CHIEF OF DETECTIVES

NOTICE
1.8

April 17, 2014

TO: All Concerned Personnel

FROM: Chief of Detectives

SUBJECT: LEXISNEXIS/ACCURINT FOR LAW ENFORCEMENT – EXCLUSIVE PUBLIC RECORDS DATA PROVIDER FOR THE LOS ANGELES POLICE DEPARTMENT

The Department has transitioned from the Consolidated Lead Evaluation and Reporting information resource system and contracted with Accurint for Law Enforcement, a service of LexisNexis Risk Solutions, to be the exclusive public records data provider for the Los Angeles Police Department (LAPD). The LexisNexis Accurint for Law Enforcement Plus (Accurint LE Plus) account allows a simultaneous query of multiple public databases via a Department-owned computer. Authorized Department personnel will be able to query and access real-time information from multiple database sources, including person and business locators, telephone sources, assets (e.g., motor vehicles, watercrafts, and aircrafts), nationwide bankruptcies, liens, and judgments, professional licenses, property records, and death records.

The Detective Bureau Coordinator will issue Accurint LE Plus accounts to authorized Department personnel to enhance their ability to rapidly locate suspects and witnesses involved in criminal and Department investigations.

All Accurint LE Plus users are reminded that any information gathered through the Accurint LE Plus accounts must be used in the course and scope of the employee's duties. All authorized users must be aware of the responsibilities for safeguarding the data/information gathered. Department Manual Section 3/405 outlines the Department's policy regarding confidential files, documents, records, and reports. Employees should be aware of pertinent Department Manual Sections, Notices, Orders, and Memorandums, that govern the operation, maintenance, or use of Department-owned computers and/or Department-owned electronic services accounts. Employees should keep in mind that all internet email traffic and inquiries utilizing Department contracted web-based accounts are recorded and subject to audits.

Employees must not perform Department activities outside scheduled work hours without obtaining prior approval from his/her immediate supervisor or Commanding Officer. Department employees shall conform to Fair Labor Standards Act rules and comply with the

Department's procedures to obtain approval for overtime and to report overtime in a timely manner.

The use of LexisNexis Accurint Mobile Application is restricted to Department approved devices. Employees should submit an Intradepartmental Correspondence, Form 15.02.00, to the Chief of Detectives, requesting permission to access Accurint LE Plus for Law Enforcement from any Department-owned device.

If there are any exigent circumstances that require access to LexisNexis from the field, request for information can be made by contacting Real-Time Analysis and Critical Response Division, at (213) 484-6700.

If you have any questions regarding this Notice, please contact Investigative Analysis Section, Detective Bureau, at (213) 486-7010.

APPROVED:

KIRK J. ALBANESE, Deputy Chief
Chief of Detectives

STEPHEN R. JACOBS, Deputy Chief
Chief of Staff
Office of the Chief of Police

DISTRIBUTION "D"

Computer / Electronic Devices Related Investigations

Since the onset of the 21st Century, computer related crimes have increased significantly. Unfortunately, police officers are not immune to becoming involved in these types of crimes. Therefore, investigators need to have a basic understanding as to how to investigate these types of misconduct.

Internet Crime

There have been reported cases of officers committing a variety of crimes via the computer or internet:

- Child pornography.
- Child enticement.
- Fraud (various types).
- Identity Theft/ Impersonation.
- Terrorist/Criminal Threats.
- Sexual Harassment/Retaliation/Discrimination/Hostile Work Environment.

It is against Department policy to use computers connected to the Department LAN for non-business related access to Internet sites, to listen to music, audio material, or to watch video clips.

Standards of Review

Listed below are some of the laws governing the use of computers:

- Federal Electronic Communications Privacy Act (FECPA) 18 United States Code 2510
- Identity Theft: California Penal Code, Section 530.5
- Annoying/threatening communications: California Penal Code, Section 635(m)
- Child Pornography: California PC Section 311
- Computer Data Access and Fraud Act: California PC Section 502
- Searching cellular phones incident to arrest: California v. Diaz, 2011

Social Networking Issues

Social Media websites such as Facebook, Pinterest, Instagram and Twitter have over a billion users worldwide. It is correctly believed that these sites are personal and have some First Amendment protections in the United States. These protections are from certain types of government intrusion or search. Generally, a search warrant is required since protections are in place.

However, today's "friends, girlfriends, boyfriends, husbands, wives" do not always remain so forever. These individuals have captured the information contained on these sites and brought them to the Departments' attention. Any conduct which may tend to reflect unfavorably upon the employee or the Department is unbecoming conduct. This may also apply to information revealed during "blogging."

Additionally, defense attorneys have gained access to these sites and successfully used them against officers in court as impeachment material. Convictions rest on the credibility of the officer(s). *Brady v. Maryland (1963)* states evidence affecting the credibility of the police officer as a witness may be used as exculpatory evidence and shall be given to the defense. Brady issues affect the officers' future ability to testify in court and will therefore impact his/her ability to complete some essential duties.

Case Strategy

The goal is to gather all evidence that proves or disproves the allegation. The more difficult issue associated with this type of investigation is that there are usually few witnesses to the acts. The benefit of this type of investigation is that there is more technological evidence. While investigating a computer related crime, investigators should consider the following:

☐ Use Department experts and resources, such as Commercial Crimes Division, Computer Crimes Unit, Juvenile Division, Cyber Unit, Criminal Investigation Division, and/or Scientific Investigation Division.

☐ Record all results of seizures of computer hard drives, memory, files, photographs, and site content.

☐ Request Information Technology Division (ITD) to conduct checks and results.

Search Warrants

Most internet companies will require a warrant prior to releasing information regarding a client/user. A judge will require prima fascia (evidence) for a crime where the internet or electronic device is a factor prior to issuing a warrant. Generally, there is no issue when conducting criminal investigations. Cellular phones are considered electronic devices under the current definitions of the law. It is illegal to knowingly access without permission or authority, any electronic device data, electronic device system or electronic device network in order to wrongfully control or obtain property, software, or data. However, the same case authorized law enforcement officers to conduct a warrantless search of the contents of a cellular phone incident to arrest, as long as the cellular phone is in the arrestee's immediate control (See California Penal Code, Section 502 and California v. Diaz).

