NEWARK POLICE DIVISION
GENERAL ORDER

SUBJECT:	GENERAL ORDER NO.
IAPRO & BLUETEAM	**19-05**
SUPERSEDES:	DATED:
General Order 05-02 Dated June 23, 2016	**July 8, 2019**

RELATED POLICIES & GENERAL ORDERS:
NJ Attorney General Directive 2018-3;
General Order 10-02, Early Warning System & Performance Monitoring;
General Order 17-02, Risk Analysis Review;
General Order 18-21, Use of Force Reporting & Investigations;
General Order 18-25, Complaint Intake & Investigations Process;
General Order 18-26, Disciplinary Process & Matrix;
General Order 19-02, Motor Vehicle Crash Investigation Unit

NEWARK POLICE DIVISION
GENERAL ORDER

I.   Purpose

This order will provide instructions and guidance in the proper use and management of the IAPro and Blue Team systems. Through proper use the software will provide; an Early Warning System, (*refer to General Order 10-02, Performance Monitoring*) designed to detect patterns and trends in police conduct before the conduct escalates, case management of investigations, the linking and storing of files, statistics of personnel activity and achievements and allow for automated correspondence, forms, reports, and charts. This order will also provide direction for the proper access and security of the systems.

II.   Policy

The Newark Police Division recognizes the importance of monitoring its personnel and taking proactive steps towards self-discipline to ensure a professional and positive public image. The ability to document and track employee performance and behavior in a large police agency can present challenges. To achieve our goals, the Newark Police Division employs modern technology and tools capable of storing and analyzing such large amounts of detailed information.

It is the policy of the Newark Police Division to utilize IAPro and BlueTeam software to its fullest potential in accordance with the manufacturer's specifications to manage, document and analyze personnel incidents and activities, to provide early intervention against misconduct, and to electronically manage the disciplinary process and personnel disciplinary records of the Newark Police Division.

III.   Responsibility for Compliance

All Division members are responsible for complying with this General Order. Command and supervisory officers shall ensure that subordinates are aware of, understand and comply with this General Order. All Division members are subject to discipline for violations of the contents of this General Order.

IV.   System Capabilities; IAPro & BlueTeam:

A.   **IAPro** is an inter-relational database software program capable of providing the following:

1.   Personnel Records – IAPro stores and analyzes personnel information such as complaints, charges, hearings, discipline, grievances, firearms discharges, police pursuits, police involved accidents, use of force, awards, commendations, training, and the various monitoring levels of individual employees. IAPro stores and provides quick access to personnel details such as important dates, personal identifiers, contact information, photographs, supervisors and assignment histories. IAPro will also track disclosure records whenever personnel information is released.

2.   Early Warning System, (EWS) – EWS is used to assist in identifying employees whose performance warrants review and when appropriate, intervention. EWS continuously monitors the performance and behavior of all personnel and components of the organization. EWS provides for the systematic review of select activities or incidents received or generated by an employee or the Division.

3. <u>Case Management</u> – IAPro allows for management of Office of Professional Standards, (OPS) caseload along with drill down capability. It provides for automatic deadlines and reminders for tasks. The quality assurance feature ensures that information is properly entered into each incident for comprehensive documentation, tracking, analyzing, and reporting.

4. <u>File Link and Storage</u> – Digital files of any type (data, audio, or video) may be linked and Stored in IAPro.

5. <u>Statistical Reports</u> – IAPro is capable of producing a broad range of statistical reports and charts that include aggregate, trend, exception, and comparative formats. Reports can also be customized.

6. <u>Automated Correspondence and Forms</u> – Correspondence and Forms created in Microsoft Word can be integrated into IAPro for automated production saving investigators and staff significant time.

7. <u>Access and Security Controls</u> – Access and use of IAPro can be customized to each user. Individual security features can be set for individual users, incidents and reports.

B. **BlueTeam** is companion software to IAPro that allows for limited and secure interaction with IAPro by personnel assigned outside of OPS. It is designed to simplify and assist with incident reporting, EWS, Transparency, and the Internal Affairs process. Presently, NPD BlueTeam provides the following:

1. **Incident Entry:**

   a. Internal, External, and Anonymous Complaints;

   b. Use of Force;

   c. Constructive Authority (pointing firearm);

   d. Vehicle Pursuits; and

   e. Non-Disciplinary Actions

2. A **chain-of-command review and approval process** for all reports entered into the system.

3. An individual "dashboard" that may be activated to allow each employee to constantly monitor their own early intervention activities.

4. A supervisor "dashboard" that may be activated to allow each superior officer to monitor, in real-time, the individual early intervention activities of every employee under their purview.

V. <u>Confidentiality</u>

All information contained in, or derived from IAPro and BlueTeam is considered "CONFIDENTIAL". Access to IAPro and BlueTeam is permitted only on a need to know basis and is limited to the minimum amount of information necessary to accomplish the intended purpose of the use, disclosure or request. Accessing information that is not within the scope of someone's duty, altering, misusing or disclosing information without

authorization to IAPro, BlueTeam or their restricted areas is strictly prohibited. Users shall not disclose their log-in information nor shall anyone use another person's log-in information. Users shall not leave IAPro or BlueTeam unattended while signed on.

VI.   Access

Access to IAPro, BlueTeam, and its servers shall be restricted in accordance with the New Jersey Attorney General Directives governing "Law Enforcement Computers", the Guideline governing Internal Affairs Policy, and Newark Police Division Rules & Regulations.

VII.   Security

IAPro and BlueTeam have various levels of security features and permissions. All new user accounts shall be created by the IAPro and BlueTeam administrator with the user's title, first name, last name, assigned unit, and user e-mail. IAPro and BlueTeam will automatically create a "last name, first name" login for the user.

Each user shall create a unique password. The term of each password shall be set by the administrator for a maximum of one (1) year. IAPro and BlueTeam will automatically prompt users to create a new password upon expiration. Users can also change their password at any time or as often as needed.

Once an IAPro user file is created it shall never be deleted until the individual has permanently separated from the division (i.e. retired, resignation, termination etc.). Should a user be transferred or reassigned to another command, or no longer be permitted into IAPro, the administrator shall only disable that individual's login capability to preserve that user's links to cases within the system. If a user returns to OPS, then the administrator need only re-enable the individual's login capability which will restore links to all previous cases in the user's history.

