administration*, GH-2, *Internal Investigations*, GH-4, *Bureau of Internal Oversight*	GH-5 (11-18-15)

PURPOSE

The purpose of this policy is to provide procedures for an Early Identification System (EIS) which is designed to identify Office operating procedures that may need reevaluation and to assist supervisors with consistently evaluating employees, conducting performance evaluations, identifying outstanding employee performance, identifying those whose performance warrants further review, intervention, and when appropriate, a referral to the Professional Standards Bureau (PSB) for alleged misconduct.

Although this Policy refers to "employees" throughout, this Policy also applies with equal force to all volunteers. Volunteers include, but are not limited to, reserve deputies and posse members.

POLICY

It is the policy of the Office to use data from the EIS to support effective supervision, evaluation, and management of employees in order to promote lawful, ethical, and professional police practices; to identify behavior that represents a risk to the employee, community or the Office; and to evaluate Office operating procedures.

DEFINITIONS

Alert: A notification generated by the EIS that initiates a review of employee performance and/or conduct or of an Office operating procedure.

Blue Team: The EIS application that allows employees and supervisors to record information in a database regarding incidents, performance, and conduct. The information from Blue Team is transferred to the IAPro Early Identification case management system.

Bias-Based Profiling: The selection of an individual for law enforcement contact or action based to any degree on an actual or perceived trait common to a group, including race, national origin, ethnic background, immigration status, gender, sexual orientation, gender identity, religion, economic status, age, cultural group, or any other identifiable group characteristic, except as part of a reliable and specific suspect description. Selection for law enforcement contact or action includes selection for a stop, detention, search, issuance of citation, or arrest. Such bias-based profiling is prohibited even when a deputy otherwise has reasonable suspicion or probable cause justifying the law enforcement contact or action. The establishment of reasonable suspicion and/or probable cause must remain neutral as to race and the other characteristics listed above.

Boilerplate: Language that is stock, formulaic, unoriginal, appears repeatedly in different reports, and fails to attest to the unique facts of an incident.

Conclusory: An assertion for which no supporting evidence is offered.

Disparities: Lack of similarity or equality, inequality, difference.

***Early Identification System* (EIS):** A system of electronic databases that capture and store threshold events to help support and improve employee performance through early intervention and/or to identify problematic operating procedures, improving employee performance, identifying detrimental behavior, recognizing outstanding accomplishments, and to improve the Office's supervisory response. The computerized relational database shall collect, maintain, integrate, and retrieve information gathered in order to highlight tendencies in performance, complaints, and other activities. The database allows the Office to document appropriate identifying information for involved employees, (and members of the public when applicable), and the actions taken to address the tendencies identified. Blue Team, the EIS Dashboard, IAPro, and EIPro are applications of EIS.

EI Dashboard: A Blue Team database tool that provides a visual overview of an employee's status in the EIS and is used to monitor alerts within the system. The color green in the EIS Dashboard indicates the number of the identified incidents for one of the tracked threshold events is within the standard range. The color yellow indicates the employee is one incident away from reaching a threshold. The color red in the EIS Dashboard indicates the employee has reached or surpassed a threshold.

***Early Intervention Unit* (EIU):** The EIU is part of the Bureau of Internal Oversight. The EIU is responsible for the implementation, maintenance, and operation of the EIS and for providing training and assistance to the EIS users. The unit conducts data analysis, data input, and review of activities exceeding thresholds to address potentially problematic conduct or operating procedures. The Office shall ensure there is sufficient staff to facilitate EIS input and training.

Employee: A person currently employed by the Office in a classified, unclassified, full-time, part-time, contract, or probationary status.

EIPro: The Office's web-based software application that allows employees and supervisors to view incident information in the IAPro case management system.

IAPro: A case management system used by the EIU, the Professional Standards Bureau, and the Compliance Division that tracks and analyzes information, including but not limited to, complaints, commendations, use of force incidents, pursuits, discipline, supervisor notes, and internal investigations.