788.30 PROVISIONS FOR THE USE OF PERSONAL COMPUTERS. The Personal Computer Guidelines and Standards contains provisions for the use of personal computers within the Department. This includes computers that are donated, loaned, or purchased by the Department, as well as employee-owned personal computers to the extent that they are used in Department activities. Copies of the guidelines shall be maintained by Information Technology Division.

Employee's Responsibility. Department employees wishing to use employee-owned computers for Department business, at a Department facility, shall submit their request on an Employee's Report, Form 15.07.00 (two copies), to their commanding officer. The Form 15.07.00 shall describe the functions to be performed by the computer and the objectives to be achieved. Upon approval of the request by the employee's commanding officer, the employee shall:

- Adhere to the provisions of the Personal Computer Guidelines and Standards; and,
- Adhere to the provisions of Manual Section 3/405 relating to the confidentiality of Department records, reports, and information when using computers. These provisions apply to the use of computers that are donated, loaned, or purchased by the Department, as well as to employee-owned personal computers used for Department business.

Note: Additional care shall be exercised concerning Department-sensitive data. Department-sensitive data is that data which is not routinely available to the public. Under no condition is Department-sensitive data to be created, stored, processed, or duplicated by employees outside of official Department facilities, without specific **written** permission by the concerned employee's commanding officer. The commanding officer granting such permission shall also ensure that the Department business performed on other than Department-owned personal computers is continuously monitored to ensure compliance with the Personal Computer Guidelines and Standards.

Commanding Officer's Responsibility. Commanding officers shall be responsible for:

- Reviewing requests to use personal computers for Department business within their command;
- Approving or disapproving requests based upon the functions to be performed and the Department objectives to be achieved, within the following general parameters:
- No Department-sensitive data is to be created, stored, processed, or duplicated by users outside of official Department facilities without specific written permission of the concerned commanding officer;
- All software used must be legally acquired and installed;
- If Department sensitive data is stored within a Department entity, access shall be limited to Department employees on a right-to-know, need-to-know basis; and,
- Attention must be directed towards the avoidance of duplication of Department developed and supported systems.
- Forwarding a copy of the approved request to the Department Personal Computer Coordinator;
- Maintaining a copy of the Personal Computer Guidelines and Standards accessible to employees using personal computers; and,
- Ensuring that the Department business performed on such personal computers is continuously monitored and is in compliance with the Personal Computer Guidelines and Standards.

788.40 INTERNET USAGE GUIDELINES. The use of the Internet or e-mail on a Department computer shall be restricted to "official Department business." Personal use of the Department computer or time spent on it for personal gain is prohibited. Violation of any of these guidelines may be considered misconduct and may result in disciplinary action.

These guidelines are applicable to all City or Department-owned or controlled computers, (LAN, Personal Computers and Laptops) and telephone lines. This includes access to computers at sites and facilities that are owned, leased, rented, or utilized by Department employees. Department employees utilizing the Internet or e-mail **shall** cooperate with any investigation regarding the use of computer equipment.

Department employees **shall not**:

- Gain access to or transmit California Law Enforcement Telecommunications System (CLETS) information through the Internet, including secondary dissemination of Criminal History Record information through a communications media such as Internet e-mail facilities and remote access file transfer;
- Conduct an unauthorized attempt or entry into any other computer, known as hacking, which is a violation of the Federal Electronic Communications Privacy Act (FECPA) 18 United States Code 2510;
- Copy or transfer electronic files without permission from the copyright owner;
- Send, post, or provide access to any confidential Department materials or information;
- Send private or confidential e-mail as delineated in Manual Section 4/105.15;
- Transmit chain letters;
- Send threatening, slanderous, offensive, racially and/or sexually harassing messages; and,
- Represent oneself as someone else, real or fictional, or send messages anonymously.

Note: Use of the Internet for certain investigations may require a deviation from the Internet guidelines. This could include the use of offensive language, impersonation, or use of an alias, and the accessing or downloading of offensive or explicit material. Department personnel must submit an Employee's Report, Form 15.07.00, and obtain approval from his/her commanding officer prior to engaging in such conduct. The Employee's Report must be filed in the employee's divisional package. When conducting a Department authorized investigation that requires these tactics for investigative purposes, they are not considered misconduct.

In addition to these general guidelines, employees utilizing the Internet are advised that the Department has the right to access all e-mail files created, received, or stored on Department systems, and such files can be accessed without prior notification.

216.01 INTERNET/ELECTRONIC MAIL (E-MAIL) USAGE GUIDELINES

The use of the Internet or e-mail on a Department computer shall be restricted to "official Department business. Personal use of, or time spent for personal gain is prohibited. Violation of any of these guidelines may be considered misconduct and may result in disciplinary action.

The guidelines are applicable to all City or Department-owned or controlled computers, (LAN, Personal Computers and Laptops) and telephone lines. This includes access to computers at sites and facilities that are owned, leased, rented, or utilized by Department employees.

Department employees utilizing the Internet or e-mail shall cooperate with any investigation regarding the use of computer equipment.

Department employees shall not:

- Gain access to or transmit California Law Enforcement Telecommunications system (CLETS) information through the Internet, including secondary dissemination of Criminal history Record information through a communications media such as Internet email facilities and remote access file transfer;
- Conduct an unauthorized attempt or entry into any other computer, known as hacking, which is a violation of the Federal electronic communications Privacy Act (FECPA) 18 United States Code 2510;
- Copy or transfer electronic files without permission from the copyright owner;
- Send, post, or provide access to any confidential Department materials or information;
- Send private or confidential e-mail as delineated in Department Manual Section 4/105.15;
- Transmit chain letters;
- Send threatening, slanderous, offensive, racially and/or sexually harassing messages; and,
- Represent oneself as someone else, real or fictional, or send messages anonymously.

Note: Use of the Internet for certain investigations may require a deviation from the Internet guidelines. This could include the use of offensive language, impersonation, or use of an alias, and the accessing or downloading of offensive or explicit material. When conducting a Department authorized investigation that requires these tactics for investigative purposes, they are not considered misconduct.