All users shall log onto IAPro and BlueTeam at the start of each work day. Anytime a user leaves their work station they must log out from IAPro or BlueTeam and must never leave IAPro or BlueTeam open and unattended. Users shall never rely on locking a computer as an adequate safeguard against access to IAPro or BlueTeam that has been left open in the background.

BlueTeam will time out and close after 60 minutes of inactivity and any unsaved incident(s) will be lost and will need to be re-entered.

The following are special security requirements:

A.   **IAPro/BlueTeam SQL Server(s)** - Access to the server(s) is strictly prohibited. Only authorized persons with sufficient knowledge of server technology should access the server. The commanders of Communications Division/911 Call Center and OPS shall maintain written documentation of the server password(s) in a secure location.

B.   **Administrator Access** – The commander of OPS shall designate an "administrator" to the programs. The administrator must be an individual with sufficient computer knowledge or training to serve as the program administrator and shall have administrative access to IAPro and BlueTeam.

C.   **OPS Commander and Executive Officer** – The OPS commander, the OPS executive officer and the administrator will have their user access set to level 1 – "Top Secret" and shall have the following "Feature Access" settings turned on:

1.   Access system-wide tasks;
2.   Alter access levels;
3.   Change category flags;
4.   Change incident assignments;
5.   Change monitored status;
6.   Charts access;
7.   Complaint incident lock override;
8.   Delete files from incidents;
9.   Delete tasks from incidents;
10.   Display/print any report;
11.   Dissemination log features;
12.   EI features access;
13.   Enter new incidents;
14.   IA and Case number change;
15.   Incident stats tab modify;
16.   Incident type change;
17.   Query builder;
18.   Reports access;
19.   Run officer history reports;
20.   Secured incident override;
21.   Timescales change capability;
22.   View and access alerts;
23.   View category flags;
24.   View monitored status; and
25.   View why officer monitored.

The OPS commander, executive officer, and administrator shall have their overall data change capability set to read/write (default) and shall have "Advanced Incident Change Capability" enabled.

D.   **Investigative User (OPS)** – All OPS investigators, including members of the All-Force Investigation Team (AFIT) will have their IAPro user access set to level "3–Confidential". Investigators will not have the ability to edit pick list values, unlink involved officers or civilians, or to view usage logs.

The administrator shall include these individuals in the investigator assignment pick list. If the investigator is a supervisor that will oversee a module of investigators, then the "supervisor" box shall be selected to include these individuals in the supervisor's box.

Investigative users will have only the following "Feature Access" settings turned "on":

1.   Access system-wide tasks;
2.   Delete tasks from incidents;
3.   Display/print any report;
4.   Dissemination log features;
5.   EI Features access;
6.   Enter new incidents;
7.   Incident stats tab modify;
8.   Query builder;

9.   Reports access;
10.   Run officer history reports;
11.   View and access alerts;
12.   View category flags;
13.   View monitored status; and
14.   View why officer monitored.

OPS investigators shall have their "Overall Data Change Capability" set to "read/write (default)", with their "Advanced Incident Change Capability" and "Option 1" enabled. This will allow the supervisors and investigators read/write access to only those cases assigned to them or under their supervision. Investigators shall only be allowed to view the contents of their own mailbox. Investigators shall only be permitted to enter Anonymous, Citizen/External, and Division/ Internal incidents.

E.   **OPS Clerical Staff Users** – OPS clerical staff shall not have the investigator or supervisor roles turned on and their user access shall be set to level 3 – "Confidential". Clerical staff will not have the ability to edit pick list values, unlink involved officers or civilians, and will not be allowed to view usage logs. Clerical staff users will have only the following "Feature Access" settings turned "on":

1.   Access system-wide tasks;
2.   Charts access;
3.   Display/print any report;
4.   EI feature access;
5.   Enter new incidents;
6.   Incident stats tab modify;
7.   Query builder;
8.   Reports access;
9.   View and access alerts;
10.   View category flags;
11.   View monitored status; and
12.   View why officer monitored.

OPS clerical staff shall have their "overall data change capability" set to "Read/Write" (default) only. Clerical staff will only be allowed to view the contents of their own mailbox. Clerical staff shall have the ability to enter the following incidents:

1.   Anonymous Complaints;
2.   Citizen or external complaints;
3.   Division or internal complaints;
4.   Firearm Discharge incidents;
5.   Use of force incidents;
6.   Vehicle accident incidents;
7.   Vehicle pursuit incidents;
8.   Awards & Commendations;
9.   Training Records; and
10.   Non Disciplinary Action (NDA)

F.   **Advocate Unit Staff** – Advocate staff shall not have the investigator or supervisor roles turned on and their user access shall be set to level 3 – "Confidential". Advocate staff will not have the ability to input

incidents, edit pick list values, unlink involved officers or civilians, and will not be allowed to view usage logs. The Advocate Unit is responsible for the input and maintenance of all information related to the disciplinary process, such as hearings, appeals, grievances, suspension dates and terms, and any other outcomes related to the disciplinary process. Advocate staff will have only the following "Feature Access" settings turned "on":

1. Display/Print any report;
2. Query builder;
3. Reports access;
4. Run officer history reports;
5. View monitored status; and
6. View why officer monitored

G. **Office of Transparency and Risk Analysis Management** – Transparency & Risk Analysis Management staff, including the Motor Vehicle Crash Investigation Unit (MVCIU) shall not have the investigator or supervisor roles turned on. Their access level shall be set to level 3 – "Confidential". They shall have the ability to input incidents, edit pick list values, unlink involved officers or civilians and will be allowed to view usage logs. They are responsible for all matters relating to the early warning system and monitoring of personnel. Transparency & Risk Analysis staff shall have the following "Feature Access" settings turned on:

1. Access system-wide tasks;
2. Change category flags;
3. Change incident assignments;
4. Change monitored status;
5. Charts access;
6. Complaint incident lock override;
7. Delete files from incidents;
8. Delete tasks from incidents;
9. Display/print any report;
10. Dissemination log features;
11. EI features access;
12. Enter new incidents;
13. IA and Case number change;
14. Incident stats tab modify;
15. Incident type change;
16. Query builder;
17. Reports access;
18. Run officer history reports;
19. Secured incident override;
20. Timescales change capability;
21. View and access alerts;
22. View category flags;
23. View monitored status; and
24. View why officer monitored

H. **BlueTeam Users** - All BlueTeam Users <u>not</u> assigned to OPS shall have their security access level set to "5".

VIII.   **Responsibilities**

 A. **OPS Commander** – The OPS commander shall be responsible for the following:

  1. The overall proper use, maintenance, security and integrity of IAPro and BlueTeam in accordance with the manufacturer's specifications, Division policy, and New Jersey State Attorney General Guidelines.