Incident Management Dashboard: A function within the Blue Team Application that allows command staff to view, access, monitor, and reassign incidents assigned within Blue Team to anyone in their respective division.

Incident Type: The label given to an EIS entry at the time the entry is generated. The EIS utilizes the entry labels to identify, categorize, track, and sort incidents within the EIS. A complete list of the current utilized incident types with definitions are listed in Attachment A.

Intervention: An approved specified action taken by a supervisor to improve a situation or prevent a potential negative work performance situation from developing into misconduct.

Pattern: A recurring characteristic that helps in the identification of any problem. It might also act as an indicator of how that problem might behave in the future.

Peer Group: An organizational subgroup with a common work environment and common duties.

Threshold: The point at which a sufficient number of incidents have occurred to alert the EIU of conduct or performance that could become problematic for an employee or require a review of an Office operating procedure.

Volunteer: A person who performs hours of service for civic, charitable, or humanitarian reasons, without promise, expectation, or receipt of compensation for services rendered. An employee may not volunteer to perform the same, similar, or related duties for the Office that the employee is normally paid to perform.

PROCEDURE

1. **Blue Team:** Blue Team allows employees and supervisors to record information regarding incidents, performance, and conduct in a centralized location. The information entered into Blue Team is used in the EIS. The EIU shall use Blue Team to communicate with command staff, supervisors, and employees regarding EIS information.

    A. Blue Team utilizes pick-list values (i.e., drop down selections) to ensure the consistency of the data entered.

    B. Information entered into Blue Team can be routed electronically with review and approval functions at each step. The electronic routing of the information is dependent upon the type of entry made.

    C. The employee shall receive an auto generated e-mail message in their County e-mail box informing them of any EIS incidents that have been forwarded to them for action, review, approval, or correction. The message shall instruct the employee to log into Blue Team to take the appropriate action.

    D. Upon logging into Blue Team, the employee shall be notified of any EIS incidents and/or pending routings that require their action, review, approval, or correction.

2. **EIPro:** EIPro allows employees, supervisors, and command staff to review entries which have been previously entered into the EIS, including incident details, supervisor notes, alerts, and incident outcomes.

3. **EIS Incident Type Entries:** All employees are responsible for the timely, accurate, and complete entry of data in the EIS.

    A. Entries shall be entered prior to the end of the shift upon the discovery or report of the incident, unless the specific policy governing the incident type dictates otherwise.

    B. A complete list of the incident types utilized to categorize entry information in the EIS is located in Attachment A.

    C. The involved employee(s) shall be linked to the EIS entry, and when appropriate, the associated allegation(s) shall be linked with the corresponding employee(s).

    D. Attachment A provides a definition of the incident type categories, the person(s) responsible for the entry, and the available allegation(s) for each incident type entry.

4. **Supervisory Alert Notification and Intervention:** An alert for supervisory review shall be generated by the EIS when an employee meets, or exceeds, an established threshold.

    A. There are five categories of alerts generated by the EIS:

1. Allegation Alert: An alert is generated when the frequency of an allegation reaches the set threshold.

2. Incident Type Alert: An alert is generated when the frequency of an incident type reaches the set threshold.

3. Monitored Status Alert: An alert is generated when a tracked behavior is entered while an employee is in monitored status. Monitored status is used to track employees on administrative leave or probation.

4. Overall Alert: An alert is generated when the overall frequency of multiple incidents types reaches the set threshold.

5. Supervisory Alert: An alert is generated when the frequency of the tracked actions of the employees supervised by the same person reach the set threshold.

B. Supervisors may also initiate the EIS alert process on subordinate personnel prior to the employee meeting or exceeding an established threshold to address employee performance and/or conduct.

1. To initiate the process, the supervisor shall utilize the Incident Type of Discretionary Alert in Blue Team.

2. The entry shall include a written justification for the alert and be submitted through the supervisor's chain of command to the EIU.

3. If approved by the chain of command, the EIS will generate an alert and the alert process will commence.

4. If not approved by the chain of command, the reason for the non-approval will be documented within the entry by the non-approving entity, and it will be forwarded to the EIU with a carbon copy sent in Blue Team to the initiating supervisor.