In addition to these general guidelines, employees utilizing the Internet are advised that the Department has the right to access all email files created, received, or stored on Department systems, and such files can be accessed without prior notification. (Department Manual Section 3/788.40)

OFFICE OF THE CHIEF OF POLICE

ADMINISTRATIVE ORDER NO. 3 March 18, 2016

SUBJECT: **SCIENTIFIC INVESTIGATION DIVISION – DEACTIVATED; TECHNICAL INVESTIGATION DIVISION – ACTIVATED; FORENSIC SCIENCE DIVISION – ACTIVATED; REAL-TIME ANALYSIS AND CRITICAL RESPONSE DIVISION BIFURCATED FROM THE COMPSTAT FUNCTION; COMPSTAT DIVISION – ACTIVATED; AND, CATEGORICAL USE OF FORCE – NOTIFICATIONS - REVISED**

PURPOSE: This Order deactivates Scientific Investigation Division (SID) and reorganizes it into two divisions, Technical Investigation Division (TID) and Forensic Science Division (FSD). Real-Time Analysis and Critical Response (RACR) Division has also been reconfigured to bifurcate the Computer Statistics (COMPSTAT) function into a separate division.

PROCEDURE:

I. **SCIENTIFIC INVESTIGATION DIVISION – DEACTIVATED.** Scientific Investigation Division has been deactivated.

II. **TECHNICAL INVESTIGATION DIVISION – ACTIVATED.** Technical Investigation Division has been activated. The TID organization and functions are attached. Technical Investigation Division shall use the correspondence reference number 8.5. The radio unit designation for TID staff shall be 2H.

III. **FORENSIC SCIENCE DIVISION – ACTIVATED.** Forensic Science Division has been activated. The FSD organization and functions are attached. Forensic Science Division shall use the correspondence reference number 8.9. The radio unit designation for FSD staff shall be 6H.

IV. **REAL-TIME ANALYSIS AND CRITICAL RESPONSE DIVISION BIFURCATED FROM THE COMPSTAT FUNCTION.** Real-Time Analysis and Critical Response Division has been bifurcated from COMPSTAT to form two separate divisions. The correspondence reference number and the radio unit designation for RACR Division remain unchanged.

V. **COMPSTAT DIVISION – ACTIVATED.** The COMPSTAT Division has been activated. The COMPSTAT organization and functions are attached. The COMPSTAT Division shall use the correspondence reference number 3.8. The radio unit designation for COMPSTAT staff shall be 28H.

VI. **CATEGORICAL USE OF FORCE – NOTIFICATIONS – REVISED.** Department Manual Section 3/794.35, subheading, *Real-Time Analysis and Critical Response Division* has been revised. The 20-minute notification required of RACR upon learning that a Categorical Use of Force incident has occurred has been revised. Attached is the revised Manual Section with the revisions indicated in italics.

AMENDMENTS: This Order amends Section 3/794.35, and various other sections of the Department Manual. The Organization Chart and the Organization and Functions of the Los Angeles Police Department links on the Department's Local Area Network and LAPD Forms will be updated accordingly to reflect the above changes.

AUDIT RESPONSIBILITY: The Commanding Officer, Audit Division, shall review this directive and determine whether an audit or inspection shall be conducted in accordance with Department Manual Section 0/080.30.

CHARLIE BECK
Chief of Police

Attachments

DISTRIBUTION "D"

794.35 CATEGORICAL USE OF FORCE – NOTIFICATIONS. Notification responsibilities after a CUOF are established as follows:

Area Watch Commander/Incident Commander. The Area watch commander/Incident Commander *shall make* the following notifications within 30 minutes of learning that a CUOF incident has occurred:

- Real-Time Analysis and Critical Response *(RACR)* Division ;
- Area commanding officer of the Area of occurrence; and,
- Bureau commanding officer of the Area of occurrence.

Note: In such instances where the notification is beyond the 30 minutes, the justification *shall* be documented in the Watch Commanders Daily Report, Form 15.80.00.

Real Time Analysis and Critical Response Division. Real-Time Analysis and Critical Response Division *shall make* the following notifications within *15* minutes of being notified by the Area watch commander/Incident Commander that a CUOF incident has occurred:

- Office of the Chief of Police or his designee;
- Chief of Staff;
- *Force Investigation Division (FID) or FID on-call team during non-business hours; and,*
- Office of the Inspector General (OIG).

Additional Notifications Requirements. As soon as possible after *the initial required notifications*, RACR *shall* make notifications to the following entities:

- Commanding Officer, Professional Standards Bureau;
- Involved employee(s) commanding officer;
- Department Risk Manager; and,
- Los Angeles District Attorney's Office for those cases identified in the roll out protocol governing such notifications.

TECHNICAL INVESTIGATION DIVISION.

TECHNICAL INVESTIGATION DIVISION - FUNCTIONS. Technical Investigation Division (TID) has Citywide jurisdiction and is responsible for:

- Providing photographic services, including general investigative photography;
- Developing, collecting and analyzing latent print evidence;
- Functionally supervising the mechanical or technical aspects of electronic surveillance equipment usage within the Department;
- Storing Departmental recorded audio and video media, excluding Body Worn Video (BWV) and Digital In-Car Video (DICV) recordings;
- Issuing, installing, removing, and maintaining electronic investigation equipment;
- Administering forensic polygraph examinations to support the hiring process and criminal investigations;
- Operating polygraph equipment, conducting interviews, and instructing Department employees as to the proper methods for preparing persons to be interviewed or interrogated; and,
- Providing instruction for Department personnel in the current methods used by TID.

TECHNICAL INVESTIGATION DIVISION – ORGANIZATION. Technical Investigation Division is composed of:

- Office of the Commanding Officer;
- Photographic Unit;
- Latent Print Unit;
- Electronics Unit; and,
- Polygraph Unit.

COMMANDING OFFICER, TECHNICAL INVESTIGATION DIVISION. The Commanding Officer (CO), TID, under the direction of the Chief of Detectives, exercises line command over the operations of TID.

COMMANDING OFFICER, TECHNICAL INVESTIGATION DIVISION – SPECIAL DUTIES. The CO, TID, is responsible for processing and approving requests from other law enforcement agencies for TID's services.

TECHNICAL INVESTIGATION DIVISION, PHOTOGRAPHIC UNIT.

PHOTOGRAPHIC UNIT - FUNCTIONS. The Photographic Unit is responsible for all photographic work in relation to the following:

- Crime scenes;
- Evidence;
- Dead bodies;
- Aerial Photography;
- Forensic Photography including electrostatic dust lifts, alternate light source photography, photomicrography, and macrophotography;
- Arrestees claiming injuries involved in Uses of Force, or for line-ups;
- Victims;

- Department employees (except employee ID photos, which are captured by Personnel Division);
- Photographic documentation of latent evidence;
- Photographic prints, copies, and enlargements, as required; and,
- Surveillance photography of gang funerals.