  2. Shall ensure that the server(s) receive(s) annual maintenance and cleaning, the back-up system is functioning properly and archiving, and that the server environment(s) is/are properly cooled at all times.

  3. Shall maintain a written copy of the IAPro and BlueTeam Server(s) and Administrative Password(s) in a secure location (i.e. in a sealed envelope and locked in a desk or file cabinet).

  4. Shall designate an IAPro and BlueTeam "administrator(s)". The administrator(s) can be of any rank but must be assigned to OPS, possess sufficient knowledge of computers and the IAPro and BlueTeam software.

  5. Shall ensure through channels, that the manufacturer's annual maintenance fees are paid and that software updates are obtained and performed at least once per year.

  6. Shall ensure that all users enter information properly and promptly.

  7. Shall ensure that all personnel files within the IAPro system are completely filled out and immediately updated as changes become known. This shall include, but is not limited to whenever a Personnel Order announces permanent transfer or whenever recall information is updated (i.e. during bi-annual uniform inspection updates of recall information).

 B. **Administrator** – The IAPro and BlueTeam administrator shall be responsible for the following:

  1. Shall maintain a written copy of the IAPro and BlueTeam server(s) Administrative Passwords in a secure location (i.e. in a sealed envelope and locked in a desk or file cabinet).

  2. Shall obtain and install updates from the manufacturer at least once per year. After each update is installed, the administrator shall perform the required Product Upgrades per the manufacturer's instructions.

  3. Shall set and maintain all System Settings and other customizable settings per this order and prevent deviations that will negatively affect the ability of the program to perform according to standards. This includes the setting of thresholds, due dates, tasks, incident types, classifications, sub-classifications, drop-down menus, etc., that are required to comply with the reporting requirements by the County Prosecutor and New Jersey State Attorney General.

  4. Shall reset all number sequencing promptly on January 1st of each year.

5.   Shall ensure that users are prohibited from entering new officers at all times. This function shall only be enabled long enough to input new personnel at the time of appointment and must then be immediately turned off to safeguard against improper or duplicate entries of personnel or of personnel that are not employees of the Newark Police Division.

6.   Shall merge duplicate citizens, officers, and users as soon as duplicate records are discovered.

7.   Shall perform routine product maintenance quarterly. This includes the removal of obsolete reports, deleting orphan addresses, closing out unread mailbox routings, data cleansing, restoring officer links, merging and undeleting users.

8.   Shall ensure that the access level for all "Officer Records" and "Citizen Records" member file is set to "5 – Unclassified".

9.   Shall delete entry errors as required and shall document the reason for the deletion in the log when prompted.

10.   Shall unlock incidents that have been inappropriately locked.

11.   For IAPro, shall enter new users, or activate login capability for returning personnel, and shall set their individual parameters and security access as directed by this order. The administrator shall immediately disable the login capability of any person separated from the OPS or the Advocate Unit. The administrator shall also delete users only after they have permanently separated from the division (i.e. retirement, resignation, termination, etc.).

12.   For BlueTeam, shall activate BlueTeam capabilities for all newly entered personnel, enter the appropriate email address for each user, and shall establish each user's "purview" per their assignment and chain of command.

13.   Shall limit all password terms to expire within one year or less.

14.   Shall "flush" personnel from IAPro that are logged into the software that have failed to log out of the system.

15.   Shall unlink personnel or files that have been improperly linked to an incident.

16.   Shall create and maintain all Word templates used in IAPro.

17.   Is responsible for the training of OPS personnel in the proper use of IAPro and BlueTeam incident entry into IAPro.

C.   **OPS Executive Officer** – The executive officer of OPS shall be responsible for the following:

1.   Upon the receipt of any new investigation, the executive officer shall be responsible for assigning the Investigation of Personnel number.

2.   Shall enter the Unit Assigned, the Investigator Assigned and the Supervisor Assigned on the Status and Assign page.

a. If the investigation is being assigned to be handled at the command level, shall enter the command in the "Unit Assigned" field, shall check off that the investigation is being handled at the field/unit level, and shall enter the field-level investigator's name once known or upon receipt of the completed investigation.

3. Upon assigning the investigation, shall change the status from "Initial" to "Active", shall enter the "Assign Date" and ensure that the "Due Date" is set for thirty (30) days and entered. Forty-five (45) days for Command level investigations.

a. If the incident is to be investigated by a command other than OPS, then the investigation shall be forwarded out through BlueTeam to the appropriate command for investigation.

b. Upon receipt of an investigation from OPS, a Commander shall assign the investigation to a supervisor and shall forward the investigation to that supervisor through BlueTeam.

c. Upon completion, the investigation and all associated documents that are linked into the incident shall be forwarded through BlueTeam up the chain of command to OPS.

4. Whenever a case is forwarded to a prosecutor or higher authority, or whenever a case is legally suspended according to law, the executive officer shall change the status from active to "Suspended/Pending" and shall document the date and the reason the case was forwarded. Cases shall not be listed as "Suspended/Pending" for any other reason.

a. In addition to changing the status, the OPS executive officer shall modify the "Prosecution" tab on each involved officer's "Snapshot Info" located on the "Links" page. The Executive Officer shall enter the Prosecutor, Prosecution Status, Primary Related Charge and the Prosecutor's Case Number once it becomes known.

b. Shall enter the assistant prosecutor's name in the "Outside Investigator" field on the Status and Assign page.

c. Whenever a Disposition Letter is received from a prosecutor, the executive officer shall return the case status to "Active" and enter a new Assign Date and set a new "Due Date" for not more than thirty (30) days from the official receipt of the disposition letter.

d. In addition to changing the status, the OPS executive officer must enter the disposition in the "Prosecution Status" on the Prosecution tab on each involved officer's Snapshot Info.

5. Whenever a case is forwarded for final administrative review by either the commander of OPS or the Chief of Police, shall change the status to "Forwarded" and shall enter the date that the file was forwarded.

6. Upon receipt of a properly executed Complaint Against Personnel (CAP) form, shall assign the CAP number and enter the charge(s) recommended for each officer, shall enter the date that the recommended charge was approved, shall enter a finding of "sustained" for each affected allegation and shall enter the Finding Date. All other allegations will remain open until the completion of the investigation when they will be closed according to their dispositions.