5. Non-approved Discretionary Alerts will be stored within the EIS Supervisor Notes of the employee.

C. Established thresholds are viewable within EIS by accessing the EI Dashboard.

6. Thresholds are calculated within the EIS on a specified rolling time period.

7. While specified thresholds are established to assist supervisors with identifying patterns of conduct, thresholds do not substitute for continual proactive supervision.

8. Supervisors shall not wait for an alert to be received prior to taking corrective action for observed patterns, practices, or activities in violation of Office Policy.

5. **Alert Process:** When an EIS alert is generated, the EIU shall send the alert to the immediate supervisor of the identified employee through Blue Team. The next level supervisor shall also be advised of the alert assignment by the EIU through a carbon copy of the alert in Blue Team. Command staff can view all open alert incidents assigned to their respective division through the Blue Team Incident Management Dashboard.

A. The immediate supervisor shall log into Blue Team and review the alert information. The

review shall include the alert notification, type of alert, attached documentation, entries that generated the alert, and any other relevant resources to assess the alert and identify an appropriate level of intervention, the initiation of the disciplinary process, or acknowledgement of commendable behavior.

B. The supervisor shall analyze and assess available data/information to look for behaviors, issues, concerns, or policy violations on an individual-level, unit-level, or systemic level warranting attention.

C. The scope of the review must be thorough enough to identify factual circumstances surrounding the initiation, progression, and conclusion of the generating incident(s) and to enable the supervisor to identify potential issues.

D. The supervisor shall review all incident reports, supplemental reports, and body camera footage for each underlying incident, if such information exists.

E. If the generating incident(s) have already gone through a separate administrative review, such as a use of force committee review, the supervisor should be aware of the outcome of such review and should verify that the employee has followed through with any training recommendations or requirements, or is scheduled to do so.

F. The exact method of an intervention shall depend on the nature of the alert, the circumstances revolving around the activity that generated the alert, and the information specified in the alert Blue Team entry.

G. The supervisor shall take into consideration all relevant factors when determining the appropriate level of intervention, including, but not limited to the following:

1. The current EIS information of the employee;

2. Past EIS alerts and their dispositions;

3. Past work performance of the employee;

4. Current work performance of the employee;

5. Changes in the work performance of the employee;

6. Off-duty employment of the employee;

7. Known personal circumstances of the employee;

8. The overall training/experience of the employee;

9. The exact nature of the activities that generated the alert;

10. The nature of the employee’s assignment;

11. The work performance of the employee when compared to a peer group across the same squad, shift, beat, district, or entire organization; and

12. The results of any discussion or meeting with the employee regarding the alert

incident.

H. Depending upon the conduct that initiated the alert, an administrative investigation may be warranted, as specified in Office Policy GH-2, *Internal Investigations*, and/or discipline may be warranted, as specified in Office Policy GC-17, *Employee Disciplinary Procedure*. The supervisor shall utilize the Internal Complaint process to initiate the administrative investigation process, if warranted.

I. Based upon the supervisory assessment, the supervisor shall identify an approved intervention in response to the alert.

J. The approved intervention shall begin within 14 calendar days of receipt of the alert.

K. The supervisor shall select at least one of the following approved interventions:

1. No Further Action: Selected when, after the supervisory assessment, no pattern of at-risk behavior was identified or appropriate corrective action was taken prior to the activation of the alert. This selection is also appropriate if the alert was generated by an entry error.

2. Commendation: Selected when, after the supervisory assessment, the behavior is deemed worthy of department recognition. The commendation shall be submitted in accordance with Office Policy GC-13, *Awards.*

3. Meeting with Supervisor: Selected when the supervisory assessment determines that the employee needs a formal meeting with the supervisor to discuss the circumstances of the alert that does not result in any further action.