PHOTOGRAPHIC UNIT - SPECIAL DUTIES. The Photographic Unit is responsible for the following special duties:

- **Digital Imaging.** Maintaining digital image files; and,
- **Evidence.** Retention/Archiving of all photographic evidence.

TECHNICAL INVESTIGATION DIVISION, LATENT PRINT UNIT.

LATENT PRINT UNIT - FUNCTIONS. The Latent Print Unit is responsible for:

- Investigating crime scenes for latent print evidence;
- Chemical processing of requested evidence for latent prints;
- Photographic documentation of alternate light source and chemically enhanced latent prints;
- Automated Fingerprint Identification System (AFIS) latent print inquiries;
- Comparison of suspects' prints with latent prints obtained at crime scenes;
- Taking plaster casts of shoe and tire impressions; and,
- Maintaining files of latent prints obtained at crime scenes and palm print cards of arrested persons.

TECHNICAL INVESTIGATION DIVISION, ELECTRONICS UNIT.

ELECTRONICS UNIT - FUNCTIONS. The Electronics Unit is responsible for:

- Installing, removing and operating covert electronic investigation equipment;
- Temporary issuance of electronic investigation equipment to other divisions;
- Storing Departmental recorded audio and video media, excluding BWV and DICV recordings;
- Providing forensic examination services for audio, video, and small scale digital devices such as cell phones, tablets and digital video recorders (DVRs) for Department entities and City government;
- Providing electronic countermeasure sweeps (debugging) for Department entities and City government;
- Maintaining audio and video equipment in Department interview rooms;
- Crime scene video retrieval assistance; and,
- Digital media duplication.

ELECTRONICS UNIT - SPECIAL DUTIES. The Electronics Unit is responsible for the following special duties:

Construction of Special Equipment. Designing, constructing, and modifying covert electronic investigation equipment.

Special Files. Maintaining a file of information pertaining to electronic investigation equipment issued or installed by the Electronics Unit.

Special Logs. Maintaining special logs of:

- Audio and video recordings made throughout the Department, excluding BWV and DICV; and,
- Electronic equipment borrowed from the Electronics Unit.

TECHNICAL INVESTIGATION DIVISION, POLYGRAPH UNIT.

POLYGRAPH UNIT - FUNCTIONS. The Polygraph Unit is responsible for:

- Evaluating credibility assessment techniques and technology;
- Operating all credibility assessment equipment;
- Instructing interview and interrogation techniques to Department personnel;
- Providing training for Department employees regarding the effective use of polygraph as an investigative tool; and,
- Administering the following types of polygraph examinations:

    - Police candidate testing for the Personnel Department;
    - Los Angeles Fire Department firefighters testing for Personnel Department, seeking assignments as arson investigators;
    - Internal screening for sworn and civilian employees seeking assignments to specialized units;
    - Criminal examinations of suspects and/or witnesses, including those requiring travel to off-site locations; and,
    - Courtesy polygraph examinations for City, and other law enforcement agencies.

ORGANIZATION AND FUNCTIONS OF THE LAPD
Revised By Administrative Order No. 3, 2016

FORENSIC SCIENCE DIVISION.

FORENSIC SCIENCE DIVISION - FUNCTIONS. Forensic Science Division (FSD) has Citywide jurisdiction and is responsible for:

- Analyzing physical evidence;
- Photographing all narcotics evidence;
- Maintaining liaison with the Superior and Municipal Courts to ensure that the Department's procedure for photographing narcotics evidence continues to be in compliance with the courts' standards;
- Performing the court-ordered split or sample selection for the release of evidence samples for private laboratory analysis;
- Surveying crime locations;
- Rendering safe black powder firearms and other firearms unfamiliar to booking officers;
- Providing firearm evidence identification;
- Performing bullet path analysis at the scene of shootings where trajectories and positioning is probative to the investigation;
- Performing forensic photography, including electrostatic dust lifts, infrared photography, photomicrography, and macrophotography;
- Examining questioned documents;
- Providing expert testimony pertaining to laboratory analysis and field investigations;
- Maintaining liaison with commercial and law enforcement organizations to support forensic database systems;
- Maintaining field alcohol breath testing equipment;
- Performing analysis of samples from the Department's random (and for cause) Employee Drug Testing Program;
- Obtaining casts or photographs of marks or tracks;
- Handling of hazardous chemicals;
- Providing six and twelve month Evidence Drying Cabinet (EDC) filter maintenance;
- Ensuring cleaning solution is made available to all geographic Areas;
- Maintaining liaison with Facilities Management Division for repairs to the EDCs;
- Processing crime scenes for physical evidence as needed;
- Providing instruction for Department personnel in the current methods used by FSD;
- Assisting officers with nitrous oxide investigations;
- Transporting the seized nitrous oxide tank or cylinder to the commercialized warehouse; and,
- Obtaining and analyzing a sample of nitrous oxide from a cylinder or balloon.

FORENSIC SCIENCE DIVISION - ORGANIZATION. Forensic Science Division is composed of:

- Administrative Unit; and,
- Criminalistics Laboratory.

COMMANDING OFFICER, FORENSIC SCIENCE DIVISION. The CO, FSD, under the direction of the Chief of Detectives, exercises line command over the operations of FSD.

COMMANDING OFFICER, FORENSIC SCIENCE DIVISION - SPECIAL DUTIES. The CO, FSD, is responsible for processing and approving requests from other law enforcement agencies for FSD's services.

FORENSIC SCIENCE DIVISION, CRIMINALISTICS LABORATORY.

CRIMINALISTICS LABORATORY - FUNCTIONS. The Criminalistics Laboratory is comprised of the following:

Toxicology Unit.

The Alcohol Analysis Detail. The Alcohol Analysis Detail is responsible for:

- Analysis of breath, blood, urine, and beverages for ethyl ("beverage") alcohol;
- Providing instruction to operators in the use of approved alcohol breath testing equipment;
- Maintenance, repair, calibration, and accuracy checking of approved breath testing equipment;
- Expert testimony in local courts regarding alcohol's impairing effects on the driving task; and,
- Expert testimony in local courts and DMV Driver Safety offices in support of the Unit's approved breath testing instruments, and blood, urine and beverage alcohol analysis procedures.