7.   Upon completion of the investigation, shall ensure that all allegations entered are correct and shall edit each allegation "Finding" and "Finding Date" to match the date that the investigation was approved.

8.   Shall ensure that the charges and dates listed under each officer are accurate.

9.   Upon final approval of each incident, shall change the status of the incident to "Completed" and shall enter the approved date and the appropriate case "Disposition".

10.   Upon marking any incident as Completed, shall close any remaining incomplete tasks and shall ensure that the incident's access level is set to "5 – Unclassified".

11.   Proper entry and maintenance of the "Disclosure Log" for each incident and personnel record to document every review or release of any information (i.e. Giglio or Brady Requests, in-camera reviews, etc.) other than for internal disciplinary purposes.

12.   Proper entry and maintenance of the "Disclosure Log" for each personnel record background review (i.e. Retirement Applications, Secondary Firearm Applications, etc.) listing the outcome of the review and, if applicable, a description of the weapon approved.

13.   Shall review BlueTeam entries each day. Once approved, shall transfer incidents from BlueTeam into IAPro's main database.

14.   Shall assign all field level investigations to the appropriate command and shall forward investigations to those command via BlueTeam.

D.   **Investigators (OPS)** – All OPS investigators, including AFIT investigators, are responsible for the following:

1.   The prompt and proper entry and maintenance of incidents assigned to them. This includes the immediate linking of personnel and civilians as their identities become known, the correction of any errors in individual profile details, statistical information, location and address details, allegations and dispositions, and all other related information to ensure the most accurate and complete documentation of every incident.

2.   The linking of all important investigative documents (i.e. Preliminary Investigations, Supplemental Investigations, Notification Letters, Disposition Letters, Prosecutor receipts and correspondence, and CAP forms). While there is no restriction on what documents should be linked, lower priority documents do not need to be individually linked. "Whole package" investigations will be linked after final approval.

3.   Investigators shall open and process all tasks associated with each incident to document the completion and chronology of each task.

4.   On a daily basis open all IAPro email routed to them and respond as required.

5.   Shall ensure that each incident assigned to them has the correct "Incident Type", "Classification" and "Sub-Classification" listed.

6.   Shall ensure that the "Incident Level Organizational Assignment" correctly reflects where the personnel were assigned when the incident occurred and correctly reflects the personnel's current assignment.

7.   Shall immediately correct or report to the administrator or commander of OPS, any discrepancies or errors in IAPro information that cannot be immediately corrected. This includes improperly linked persons, files, descriptions or locations, entry errors, or improper entries.

E.   **OPS Clerical Staff** – The clerical staff assigned to OPS are responsible for the following:

1.   The prompt and proper entry and maintenance of incidents assigned to them. This includes the immediate linking of personnel and civilians as their identities become known, the correction of any errors in individual profile details, statistical information, location and address details, allegations and dispositions, and all other related information to ensure the most accurate and complete documentation of every incident.

3.   When prompted by the administrator, shall enter newly hired personnel and their information into IAPro officer folders.

4.   Upon receiving personnel or training orders, shall promptly update all information, training, or awards into individual officer folders.

5.   Shall promptly update citizen information in citizen folders.

6.   Shall scan and link all <u>finalized</u> Investigation of Personnel (IOP) Reports and Complaint Against Personnel (CAP) forms into their respective incident folders.

7.   Upon receipt of an investigation from an outside command, all documents shall be scanned as one investigation PDF file and electronically linked into the respective IAPro incident file prior to forwarding documents back to the investigator for correction or to the chief of police for final review.

8.   Shall, upon final approval, scan and electronically link completed investigation packages as a single-file into the respective IAPro incident file.

9.   Shall immediately correct or report to the administrator or commander of OPS, any discrepancies or errors in IAPro information. This includes improperly linked persons, files, descriptions or locations, entry errors or improper entries.

F.   **Advocate Unit** – Advocate Unit personnel shall be responsible for the following:

1.   Shall ensure that the charges listed in IAPro under each officer are accurate, shall add information promptly, and shall modify any discrepancy without delay. Advocate is responsible for ensuring that for every charge, the charge type, charge date, statute or rule violated, charge disposition and disposition date, charge category and a brief charge narrative are listed.

2.   Shall prepare personnel history reports for the officers being charged for review by hearing officers.

3.   Shall enter "Actions Taken" for each officer charged. This includes discipline, the date of the action, number of days suspended, a brief narrative explaining the action, shall denote if discipline was handled at the command level (command level conference, etc.) and shall indicate if the action has been completed.

4.   Shall enter "Hearing" details for each officer charged including the hearing type, date, status, disclosure information, completion date and hearing outcome.

5.   Upon final disposition of any disciplinary hearing the Advocate Unit will be responsible for scanning the disciplinary hearing package into one file that shall be linked into the IAPro incident. The package must include all documents related to the post investigation disciplinary process, including:

   a.   Completed Preliminary Notice of Disciplinary Action (PNDA)

   b.   Completed Immediate Suspension Notice Documents

   c.   Correspondence of hearing adjournments, rescheduling

   d.   Completed Final Notice of Disciplinary Action (FNDA).

6.   If a grievance was filed as a result of discipline, the Advocate Unit shall document same under each "grievant" officer's "Snapshot Info" on the "Additional" tab. Advocate shall check off when the grievance is concluded and must indicate if the discipline was revoked or amended.

7.   If an employee is suspended for any reason, the Advocate Unit shall document the suspension under each suspended officer's "Snapshot Info" on the "Suspension" tab. The suspension status, the beginning and end date, and the reinstatement restrictions shall be entered.

G.   **All Force Investigation Team**

1.   Review all incoming BlueTeam Use of Force reports for accuracy and completeness, releasing all approved reports into IAPro.

2.   Return unsatisfactory BlueTeam incidents for correction.

3.   Assign a sequential number to all new Use of Force incidents.

4.   Link reports and documents into Use of Force incidents.

5.   Enter the appropriate disposition and close all Use of Force incidents.

6.   Produce the required reports, charts, or other data required to report on Use of Force.

H.   **Office of Transparency & Risk Analysis Management** – shall be responsible for the following:

1.   **Transparency**

A. Utilizing data from IAPro to produce transparency statistics.

B. Produce the required reports, charts or other data required to produce the monthly Transparency Data.

2. **Early Warning System**

A. The overall maintenance, management and oversight of the early warning system and performance monitoring.

B. Assign sequential numbers to all alerts generated.

C. Review all generated alerts, review the causes of each alert, print and forward the alerts to commands as part of the early warning system function.