4. Employee Services: Selected when, after the supervisory assessment, the supervisor identifies that the employee may benefit or the development of a negative performance issue may be prevented from available voluntary employee services for a personal matter. The supervisor shall provide the employee with resource information and document the information provided. Any additional information regarding the employee's personal matter or the employee's utilization or refusal to use such services shall be considered confidential and not documented within the EIS.

5. Supervisor Ride-Along/Work-Along: Selected when, after the supervisory assessment, the supervisor physically observes the subordinate perform daily activities and provides encouragement, instruction, and documents conformance to policy and procedures.

6. Training: Selected when the supervisory assessment identifies a need for training. The supervisor shall make a referral to the training division for training as defined in Office Policies GG-1, *Peace Officer Training Administration,* and GG-2, *Detention/Civilian Training Administration.*

7. Supervisory Evaluation Period: Selected when the supervisory assessment determines that the employee needs mentoring and a dedicated monitoring period by the supervisor. The supervisor shall identify an appropriate review period of 30, 60, or 90 days. Upon conclusion of the review period, the EIU will send a request to the supervisor in Blue Team and require a documented final assessment of the

review period.

8. Action Plan: Selected when the supervisory assessment identifies the need to address an on-going work performance issue related to an alert, or if other intervention methods have been unsuccessful. The action plan shall identify a work performance goal, clarify what resources are required to reach the goal, and formulate a timeline for when specific tasks need to be completed. Every 14 calendar days until the completion of the action plan, the EIU will send a request to the supervisor in Blue Team and require documentation pertaining to the progress or completion of the established action plan.

9. Meeting with the Commander: Selected when the supervisory assessment determines that the employee needs a formal meeting with a command officer of the employee holding the rank of lieutenant or above, or the civilian equivalent.

10. Coaching: Selected when, after the supervisory assessment, specific instances of negative work performance have been identified, and need for immediate improvement is necessary to avoid the situation from developing into misconduct. Coaching shall be documented with the Incident Type of Coaching in Blue Team and the specific policy or policies involved in the performance issue linked to the employee.

11. Re-assignment: Selected when the supervisory assessment determines that the employee should be removed from their present assignment, shift, or work location, and placed into a different duty assignment, shift, or work location.

12. Referral to the PSB: Selected when, after the supervisory assessment, the conduct that initiated the alert warrants an administrative investigation. The supervisor shall utilize the Internal Complaint process in accordance with Office Policy GH-2, *Internal Investigations,* to initiate the administrative investigation process.

L. Alerts shall not be cleared/closed by reference to the above listed intervention strategies alone. Supervisors shall specify why the intervention fits the circumstances and provide sufficient information to support and understand the alert closure.

M. The supervisor shall document in detail the supervisory review conducted, the intervention implemented, any discussion with the employee, action(s) taken, conclusions rendered, and the intervention type of the alert within the alert report in Blue Team.

N. The supervisor shall complete and attach the *Early Identification System Alert Response Form* to the alert report in Blue Team. A blank copy of the form will be attached to every alert assigned to a supervisor for disposition. A copy of the *Early Identification System Alert Response Form* is attached to this policy, as Attachment B.

O. Completed alerts shall be submitted in Blue Team through the chain of command to the Division Commander. At every level of review each supervisor shall document in detail the supervisory review conducted, conclusions rendered, action(s) taken, and their approval of the alert response. Deficient entries shall be returned to subordinate personnel for corrections and the deficiency documented within the entry. Once reviewed/approved by the Division Commander, the alert shall be sent to the EIU.

P. Alerts assigned to an employee with the rank of Division Commander, or above, shall

require the review/approval of the next level command officer.

Q. Alerts shall be completed, reviewed by the chain of command, and returned to the EIU within 30 calendar days of assignment of the alert. Interventions requiring a follow up review period will be sent back to the supervisor by the EIU at the designated time period in Blue Team for appropriate follow up and documentation. Once completed, the follow up will also be submitted through the chain of command for review/approval.

R. Throughout the intervention process, the supervisor shall continue to maintain a written record of each of their employee's performance within the Blue Team Supervisor Notes.

S. Refusing to participate in an intervention shall result in disciplinary action, as specified in Office Policy GC-17, *Employee Disciplinary Procedure*.