The Toxicology Unit Drug Detail. The Toxicology Unit Drug Detail is responsible for testing blood and urine samples for:

- Under the influence of controlled substance;
- Driving under the influence of drugs;
- Random and "for cause" employee samples; and,
- Drug facilitated sexual assaults.

Field Investigation Unit. The Field Investigation Unit is responsible for:

- Preservation, collection and booking of evidence from major crime scenes; and,
- Making surveys at the scenes of major crimes and preparing maps or sketches as required.

Firearms Analysis Unit. The Firearms Analysis Unit is responsible for:

- Investigating crime scenes for firearm evidence and trajectories;
- Physical examination of requested evidence (fired ammunition components) to determine type and caliber(s) of involved firearms;
- National Integrated Ballistics Information Network (NIBIN) entries and inquiries;
- Microscopic comparison of fired cartridge components and test fired specimens;
- Physical examination and identification of fixed ammunition and ammunition components, .50 caliber and less;
- Examination of evidence for gunpowder residues in estimating muzzle to target intervals;
- Re-stamping serial numbers on firearms for official use or custodial release;

- Examination of evidence firearms for classification as California Assault Weapons;
- Examination of evidence firearms for classification as fully automatic firearms;
- Examination of evidence devices for classification as firearms;
- Examination of evidence devices for classification as silencers (sound suppressors);
- Examination of evidence firearms for classification as short-barreled rifles or shotguns;
- Test-firing and specimen imaging of booked firearms suitable for NIBIN entry;
- Test fire of booked and unbooked firearms for scientific investigation; and,
- Retention of firearms and components commonly encountered in police investigations.

Note: These are used for court demonstration, training and other police investigations.

Narcotics Analysis Unit. The Narcotics Analysis Unit is responsible for:

- Photographing narcotics evidence for court;
- Examination of physical evidence for controlled substances;
- Split narcotic samples for independent analysis; and,
- Advising officers on proper procedures for booking narcotics evidence.

Quality Assurance/Quality Control Unit. The Quality Assurance/Quality Control Unit is responsible for:

- Monitoring laboratory practices to assure compliance with accreditation standards established by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB);
- Managing the Quality System;
- Coordinating Training; and,
- Overseeing the Safety Program.

Questioned Documents Unit. The Questioned Documents Unit is responsible for examining all document evidence, in particular:

- Handwriting, hand printing, signatures;
- Indented writing;
- Typewriting;
- Office machine classification and identification;
- Hand stamps;
- Printing methods;
- Fracture matches;
- Alterations, and obliterations; and,
- Obtaining handwriting samples from suspected writers for comparison.

Serology/DNA Unit. The Serology/DNA Unit is responsible for:

- Analyzing evidence for the presence of body fluids, including blood, semen and saliva;
- Determining the DNA types (profiles) present in body fluids and on evidence items;
- Combined DNA Index System (CODIS) DNA profile uploads and inquiries; and,
- Comparison of DNA profiles from crime scenes with suspects and victims.

Trace Analysis Unit. The Trace Analysis Unit is responsible for the analysis and/or comparison of various types of physical evidence including:

- Hairs;
- Fibers;
- Gunshot residue from hands;
- Arson residue and ignitable liquids;
- Explosives;
- Shoeprints and tire tracks;
- Toolmarks;
- Physical/fracture matches;
- Tape; and,
- Other miscellaneous chemical and physical evidence.

CRIMINALISTICS LABORATORY - SPECIAL DUTIES. The Criminalistics Laboratory is responsible for the following special duties:

Hazardous Chemicals. Arranging for the disposal of hazardous materials and providing on-scene determination of the dangers posed by hazardous chemicals, implementing safeguards relative to its handling, and obtaining samples of each chemical, if conditions permit.

Large Seizures of Controlled Substances. Provide sampling, weighing, and packaging of seized controlled substances in excess of 30 pounds net weight, which are to be booked into Department facilities.

Nitrous Oxide. Transporting and providing samples of nitrous oxide from cylinders or balloons for analysis.

Black Powder and Other Dangerous or Damaged Firearms. Safe unloading of black powder weapons, damaged or corroded firearms and other firearms that are too dangerous or unfamiliar to Department employees.

Officer-Involved Shootings. Forensic support of Officer-Involved Shooting investigations, in the field and laboratory, sufficient to satisfy the Department's review process.

ORGANIZATION AND FUNCTIONS OF THE LAPD
Revised By Administrative Order No. 3, 2016

OFFICE OF ADMINISTRATIVE SERVICES, REAL-TIME ANALYSIS AND CRITICAL RESPONSE DIVISION

REAL-TIME ANALYSIS AND CRITICAL RESPONSE DIVISION - ORGANIZATION. Real-Time Analysis and Critical Response (RACR) Division is comprised of:

- Department Operations Center (DOC) Unit; and,
- Regional Crime Center Unit.

COMMANDING OFFICER, REAL-TIME ANALYSIS AND CRITICAL RESPONSE DIVISION. The Commanding Officer (CO), RACR, under the direction of the Director, Office of Administrative Services, exercises line command over the operations of RACR Division.

REAL-TIME ANALYSIS AND CRITICAL RESPONSE DIVISION - FUNCTIONS. Real-Time Analysis and Critical Response Division is responsible for the following:

Department Operations Center Unit.

- Activating the DOC during a major occurrence or when a major occurrence appears imminent;
- Training personnel for the DOC operations;
- Planning and developing DOC systems and procedures;
- Coordinating and organizing deployment plans for major unusual occurrences;
- Maintaining and providing expertise to the Police DOC;
- Preparing and coordinating requests for resources [Size, Activity, Location, Units, Time and Equipment (SALUTE)] for the DOC ; and,
- Maintaining a link between field operations and the DOC.

Regional Crime Center Unit.