D. Receive, review and approve all reports submitted in conjunction with early warning system and performance monitoring. Any deficient reports shall be sent back to the affected commands for revisions.

E. Ensure the Commander of OPS, or his/her designee is made aware, in writing, of all officers on performance monitoring, and their outcomes.

F. Link files and documents related to the alerts.

G. Enter comments documenting the management of each alert.

H. Close each alert upon completion.

I. Maintain all personnel on "Monitored" status. Remove or upgrade monitored personnel according to policy.

J. Produce the required reports, charts, or other data required to report on early warning system measures.

3. **Police Pursuits**

A. Review all incoming BlueTeam Police Pursuit reports for accuracy and completeness, releasing all approved reports into IAPro.

B. Return unsatisfactory BlueTeam incidents for correction.

C. Assign a sequential number to all new Police Pursuit incidents.

D. Link reports and documents into Police Pursuit Incidents.

E. Enter the appropriate disposition and close all Police Pursuit Incidents.

F. Produce the required reports, charts, or other data required to report on Police Pursuits.

4. **Motor Vehicle Crash Investigative Unit**

    A. Review all incoming BlueTeam police involved Motor Vehicle Crash reports for accuracy and completeness, releasing all approved reports into IAPro.

    B. Return unsatisfactory BlueTeam crash reports for correction.

    C. Assign a sequential number to all new police involved motor vehicle collisions.

    D. Link reports and documents into police involved into motor vehicle incidents.

    E. Enter the appropriate disposition and close all police involved motor vehicle incidents.

    F. Produce the required reports, charts or other data required to report on police involved motor vehicle collisions.

IX. Entering Incidents & Data

The IAPro and BlueTeam software are only as good as the information that is entered. All information entered must be accurate and conform to standards. Incorrectly entered or incompatible data, or data that is missing adversely affects the program's ability to properly analyze information or to produce accurate reports. Therefore, all persons responsible for entering and working with the data within these programs are responsible for accuracy and completeness at all times.

Only those incidents where a Newark Police Division employee is involved and will be linked to an incident shall be entered into IAPro or BlueTeam. Every incident entered **MUST** include a linked "involved officer (employee)" or if the employee's identity is unknown then "An Unknown Officer" must be linked. Police impersonation incidents shall not be entered into IAPro until reasonable belief exists that Newark Police Division personnel are involved.

A. **Drop-Down Menus -** Whenever a drop-down menu is present, persons entering information shall rely on the information listed in that menu. If an item is not listed and needs to be entered the executive officer or administrator shall be consulted who may add the item to the drop-down menu using the "F2" function if the modification is reasonable.

B. **Formatting** – The manner that items are entered into IAPro and BlueTeam must be consistent. The following rules must be followed when entering data:

    1. **Names** – To ensure consistency, names in shall be formatted as follows:

        a. Last names with prefixes or hyphens shall be typed without spaces (i.e. "McMahon" not "Mc Mahon", "O'Connor" not "O' Connor", "Johnson-Smith" not "Johnson – Smith", etc.).

        b. Suffixes shall be typed after first names following a comma and a space (i.e. "John, Jr" or "James, III", etc.).

  c. Ranks are pre-established in the drop down menus of IAPro and must not be free typed. Civilian titles are all grouped as "civ".

 2. **Locations/addresses** – To ensure consistency and the ability to query locations, all addresses shall be formatted as follows:

  a. Street names shall be spelled out in full (i.e. Irvine Turner, Muhammad Ali, North 6th, East Alpine, etc.). At no time shall initials be used. Intersecting streets shall be entered in alphabetical order without suffixes and separated by a right slash without spaces (i.e. Broad/Market, 16th/South 16th, etc.).

  b. Street suffixes shall be selected from the drop down menu – not typed in.

  c. Cities and counties shall be selected from the drop down menu. However, if a city or county is not listed it may be manually entered. City and county names shall be spelled out in full without abbreviations.

  d. States shall be selected from the drop down menu and shall be the accepted two-letter initial.

  e. Once entered IAPro and BlueTeam may suggest a list of previously entered addresses. If a match is presented and confirmed it shall be selected and linked. Corrections to the formatting of the address shall be made at the time the address is linked. This will allow IAPro and BlueTeam to keep a searchable history on all locations entered.

 3. **Precinct/Sector** - Information shall be selected from the drop down menu. These are pre-formatted to capture certain statistics and must not be altered or typed in.

  a. Non-Police Facility – means any police facility that is NOT a precinct (i.e. Communications, courthouses, Juvenile Services, Fleet Management, etc.).

  b. Outside City Limits – is any location outside of the City of Newark.

C. **Incident Types** – In addition to incident types that come pre-programmed with IAPro (colored icons), the software allows for the creation of customized incidents (yellow folder icons). These incidents are created based on the regional requirements (i.e. A.G. Guidelines, N.J. Law, etc.) or the needs of the police division (e.g. Compliance Tests, Non-Disciplinary Actions, etc.). Creating incidents directly affects the program's ability to provide comprehensive reports. Incident Types created in IAPro can also be activated in BlueTeam. Therefore, IAPro shall be limited to the following incidents:

 1. Custom Incidents – are incidents created in IAPro by users that must be associated to one or more employee records. They are:

  a. Anonymous complaints – Investigative incidents stemming from complaints received from anonymous sources.

  b. Civilian (or external) complaints – Investigative incidents stemming from complaints received from a civilian, or from any person or agency outside of the Newark Police Division.

      c.   Division (or internal) complaints – Investigative incidents stemming from complaints generated from within the Newark Police Division.

      d.   Compliance Tests – Statistical incident entered when a single Compliance Test is completed and shall list all involved employees. The test will appear on each employee's history. Although a report detailing the Compliance Test can be completed within this incident, any violation occurring during the compliance test should be entered separately as a Division Complaint.

      g.   Non-Disciplinary Actions – Statistical incident entering all remedial or corrective actions taken by a supervisor to address **minor** performance deficiencies or inadequacies committed by subordinates.

2.   Pre-Programmed Statistical Incidents – The following statistical incidents are pre-programmed into IAPro. Although documents can be linked into a statistical incident, Professional Standards investigations must be tracked separately and <u>shall not</u> be conducted within any of the following statistical incidents:

      a.   Firearms Discharge – every firearm discharge incident;
      b.   Use of Force – every use of force incident;
      c.   Vehicle Accidents – every police involved accident; and
      d.   Vehicle Pursuit – every police pursuit.