T. The intervention documentation shall make no reference to any Family Medical Leave Act (FMLA) protected information, medical symptoms, conditions, or diagnosis of the employee.

6. **EIU Responsibilities:** The EIU shall coordinate the EIS and related programs and shall be responsible for maintaining all records associated with the EIS. This includes data storage, data retrieval, reporting, data analysis, pattern identification, identifying actions taken by employees that require intervention, supervisor use of system, Office procedure evaluations, documentation, auditing, and general training on the EIS. To meet this responsibility, the EIU shall:

A. In conjunction with the Training Division, provide training to employees and supervisors on the proper use of the EIS. This includes providing information to employees and supervisors regarding the proper understanding of the system's purpose, required data entry, and routing of information. Supervisors shall also be trained through the Training Division and the EIU regarding how to use the information to evaluate and make appropriate comparisons for significant individual or group patterns of concern.

B. Monitor the EIS and respond to alerts generated. This includes reviewing alerts for accuracy and routing information to the employee's direct supervisor within 72 hours of the alert. Alerts which are found to be generated due to an entry error, system error, duplication, or if the employee involved in the alert is no longer employed by the Office, shall not be sent to the supervisor and shall be closed in accordance with Section 5.K.1 of this Policy.

C. Review all EIS entries, including alert interventions, to verify compliance with entry, routing, review, and reporting requirements in Policy.

D. Request additional information through Blue Team and track EIS entries that are found deficient in entry, routing, review, and reporting requirements, in order to identify employees needing repeated corrective action.

E. Review, process, and enter all EIS entry purge requests submitted in accordance with Section 7.B of this Policy in the EIS. All purge requests with their supporting documentation will be entered into the EIS by the EIU with an incident type of EIS Action.

F. Conduct follow up on all interventions in order to confirm the approved intervention steps have been completed and documented in the EIS.

G. Initiate and send follow up documentation requests to supervisors through Blue Team if the

approved intervention involves a follow up period, or if intervention steps are unable to be confirmed to have been completed.

H. Conduct manual data entry and data management.

I. Facilitate the automated integration process for data being entered and incorporated into the EIS. A complete list of the types of data entered into the EIS is provided in Attachment A.

J. Conduct comparative data analysis of traffic stops and significant operations to identify patterns of activity by individual employees or groups of employees, and identify those whose performance warrants further review, intervention, and when appropriate, a referral to the PSB for alleged misconduct.

K. Analyze collected data on a monthly, quarterly, annual, or any other basis requested by a Division Commander to identify possible individual-level, unit-level, or systemic problems.

L. Conduct one agency-wide comprehensive analysis of the data per year, which shall incorporate analytical benchmarks previously reviewed. The benchmarks may be derived from the EIS or IAPro system. The yearly comprehensive analysis shall be made available to the public.

M. Warning signs or other indicia of possible misconduct, include, but are not limited to, the following:

1. Failure to complete appropriate documentation related to traffic stops, as specified in Office Policies EB-1, *Traffic Enforcement, Violator Contacts, and Citation Issuance* and EB-2, *Traffic Stop Data Collection*.

2. Racial and ethnic disparities in employee traffic stop patterns, including disparities or increases in stops for minor traffic violations, arrests following a traffic stop, and immigrations status inquiries, that cannot be explained by statistical modeling of race neutral factors or characteristics of the employees specific duties, or racial or ethnic disparities in traffic stop patterns when compared with data of peers.

3. Evidence of extended traffic stops or increased inquiries/investigations where investigations involve a Latino driver or passenger(s), any other ethnic minority, or any other group that may be subject to bias-based profiling.

4. A citation rate for traffic stops that is an outlier when compared to data of peers, or a low rate of seizure of contraband or arrests following searches and investigations.

5. Racial or ethnic disparities in the rate of seizure of contraband.

6. Complaints by members of the public or other employees.

7. Other indications of bias-based profiling in the exercise of official duties.

8. Indications that individuals, units, or the Office are not complying with Office data collection requirements.

N. Office personnel reviewing the collected data shall not review or analyze collected traffic stops data or collected patrol data relating to their own activities.