- Monitoring Citywide Department radio frequencies for critical incidents such as homicides, shootings and other major calls for service.
- Making notification as needed for the following:

    - Officer-Involved Shootings;
    - All uses of an upper body control, including the use of a modified carotid or locked carotid hold;
    - In-custody deaths;
    - A use of force incident resulting in death or injury requiring hospitalization (LERI);
    - An incident in which a member of the public is bitten by a Department canine and hospitalization is required;
    - Negligent discharge of a firearm by a sworn member of the Department;
    - Animal shootings;
    - Incidents where the Department has agreed to conduct similar critical incident investigations for a non-Department entity;
    - Barricaded suspects or SWAT Call-Outs;
    - Bomb Squad Call-Outs;

- Demonstrations or mass arrests;
- Pursuits;
- Disasters;
- Chemical spills/gas main leaks or breaks;
- Red Flag Alerts;
- Incidents Involving hazardous, toxic or radioactive materials;
- Tactical Alerts;
- Change in the federal terrorism threat level (up or down);
- Major fires;
- Homicides;
- Commercial Robberies;
- Take-Over Robberies;
- Hot Prowl Burglaries;
- Stranger Rapes;
- Incidents motivated by hatred/prejudice;
- Fatal traffic collisions;
- Traffic collisions involving multiple victims with serious injuries;
- Traffic collisions involving children under fifteen years of age with serious injuries;
- Aircraft accidents;
- Incidents involving celebrities or dignitaries;
- Newsworthy incidents involving the Department ;
- CARE/AMBER Alerts, Blue Alerts and Silver Alerts;
- Critical missing persons investigations;
- Incident Command Post activations at the scene of a noteworthy or newsworthy incident;
- Requests for Crisis Response Team; and,
- Local, National, and Global events that could impact the City of Los Angeles.

Notable Notification after a Categorical Use of Force.

Within 15 minutes of a RACR notification by the Area Watch Commander or Incident Commander, RACR must contact (Department Manual Section 3/794.35):

- Office of the Chief of Police or his designee;
- Chief of Staff;
- Force Investigation Division (FID) or FID on-call team during non-business hours; and,
- Office of the Inspector General (OIG).

As soon as possible after the initial required notifications, RACR is responsible for making notifications to the following entities:

- Commanding Officer, Professional Standards Bureau;
- Involved employee(s) commanding officer;
- Department Risk Manager; and,

- Los Angeles District Attorney's Office for those cases identified in the roll out protocol governing such notifications.

Regional Crime Center Unit Support Functions.

- Providing after hour investigative information, advice and assistance to officers investigating calls for service, when the following units or functions of Detective Bureau are closed:
  - Missing Persons Unit;
  - Mental Evaluation Unit;
  - Juvenile Division;

- Providing after hour investigative support and booking assistance to officers and specialized units;
- Reviewing and transporting Probable Cause Declarations (PCDs) for all 21 Areas to the court on weekends and holidays when the court is open for PCD hearings;
- Providing information normally obtained from Personnel Division when that division is closed;
- Providing information obtained from telephone numbers when Detective Support and Vice Division is closed;
- Using Department resources to complete database research to assist in identifying the victim(s), suspect(s) or background information on the crime location;
- Receiving and forwarding information obtained on the toll free tip line (877-LAPD 24/7, Crimestoppers, iWatch, and 1-800-A-Threat) to the appropriate investigative entity;
- Monitoring, receiving and forwarding internet tips through TipSoft;
- Monitoring and collecting data from social media and internet sites for planned and unplanned protests, rallies, and marches that could impact the City;
- Responding to outside entity requests for analysis, research and data mining;
- Maintaining a liaison with California State Parole, Bureau of Alcohol, Tobacco, Firearms and Explosives, FBI and County Probation; and,
- Upon request from Robbery-Homicide Division (RHD), contact the California Highway Patrol's Emergency Notification and Tactical Alert Center to initiate a Blue Alert, coordinate alert information with LAPD Communications Division for the broadcast and cancellation of CARE/AMBER, Silver or Blue Alerts.

REAL-TIME ANALYSIS AND CRITICAL RESPONSE DIVISION – SPECIAL DUTIES. Real-Time Analysis and Critical Response Division is responsible for the following special duties:

Reference Data. Maintaining reference data of the following:

- Fiscal Operations Division-Travel and Per Diem Guidelines;
- Emergency Operations Master Plan and Procedures Manual;
- National Directory of Law Enforcement Administrators;

- Call codes of chiefs of police and sheriffs, prosecutors, and penal institutions;
- List of names, official titles, addresses of government officials and special locations;
- Directory of the State Board of Medical Examiners;
- Directory of the State Board of Osteopathic Examiners;
- Chief Special Agents Association, Inc.,
- Directory of police and government agencies in the State, including selected local public and private enterprises;
- Department and Emergency Operations Guide; and,
- U.S., Penal, Vehicle, and Municipal Codes.

Special Logs. Maintaining logs of the following:

- Security Inspections;
- Booking advice;
- Requests for assistance by outside agencies;
- Officers visiting from outside jurisdictions;
- Out-of-county vehicle trips;
- Mileage use; and,
- Collect telephone calls.

Special Files. Maintaining files of the following:

- Writ teletypes;
- Emergency Investigative Travel Fund;
- Emergency Witness Relocation Fund; and,
- Legal Information.

Emergency Investigative Travel Fund.

- Maintaining and disbursing money from the Emergency Investigative Travel Fund; and,
- Providing a copy of the Fiscal Operations Division-Travel and Per Diem Guidelines to each Department employee going on emergency investigative travel for the Department.

Emergency Witness Relocation Fund.

- Maintaining and disbursing money from the Emergency Witness Relocation Fund; and,
- Providing a copy of the Fiscal Operations Division-request for immediate disbursement of California Witness Relocation and Assistance Program funds to the concerned Department employee.

ORGANIZATION AND FUNCTIONS OF THE LAPD
Revised By Administrative Order No. 3, 2016

COMPSTAT DIVISION - FUNCTIONS. Computer Statistics (COMPSTAT) is the Department's command accountability inspection process. The COMPSTAT Division reports directly to the Director, Office of Administrative Services (OAS). The COMPSTAT Division is responsible for:

- Developing, implementing, and evaluating the crime analysis systems/processes, utilized throughout the Department;
- Providing ongoing support, product development, and training to bureau, Area, and Divisional Crime Analysis Details (CADs);
- Assisting the CADs in coordinating timely and accurate crime analysis information in support of line operations;
- Monitoring and auditing the production and dissemination of all crime analysis products relating to crime series, patterns, hot spots, trends, clusters, spikes and/or offenders, for the purpose of identifying, arresting and prosecuting criminals;
- Directing the CADs and providing the necessary information to ensure readiness of coded crime, traffic, personnel and other risk management data for downloading and analysis on a daily basis;
- Analyzing bureau, Area, and Citywide crime, arrest and traffic data in order to identify series, patterns, hot spots, trends, clusters, spikes, and victim/offender information for the weekly COMPSTAT meeting;
- Conducting inspections, analyses and special COMPSTAT/crime analysis-related projects as directed by the Director, OAS, and other Department command staff;
- Preparing information and the electronic media used for data presentation for the Director, OAS, as required for the weekly COMPSTAT meeting;
- Preparing all applicable maps, charts, graphs, reports and other products needed at the weekly Situation Room briefing with the COP;
- Analyzing all homicides Citywide and producing daily reports of any changes; and,
- Providing training to Department personnel on the proper classification of crimes in accordance with the Uniform Crime Reporting (UCR) Guidelines, conducting inspections of crime classifications and acting as the Department's UCR coordinator with the California Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).