D.   **Incident Numbering** – The following number sequences shall be maintained by the administrator of IAPro in the format shown:

1.   Alerts – **A**YYYY-0000
2.   Compliance Test – **CT**YYYY-0000
3.   Firearms Discharge – **FD**YYYY-0000
4.   Investigation of Personnel – YYYY-0000
5.   Use of Force – **F**YYYY-0000
6.   Vehicle Accident – **MVA**YYYY-0000
7.   Vehicle Pursuit - **P**YYYY-0000
8.   Event Numbers – PYY000000
9.   Non-Disciplinary Actions – NDAYYYY-0000
10.   Civil actions against a police officer – LYYYY-0000
11.   Constructive Authority with firearm – CAYYYY-0000

E.   **Entering an Incident into IAPro**. Each IAPro incident has seven (7) tabs; Links, Summary, Status & Assign, Tasks, Routings, When & Where, and a statistical page. The final tab is a statistical page and will differ depending on the type of incident being entered. The process for entering all incidents is the same with the exception of the statistical tab.

Upon opening an incident, the following information shall be entered:

1.   The access level. All investigations shall begin at level "5-Unclassified" unless otherwise stipulated by the commander or executive officer of OPS.

2.   The date and time that the complaint was received shall be documented keeping in mind that his may not be the same as the date the incident is being entered.

3. Enter the involved citizen. The primary involved citizen shall always be entered first, then other citizens in order of importance or role in the incident:

    a. Citizen names shall first be searched for prior activity. If their record already exists, then the citizen folder should be selected and linked and all their information must be verified or updated. When updating information, prior phone numbers and addresses shall not be deleted. Indicate if the citizen is the person reporting the complaint or is a third party to the complaint.

    b. If this is the first time that the citizen is being entered, enter as much information as possible. Multiple addresses and telephone numbers can be added. <u>Driver's license information, social security numbers, race, sex, and birthdate must be requested and entered</u>. An e-mail address is optional and helpful. Additional and unique information can be entered in the summary box. This is especially helpful in developing a history for each complainant. Employer information should be added if available.

    c. Criminal charges lodged against the citizen must be listed. These may become pertinent to the investigator.

    d. Enter the citizen's role in the incident.

    e. You may also change the citizen's status from "involved" to "witness" or from "witness" to "involved".

4. Link the involved officer or employee. Always enter the primary involved employee first, and then add other personnel based on their order of importance or role.

    a. If the identity of an officer is unknown, then the "Add an unknown officer…" link shall be selected from the menu. <u>At no time should an officer with the name "unknown" be selected from the Officer Search Form, created, or linked to any incident</u>.

    b. Personnel entering assignments should not be permitted to "enter a new officer". This feature must remain disabled by the administrator to prevent duplicate entries.

    c. Once an officer has been selected, the officer's type of involvement must be entered.

    d. In the "Officer's Snapshot", input the officer's permanent assignment at the time the incident occurred for each officer. This may be different from the officer's assignment at the time of the incident especially if the officer was working a special detail, or was detailed out to another command at the time the incident occurred.

    e. In the "Snapshot" for each officer, enter the officer's supervisor at the time of the incident.

    f. In the Snapshot for each Officer, enter the officer's status indicating if the officer was on or off duty, employed off duty, in uniform, arrested or injured at the time of the incident.
    g. Enter one or more allegation for each involved officer.

        h.   Enter the officer's role (i.e. arresting officer, back-up officer, driver, passenger, etc.).

5.   Electronically scan and link any file or document (summonses, arrest reports, incident reports, identification or driver's licenses, etc.) that may be helpful to the investigator.

6.   Link any numbers (Event, Incident, Arrest, CDR, CAP etc.) that are pertinent to the investigation along with their description or title. It is important to enter all numbers in the appropriate format as these will become searchable.

        a.   Any number linked that can cross-reference with another IAPro number (i.e. Event number, IOP number, CAP Number, Use of Force, etc.) will direct the user to that incident when the linked number is double-clicked.

7.   Enter a "Summary of Incident". Summaries must be a <u>brief and concise</u> explanation of the incident/allegation(s). Each summary must also be specific to the incident being entered, (i.e. use of force, vehicle pursuit, etc.). **At NO time** should information regarding investigative procedures taken or other unrelated information or notes be documented here. Personnel shall never "copy and paste" the narrative from an incident report or other report into IAPro or BlueTeam. Whatever is typed in summaries will also appear on various IAPro reports, histories, which may be released to outside agencies in various IAPro reports.

8.   The "Source of Information" shall be one of the following:

        a.   <u>Document/Fax/Email</u> – Shall be any complaint received via mail, fax, e-mail, hand delivered or discovered document (i.e. newspaper or media). The purpose of this statistic is to capture complaints made in document form rather than in-person or via telephone.

        b.   <u>In Person</u> – Shall be any complaint taken in person by personnel not assigned to OPS (i.e. at a command or by a field supervisor). The purpose of this statistic is to capture the number of in-person complaints made directly to a Newark Police representative other than from OPS.

        c.   <u>Telephone</u> – any complaint received by telephone at any location including OPS. The purpose of this statistic is to capture the number of complaints made via telephone.

        d.   <u>Walk-In (OPS Only)</u> – Shall be only in-person complaints made at the OPS or directly to a representative of OPS (i.e. during a field visit, etc.). The purpose of this statistic is to capture the number of in-person complaints made directly to OPS.

        e.   <u>Complaint of Employee Misconduct</u> – Shall be complaints made by members of the public and submitted via 'Complaint of Employee Misconduct' report. The purpose of this statistic is to determine how many complaints are generated/received directly from the public, without Police Division assistance.

9.   Incident Level Organizational Assignment – shall reflect the command where the involved personnel were working at the time of the incident. This includes temporary assignments, special details, overtime assignments, and outside employment that may be different than the officer's regular assignment.

10. Enter the date, time and county where the allegation occurred. "Outside New Jersey" is an option for incidents that occurred outside of the state boundary.

11. Enter the primary incident location first, then any subsequent locations. Indicate the reason for each location (i.e. location of incident, where incarcerated, etc.).

F. **Classifications and Sub-Classifications**: Classifications and sub-classifications must be set to match the New Jersey State Attorney General Guidelines Table 1 reporting requirements so that IAPro can produce reliable tables for the quarterly and annual reports. Classifications and sub-classifications remain the same for all investigative incidents.