O. On a Quarterly and Annual basis, within 30 days of the end of the period, the EIU shall document and review all EIS Alerts generated from the IAPro database.

1. Based upon that review, the EIU Commander shall send a report to the Sworn Advanced Officer Training (AOT) Commander recommending specific formal training topics for individuals or groups to improve employee performance and address systemic issues. The EIU Commander and staff shall be available to assist and consult with the Sworn AOT Commander in identifying the EIS performance patterns or trends requiring attention. The Sworn AOT Commander and staff shall be responsible for development, implementation, and updates of all formal training events relevant to the EIS Alert data.

2. Based upon that review, the EIU Commander shall send a report to the Detention/Civilian AOT Commander recommending specific formal training topics for individuals or groups to improve employee performance and address systemic issues. The EIU Commander and staff shall be available to assist and consult with the Detention/Civilian AOT Commander in identifying EIS performance patterns or trends requiring attention. The Detention/Civilian AOT Commander and staff shall be responsible for development, implementation, and updates of all formal training events relevant to EIS Alert data.

P. Monitor and evaluate the EIS for efficiency, consistency and effectiveness of interventions for improved performance across the agency, and compliance with Office operating procedures, and make recommendations for training and/or policy revisions.

Q. Monitor and utilize access control to maintain the integrity, confidentiality, and proper use of the data contained within the EIS.

R. Maintain an intervention resources library and assist supervisors with interventions, as requested.

S. A semi-annual inspection of supervisory and command staff use of the EIS to enhance effective and ethical policing shall be conducted by the Bureau of Internal Oversight (BIO) in accordance with Office Policy GH-4, *Bureau of Internal Oversight.*

7. **Employee Responsibilities:** Employees are responsible for keeping supervisors informed of their actions in accordance with Office Policy CP-2, *Code of Conduct*.

A. Employees shall utilize the EIS to enter information, review and complete incidents assigned to them in EIS, and route incidents as required by Policy.

B. If an employee generates an EIS entry in error that requires the entry to be deleted or purged from the EIS, the employee shall forward the entry in Blue Team with an explanation to their supervisor for approval. The supervisor shall review the request and if approved, forward the entry to the EIU to be removed.

C. Attachment A provides a definition of the incident type categories, the person(s) responsible for the entry, and the available allegation(s) for each incident type entry.

D. The Employee Grievance Procedure governed by Office Policy GC-16, *Employee Grievance Procedures*, is the method for an employee to resolve concerns pertaining to grievance eligible matters entered on them in EIS. Non-grievable matters are defined in Office Policy GC-16, *Employee Grievance Procedures*.

8. **Supervisor Responsibilities:** Supervisors are responsible for entering employee information into the EIS

and using the EIS to monitor subordinates' conduct. Supervisors shall attempt to identify and address performance or conduct issues before they reach an alert within the EIS.

A. Attachment A provides a definition of the incident type categories, the person(s) responsible for the entry, and the available allegation(s) for each incident type entry.

B. All EIS entries initiated by a supervisor, with the exception of Internal and External complaint entries shall be carbon copied in Blue Team to the involved employee(s). Supervisor initiated EIS entries which do not require the approval/review by the chain of command, such as supervisor notes, shall also be carbon copied in Blue Team to the supervisor of the person initiating the entry.