COMPSTAT DIVISION – ORGANIZATION. COMPSTAT Division is comprised of:

- Office of the Commanding Officer;
- Applications and Initiatives Unit;
- Support Unit;
- Data Integrity Unit; and,
- Special Projects Unit.

COMMANDING OFFICER, COMPSTAT DIVISION. The Commanding Officer, COMPSTAT Division, under the direction of the Director, OAS, exercises line command over the operations of COMPSTAT Division and functional supervision and support for all CAD personnel Department-wide.

APPLICATIONS AND INITIATIVES UNIT – FUNCTIONS. The Applications and Initiatives Unit is responsible for the following:

- Maintaining liaison with and support of the COMPSTAT Division, Support Unit. This includes the preparation of maps, charts, graphs, heat maps and other products needed for the weekly COMPSTAT meeting;
- Preparing crime inspection recommendations for weekly COMPSTAT meetings;
- Providing PALANTIR training and support;
- Preparing Predictive Policing reports weekly;
- Preparing the Los Angeles Strategic Extraction and Restoration (LASER) reports weekly; and,
- Preparing monthly Law Enforcement Officers Killed and Assaulted (LEOKA) report for California DOJ.

SUPPORT UNIT - FUNCTIONS. The Support Unit is responsible for the following:

- Gathering, compiling, and presenting crime, arrest, risk management and other statistical information at the Chief of Police weekly information-sharing COMPSTAT meeting. Essential elements used to present this information are the Profiles and crime and arrest maps;
- Preparing and maintaining of the following profiles: Citywide; geographic Areas; geographic bureaus; Citywide Traffic, Traffic Divisions and several specialized divisions and bureaus;
- Using a myriad of tools and over 36 reports to collect the information for the profiles, crime maps, charts, and graphs presented via audio-visual mediums at the weekly COMPSTAT meetings; and,
- Assisting commands in developing reports to capture parameters for measures of effectiveness of operational needs upon request.

DATA INTEGRITY UNIT – FUNCTIONS. The Data Integrity Unit is responsible for the following:

- The Data Integrity Unit's Officer in Charge is the Department's Uniform Crime Reporting (UCR) Coordinator and is the liaison and point of contact with/between Department personnel, the California DOJ and the Federal Bureau of Investigation (FBI) for all UCR crime classification related questions/concerns/issues;
- Providing UCR training to all applicable Department personnel on an ongoing basis;
- Conducting routine inspections of the Department's classification of crime for all 21 geographic Areas and specialized divisions in an effort to ensure that the crime coding of records is being conducted in compliance with UCR guidelines;
- Maintaining/updating the UCR Decision Trees, Frequently Asked Questions and other related training products and makes them available on the COMPSTAT Division website; and,
- Maintaining liaison with the Office of Operations and the geographic bureaus for all UCR related issues and coordinates with the Bureau Assessor teams on their weekly inspections of crime classifications for their respective bureaus.

SPECIAL PROJECTS UNIT – FUNCTIONS. The Special Projects Unit is responsible for the following:

- Maintaining liaison with and support of the COMPSTAT Division, Support Unit. This includes the preparation of maps, charts, graphs, heat maps and other products needed for the weekly COMPSTAT meeting;
- Acting as the Division's webmaster, posting all applicable reports, graphs, charts, profiles, etc., onto the COMPSTAT Division website weekly;
- Maintaining the COMPSTAT Division Dropbox;
- Producing ad hoc reports, maps, charts, graphs, etc., on a routine basis for the Chief of Police, all Department Command Staff, the Mayor's Office, the City Attorney's Office, the City Controller's Office and all City Council Offices as needed;
- Coordinating with Information Technology Bureau's Application Development and Support Division personnel on a weekly basis regarding the classification of crimes;
- Providing Crime Analysis Mapping System (CAMS) training on an as-needed basis to all applicable Crime Analysis Detail (CAD) personnel; and,
- Preparing crime statistic reports on a daily basis for all applicable command staff.

SPECIAL LIAISON. The COMPSTAT Division is responsible for maintaining liaison with:

- Information Technology Division to coordinate the installation, maintenance and servicing of COMPSTAT and Crime Analysis Detail computer equipment and software;
- Application Development and Support Division to coordinate support for the Department's CAMS and statistical reports needed for the COMPSTAT process; and,
- Information Technology Bureau and Information Technology Agency to coordinate the integration and compatibility of crime analysis computer systems with other related Department and City software and hardware systems.

OFFICE OF THE CHIEF OF POLICE

ADMINISTRATIVE ORDER NO. 2 March 16, 2016

SUBJECT: **COMMUNITY RELATIONS SECTION – DEACTIVATED; COMMUNITY POLICING UNIT – DEACTIVATED; AND, COMMUNITY RELATIONSHIP DIVISION – ACTIVATED**

PURPOSE: This Order deactivates Community Relations Section (CRS), formerly assigned to the Office of the Chief of Police, and deactivates the Community Policing Unit (CPU), formerly under the command of the Assistant to the Director, Office of Operations (OO). This Order also activates the Community Relationship Division (CRD), under the command of the Director, Office of Constitutional Policing and Policy.

The CRD seeks to build relationships and trust between the Department and the diverse communities in the City of Los Angeles. To achieve this, the CRD will leverage best practices in community outreach, police-community relations, and cutting-edge digital media technologies. The CRD will ensure outreach efforts are consistent by partnering with Area Community Relations Offices. In addition, seven-day digital media support will be maintained and coordinated with Media Relations Section to ensure consistent messaging, and eliminate redundancy. By combining community outreach specific to each geographical Area, and a commitment to digital and social media, the CRD will build and develop relationships with community stakeholders to foster trust and mutual understanding.