The following are the "Classifications" with their respective "Sub-Classifications" listed below:

1. Criminal Law Violation
   a. A list of commonly alleged federal, state (criminal and motor vehicle), and municipal law violations.

2. Compliance Test
   a. Pass
   b. Fail

3. Demeanor
   a. Unprofessional Conduct
   b. Unprofessional Gestures
   c. Unprofessional Language

4. Differential Treatment
   a. Arrest
   b. Field Inquiry
   c. Summons
   d. Tow

5. Domestic Violence
   a. Victim
   b. Suspect

6. Excessive Force
   a. Arrest
   b. Citizen Contact
   c. Motor Vehicle Stop
   d. Prisoner Handling

7. Firearm Discharge
   a. Accidental Discharge
   b. Animal
   c. Fatal
   d. Injury
   e. No Hit/Injury

8. Improper Arrest

        a.   Warrant

        b.   Warrantless

9.   Improper Entry

        a.   Warrant

        b.   Warrantless

10.   Improper Search

        a.   Person

        b.   Residence

        c.   Structure

        d.   Vehicle

11.   Other Rule Violation

        a.   A list of commonly alleged rule violations.

G.   **Statistical Tabs** - The statistical (or seventh) tab for the remaining types of incidents are pre-set with drop-down menus and check boxes. The following are the other four types of incidents:

1.   Firearm Discharge – the "Classification" shall be "Firearm Discharge" and the "Sub-Classifications" shall be Accidental, Animal, Fatal, Injury, or No Hit. The "Firearm Discharge Specific" tab will also ask for miscellaneous statistics and firearm discharge statistics.

2.   Use of Force – the "Use of Force Specific" tab will ask for incident specific information such as the reason for the use of force, weather, lighting, and the service being rendered at the time force was used. Citizen-specific information includes whether the citizen was injured, treated at a hospital, arrested, whether additional suspects were involved, the citizen's condition, the distance from the officer, and the physical characteristics of the suspect involved. The page also asks if the officer was injured or treated at a hospital.

3.   Vehicle Accident - The "Vehicle Accident Specific" tab will ask for the time and cause of the accident, the weather conditions, vehicle information, the amount of damage in dollar figures, whether the employee was at fault, and whether the employee or others were injured.

4.   Vehicle Pursuit - The "Vehicle Pursuit Specific" tab will ask for multiple bits of information that should be taken from the division's Incident and Vehicle Pursuit Reports. Indicate whether an accident occurred and the monetary amount of damage. The person inputting the information must also indicate if the pursuit itself was justified and if the pursuit was conducted within the policy guidelines.

X.   **BlueTeam Entry:**

BlueTeam allows for the entry of incidents and complaints into IAPro by non-OPS personnel. All information entered into BlueTeam must comply with the same entry standards required for IAPro outlined in this General Order.

A.   **Adding A New Incident:**

1.   The following "Incident Types" will be entered into BlueTeam:

      a.   **Investigation of Personnel (IOP), internal, external or anonymous;**
      b.   **Firearms Discharge;**
      c.   **Use of Force;**
      d.   **Constructive Authority (pointing/displaying firearm);**
      e.   **Police Involved Vehicle Collisions;**
      f.   **Vehicle Pursuit;**
      g.   **Non-Disciplinary Action (NDA); and**
      h.   **Any other Incident Types designated.**

2. **All incidents entered into BlueTeam will require an Event Number**. A single Event number can be used to enter multiple BlueTeam entries (i.e. use of force, vehicle pursuit, and vehicle collision, etc..) that occurred during the same incident including any subsequent complaints lodged after the incident.

3. In every case personnel shall attempt to obtain and enter the full details of all involved persons, including witnesses. This includes addresses, telephone numbers, date of birth, race, gender, age, their particular role in the incident (i.e. arrested, driver, passenger, witness, etc…), injuries, and any charges lodged against the citizen.

4. In every case, information about the officer(s) involved, including witness officers, shall be fully documented including the officer's race, age, assignment, any injuries the officer suffered, the types and effectiveness of force used, etc.

5. BlueTeam allows for the attachment of files. All associated documents pertinent to an incident shall be attached, including, but not limited to, the following:

      a.   Any documents related to a complaint;
      b.   Administrative Reports;
      c.   Incident and Arrest reports;
      d.   New Jersey Crash Investigation Reports;
      e.   1005 Investigation Forms;
      f.   Hospital and Medical Reports; and
      g.   any other necessary reports.

6. Photographs, audio recordings, or video recordings shall not be uploaded or saved into BlueTeam at this time; pending the improvement of Division capabilities. These items require large amounts of computer bandwidth to forward via the internet and require large amounts of memory for storage.

    *Photographs, audio, and video recordings shall continue to be saved to a disk.

7. Any URL address of computer files shall be added to each incident when available.

B. **Forwarding of Incidents:**

1. All incidents entered into BlueTeam shall be **forwarded via the chain of command at the time of the incident**. For example, a Use of Force Report shall be submitted at the same time of the Incident Report and Arrest Reports, typically upon the conclusion of the incident.

2.   **Incidents are forwarded to individuals by name** (e.g. Sgt. James Smith) rather than location (e.g. 3rd Precinct Desk Supervisor).

3.   Incidents can be "copied" to other individual(s) as required.

4.   Once forwarded, **the author shall monitor the incident** to ensure the intended recipient has received and processed the incident. This shall be monitored in the "Take Action" column under "Chain Routings You Sent…". **If an incident has not been reviewed in a timely fashion, the sender shall:**

   a.   Send a reminder to the recipient that the incident was forwarded and is awaiting review; or in the event that the original supervisor will be unavailable due to an extended leave, such as illness or vacation, then:

   b.   Retrieve the incident and forward it to another supervisor or commander responsible for the review of the incident.

C.   **Approving and Forwarding Incidents:**

   1.   **Supervisors and Commanders responsible for reviewing and approving incidents shall promptly process all reports and entries prior to the end of their shift.**

   2.   In cases where a supervisor or commander does not approve an incident, it shall be immediately returned to the prior level of review or entry for corrections. Each returned incident shall contain specific instructions on what corrections are expected. **Commanders and Supervisors are responsible for monitoring returned BlueTeam entries.**

   3.   Upon approval, the incident shall be forwarded up the chain of command to the next recipient.

   4.   Upon approval, Commanders shall forward BlueTeam entries to the OPS, incidents involving the **use of force** shall be forwarded to the AFIT.