C. Supervisors shall use the EIS to monitor subordinates' conduct. Supervisors shall do the following:

1. Review and respond to alerts pertaining to subordinates in accordance with Section 5 of this policy;

2. Initiate, implement and assess the effectiveness of interventions conducted in response to EIS information;

3. Document in detail the supervisory review conducted, conclusions rendered, and response to all incidents assigned or submitted by subordinate personnel within the EIS;

4. Review weekly subordinates' Blue Team entries to ensure proper action was taken, return deficient entries to subordinates for corrections, and route the approved incidents through the chain of command to the EIU;

5. Track each subordinate's violations or deficiencies in arrests and the corrective action taken, in order to identify deputies needing repeated corrective action. Deficiencies in arrests include situations where there was no probable cause for arrest or no basis for the legal action taken. These deficiencies shall be documented in the EIS in accordance with Office Policy GB-2, *Command Responsibility*, within a Blue Team IR Memorialization entry;

6. Conduct a review of EIS records within 14 days of all employees upon transfer to their supervision or command. This review shall be documented within the Blue Team Supervisor Notes;

7. Conduct two reviews per month of each sworn, and one per month of each non-sworn subordinates' EIS information for the purpose of identifying and responding to any conduct patterns or concerns including, but not limited to racial profiling, improper immigration enforcement, investigatory stop violations, detentions unsupported by reasonable suspicion or otherwise in violation of Policy. This review shall be documented within the Blue Team Supervisor Notes; and

8. Notify his chain of command so that the Office may initiate an investigation in accordance with Office Policy GH-2, *Internal Investigations*, if he believes an employee may be engaging in racial profiling, unlawful detentions or arrests, improper enforcement of immigration-related laws, or other behaviors that warrant administrative investigation. The supervisor shall also closely monitor the situation.

9. **Command Staff Responsibilities:** Command staff is responsible for entering employee information into the EIS and using the EIS to monitor subordinates' conduct.

A. Command staff shall attempt to identify and address performance or conduct issues before they reach an alert within EIS.

B. Command staff shall use the EIS in the same manner as required by supervisors. Additionally, command staff shall do the following:

1. Monitor the EIS Incident Management Dashboard to assure timely completion of all EIS incidents assigned to personnel under their command;

2. Take appropriate corrective or disciplinary action against supervisors who fail to conduct reviews of adequate and consistent quality;

3. Review and evaluate the quality and completeness of supervisory actions and interventions taken in response to EIS alerts and EIS incidents. The quality of these supervisory actions shall be taken into account in the supervisor's own performance evaluations, promotions, or internal transfers;

4. Document in detail the command review conducted, conclusions rendered, and response to all incidents assigned or submitted by subordinate personnel within the EIS;

5. Conduct quarterly reviews of broader, pattern-based reports provided by and in conjunction with the EIU to assess the quality and effectiveness of interventions. Specific attention shall be directed at investigatory stop violations and arrests without probable cause; and

6. Conduct a review of EIS records within 14 days, including disciplinary history, of all employees upon transfer to their supervision or command. This review shall be documented within the Blue Team Supervisor Notes.

10. **Hardware and Equipment:** The Office shall maintain computer hardware, including servers, terminals and other necessary equipment, in sufficient amount and in good working order to permit personnel, including supervisors and commanders, ready and secure access to the EIS system to permit timely input and review of EIS data.

11. **Data Security and Retention:**

A. Employees who have been authorized to access the EIS shall only do so in the performance of their duties. The access and use of the EIS for personal reasons, or as a matter of curiosity, is strictly prohibited. Employees who are found to be in violation of this section shall be subject to disciplinary action, as specified in Office Policy GC-17, *Employee Disciplinary Procedure*.

B. Employees who have access to the EIS shall only have the access required of their position in the Office.

C. Individual profiles are set for supervisors to see only those employees they supervise.

D. Entry to the system shall be only through authentication through username and password.

E. The EIS shall include appropriate identifying information for each involved employee, including the name, badge number, race and/or ethnicity.

F. A usage log shall be maintained by the system showing who viewed entries, made entries, and

what entries were made.

G. Office personnel shall enter information into the EIS in a timely, accurate, and complete manner, and shall maintain the data in a secure and confidential manner. No individual shall have access to individually identifiable information that is maintained only within EIS and is about an employee not within that supervisor's direct command, except as necessary for investigative, technological, or auditing purposes.

H. All personally identifiable information about an employee included in the EIS shall be maintained for at least five years following an employee's separation from the Office. Information necessary for aggregate statistical analysis shall be maintained indefinitely in the EIS.