PROCEDURE:

I. **COMMUNITY RELATIONS SECTION – DEACTIVATED.** The CRS has been deactivated.

II. **COMMUNITY POLICING UNIT – DEACTIVATED.** The CPU has been deactivated.

III. **COMMUNITY RELATIONSHIP DIVISION – ACTIVATED.** The CRD has been activated. The CRD functions are attached. Community Relationship Division shall use the correspondence reference number 14.7 and personnel assigned to CRD shall use the radio unit designation 13I.

AMENDMENTS: This Order amends various Department Manual sections pertaining to this reorganization. The Organization Chart and the Organization and Functions of the Los Angeles Police Department links on the Department's Local Area Network will be updated accordingly to reflect the above changes.

AUDIT RESPONSIBILITY: The Commanding Officer, Audit Division, shall review this directive and determine whether an audit or inspection shall be conducted in accordance with Department Manual Section 0/080.30.

CHARLIE BECK
Chief of Police

Attachment

DISTRIBUTION "D"

ORGANIZATIONS AND FUNCTIONS OF THE LOS ANGELES POLICE DEPARTMENT

COMMUNITY RELATIONSHIP DIVISION.

COMMUNITY RELATIONSHIP DIVISION – ORGANIZATION. Community Relationship Division is comprised of:

- Office of the Commanding Officer;
- Community Relationship Section;
- Community Engagement Unit;
- Crime Prevention & Digital Media Section; and,
- Training/Special Projects Unit.

COMMANDING OFFICER, COMMUNITY RELATIONSHIP DIVISION. The Commanding Officer, Community Relationship Division, under the direction of the Director, Office of Constitutional Policing and Policy, exercises line command over the operations of the Community Relationship Division.

COMMUNITY RELATIONSHIP DIVISION - FUNCTIONS. Community Relationship Division is responsible for:

- Developing and promoting community relations programs designed to foster mutual trust and respect between the Department and the community;
- Identifying and evaluating areas of tension in the community and rumors from within the community and the Department;
- Maintaining liaison with international, national, state, and Citywide organizations;
- Providing, upon request, expertise to assist the Department in alleviating specific police community relations tensions;
- Reviewing and evaluating the Department's community relations training and developing recommendations when needed;
- Assisting geographic Area commanding officers with community relations solutions during unusual incidents;
- Providing, on behalf of the Chief of Police, liaison for visiting dignitaries;
- Representing the Department in a community relations capacity while serving on panels, seminars, workshops, institutes, etc.;
- Conducting community relations classes for recruits at the Academy;
- Implementing and coordinating Department crime prevention information programs;
- Assisting basic car officers with crime prevention information visual aids, and program materials as needed;
- Developing the design and publication of all Department crime prevention brochures;
- Developing and assembling crime prevention displays;
- Conducting crime prevention training programs within the Department;
- Researching and preparing Environmental Impact Reports required of the Department, and analyzing Environmental Impact Reports that may affect the Department;
- Answering requests for information regarding the Department through personal contacts, general correspondence, and the dissemination of information pamphlets;
- Developing relationship-based policing training and curriculum design focus groups to further improve the Department's overall strategic community outreach efforts;

- Developing, recommending and strengthening policy and programs that enhance police community relations, increase understanding and cooperation, and reducing the fear of crime;
- Providing greater transparency with the community regarding Department engagement efforts in coordination with Media Relations and Community Affairs Group and the lead Public Information Officer;
- Coordinating strategic outreach programs to include the Days of Dialogue, Community Forums, Clergy, and Traffic Bicycle Liaisons;
- Coordinating and implementing Senior Lead Officer training Department-wide;
- Supporting major community outreach efforts such as the Community Safety Partnerships;
- Leveraging social and digital media platforms in order for the Department to effectively engage and inform the public, stakeholders and employees with a consistent and cohesive message;
- Providing basic social media situational awareness reports regarding events that may impact public safety;
- Providing training to Department personnel regarding issues surrounding officer safety concerns and using social media;
- Providing support and guidance for major events and programs such as Summer Night Lights, National Night Out, and the Safe Summer Tip Off; and,
- Assisting with the geographic Area footbeats by providing personnel and additional resources to augment their efforts as needed.

IN-SERVICE TRAINING
INFORMATION TECHNOLOGY BUREAU

TRAINING ORDER May 3, 2016
1.17

TO: All Concerned Personnel

FROM: Commanding Officer, Information Technology Bureau

SUBJECT: INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT AND INFLUENCING NETWORKS TRAINING

Date/Time/Location:
May 23, 2016 to May 24, 2016
0800-1700 Hours
Police Headquarters Building – ITD Training Room 3rd Floor, Room 358
100 W. First Street,
Los Angeles, CA 90012

The Intelligence Preparation of the Operational Environment and Influencing Networks training provide a foundation to intelligence analysis and integration into law enforcement operations. It focuses on the fundamentals of analysis, the intelligence cycle, and intelligence analysis. This course provides students with an introduction to the intelligence community as well as analysis of criminal operations to include human networks and social media networks. The attendance of this training is a prerequisite for the Advanced Network Analysis and Targeting.

Attire: Appropriate casual training attire (no opened toe shoes, shorts, or tank tops).

Equipment: Notebook and pencil. All officers shall have their uniforms and appropriate field equipment readily available in case of deployment.

This is a primary duty assignment. Any scheduling conflicts are to be resolved in favor of this assignment. The only acceptable reasons for non-attendance are prescheduled vacations, court, military leave, or illness.

See attached roster for names of the employees assigned to this training. If you have any questions, please contact Police Officer II Varoj Vaidhayakul #39899, Information Technology Bureau, at (213) 486-0427.

MAGGIE M. GOODRICH, Chief Information Officer
Commanding Officer
Information Technology Bureau

Attachment

INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT AND INFLUENCING NETWORKS TRAINING
May 23, 2016 to May 24, 2016

STUDENTS

INFORMATION TECHNOLOGY BUREAU

Gamero, David	#38043
Vaidhayakul, Varoj	#39899

CENTRAL BUREAU

Casalicchio, Megan	#39770

METROPOLITAN DIVISION

Schearer, Perry	#38211

SOUTH BUREAU

Crosson, Eric	#32355
Timmermans, Thorsten	#37459

SOUTHWEST AREA

Briano, Stephanie	#40637

ROBBERY HOMICIDE DIVISION

Davis, Curtis	#36712
Zehner, Nicholas	#39904

NEWTON AREA

Phillips, Dorota	#37761