D.   **IAPro Entry:**

   The OPS shall open and review all incidents forwarded through BlueTeam. Upon review, OPS shall:

   1.   Approve the incident and enter it into IAPro.

   2.   Disapprove the incident and return it to the sender for corrections. Each returned incident shall contain comprehensive instructions on what corrections are expected.

XI.   Early Warning System, (EWS)

The IAPro program is designed to provide a systematic review of select activities, incidents or allegations received or generated by an internal or external source. The intent of the EWS is to ensure that the Division is not faced with a serious case of misconduct that reveals an escalating pattern of behavior that could have been abated through early intervention. The EWS will also identify supervisors whose subordinates have collectively

exceeded threshold levels. These levels are set to ensure that supervisors are properly managing the personnel assigned to them. The EWS will apply to all Police Division employees.

The EWS is administered by the Office of Transparency and Risk Analysis Management and is designed to highlight tendencies in performance, complaints, supervision and other activities. An alert requiring supervisory review under *General Order 10-02, Performance Monitoring* will be generated by the EWS when an employee or supervisor, meets or exceeds established thresholds.

OTRAM shall be responsible for processing and monitoring all data pertinent to alerts from the EWS. OTRAM shall ensure that all alerts are processed in a timely manner and shall monitor the process to ensure that all provisions of the Early Warning System and Performance Monitoring are followed.

A.   **Selection of Performance Indicators**: Consistent with *N.J. Attorney General Directive 2018-3*, the following categories of officer conduct which indicate potentially escalating risk of harm to the public, the agency and/or the officer shall be entered into IAPro for monitoring purposes:

1.   Professional Standards (Internal Affairs) complaints against the officer, whether initiated by another officer or by a member of the public;

2.   Civil actions filed against the officer;

3.   Criminal investigations and/or criminal complaints against the officer;

4.   Any Use of Force by an officer that is formally determined or adjudicated to have been excessive, unjustified or unreasonable. The formal findings may be either criminally or administratively;

5.   Domestic violence investigations in which the officer is an alleged subject;

6.   An arrest of an officer, including driving under the influence;

7.   Sexual Harassment claims against an officer;

8.   Vehicular collisions involving an officer that are formally determined to have been the fault of the officer;

9.   A positive drug test by the officer;

10.   Arrests/Investigations by an officer that are rejected or dismissed by a court;

11.   Cases in which evidence obtained by an officer is suppressed by a court;

12.   Insubordination by the officer;

13.   Neglect of duty by the officer;

14.   Unexcused absences by the officer; and

15.   Any other indicators, as determined by the Chief of Police or Public Safety Director.

B.   **Supplemental Performance Indicators:** Performance Indicators in addition to Section A. The supplemental performance indicators have alternative time frames and/or additional particular conditions for review process triggering purposes.

    1.   2 or more 'Criminal Law allegations' in a 60-month period;

    2.   2 or more Demeanor complaints in a 12-month period;

    3.   2 or more Domestic Violence complaints, (where officer is subject officer) in a 60-month period;

    4.   3 or more Excessive Force complaints in a 12-month period;

    5.   3 or more Firearms Discharges in a 60-month period;

    6.   3 or more police involved motor vehicle collisions in a 60-month period;

    7.   2 or more threats against personnel in a 60-month period;

    8.   5 or more documented Use of Force incidents in a 12-month period;

    9.   8 or more documented Constructive Authority incidents with a firearm in a 12-month period;

    10.   4 or more Vehicle Pursuit incidents in a 12-month period;

    11.   1 sustained complaint of Theft in a 12-month period;

    12.   2 not-sustained or unfounded complaints of theft in a 12-month period;

    13.   1 sustained False Statement or Report in a 12-month period;

    14.   1 sustained complaint concerning missing/lost property or evidence in a 12-month period;

    15.   2 or more "disobedience to orders" – body worn camera violations in a 60-month period;

    16.   2 or more "disobedience to orders' – mobile digital camera violations in a 60-month period.

C.   **Non-Disciplinary Actions:** Generally defined as on-the-spot remedial or corrective actions taken by a supervisor to address **minor** deficiencies or inadequate performance committed by their subordinates.

    1.   3 or more NDA's in a six (6) month period.

XII.   <u>Monitoring</u>

IAPro has a function that allows the electronic monitoring of employees who have been identified as "at risk" for various reasons. While an employee is being monitored, if any additional incidents or complaints are entered involving the monitored employee, a "Monitored Officer Alert" will be generated to notify Professional Standards that another incident involving the employee has been received. Employees may be monitored for one or more of the following reasons:

    A.   Academy Recruit – duration of the academy
    B.   Newly Hired Civilian – 6 months
    C.   Post-Academy Monitoring – 6 months
    D.   Medical Certification (General Order 1994-04 – Sick Leave Policy) – 6 months
    E.   Early Warning System – 6 months

Whenever personnel are being actively monitored by the program, an alert will be generated each time an allegation or incident occurs. Refer to *Performance Monitoring General Order 10-02* for additional details.

XIII.   Reports & Charts

IAPro will produce dozens of pre-programmed reports and multiple pre-programmed charts while analyzing data. The software is capable of exporting data to Microsoft Excel or Microsoft Word for further manipulation and filtering.

XIV.   Training

All newly assigned personnel to the OPS, OTRAM, Advocate Unit, AFIT and the Motor Vehicle Crash Investigative Unit, (MVCIU) shall receive a minimum of four (4) hours of in service training on this general order and the proper use of IAPro prior to being given access to the program. IAPro includes a "Demo" function to allow new users to train and practice with the program without altering data in the Division's live database.

All newly hired sworn police officers and newly promoted police supervisors shall receive a **minimum of 2-hours** of training in the proper use and entry into BlueTeam.

XV.   Audits

The commander of OPS shall be responsible for conducting annual audits of IAPro to ensure that the data entry and use of IAPro complies with the tenets of this general order. Deviations must be strictly prohibited. Any improper use shall be immediately corrected to prevent corruption of the program and to ensure accurate analysis by the software at all times.

XVI.   Effect of this Order

All previous orders and sections of Division Rules & Regulations, General Orders, and Memoranda that are inconsistent with this order are hereby rescinded.

BY ORDER OF

_____
ANTHONY F. AMBROSE
PUBLIC SAFETY DIRECTOR

AFA/BO/jjc
c: Darnell Henry, Chief of Police