VOLUME 3 - CHAPTER 7

COMMUNICATIONS

3-07/000.00 COMMUNICATIONS

Radio, video, telephone and various computerized systems form the communications network for this Department. Procedures governing the individual or joint use of these systems are outlined in the following sections of this chapter. Inquiries regarding detailed procedures not included in this chapter shall be referred to the Technical Services Division (TSD).

In general, responsibility for radio communication equipment of all types within the Department lies with Communications and Fleet Management Bureau (CFMB). Responsibility for video, telephone, and computerized systems lies with Data Systems Bureau. All requests for surveys, installations, or alterations of any communication systems shall be channeled through the Chief of TSD.

Unauthorized or unofficial use of communications equipment is prohibited by the subsection titled "Use of Communications Equipment" in the Policy and Ethics Chapter of this manual.

3-07/010.00 480 RADIO SYSTEM

Radio equipment and procedures governing its use in this Department are discussed in the subsections which follow.

3-07/010.05 EQUIPMENT

Department radio equipment consists of several basic types:

- remote site radio equipment - transmitters and receivers located at remote radio sites throughout the County to overcome terrain problems. The main control point is the Sheriff's Communications Center (SCC). It serves as a relay center between the various Units of the Department;
- microwave equipment - links remote transmitter and receiver sites to SCC for control purposes; also replaces certain telephone line functions for point-to-point communications;
- mobile equipment - includes all transmitters/receivers installed in cars, buses, aircraft, motorcycles and boats;
- portable radio equipment - includes portable radios, surveillance equipment and other radios which can be moved and operated or set up by non-technical personnel; and

- fixed site radio equipment - other base Station and computer aided dispatch equipment installed at Sheriff's Stations, custody, court services, STARS Center and other County facilities.

In addition to the above basic equipment, the following are available for emergency use:

- mobile command posts - are equipped with mobile radio equipment on Sheriff and public safety frequencies and computer aided dispatch; and
- Station emergency radio transmitters - located at each Station dispatch area.

Radio monitors are located at each Station for the monitoring of radio traffic on various frequencies.

3-07/010.10 DEPARTMENT AND FCC REGULATIONS

Radio frequencies (channels) and the licenses to operate radio equipment are issued to Los Angeles County for this Department by the Federal Communications Commission (FCC). All communications equipment and its use must conform to Department and FCC regulations including:

- all temporary or permanent base Station equipment must be approved and licensed at the specified site;
- all radio equipment must be FCC type-accepted and approved by the Director of OAS;
- only communications which are essential to official police activities are permissible;
- no indiscreet or profane remarks;
- no superfluous or facetious wording or unauthorized communications,
- no personal remarks or conversation; and
- use of radio channels for training or simulation shall occur only with the prior approval of the SCC Watch Commander.

Failure to comply with FCC Rules and Regulations violates federal law and jeopardizes this Department's license to operate.

3-07/010.15 RADIO OPERATING PROCEDURES

In addition to specific radio operating procedures found in the Radio Communications Procedural Manuals, the following shall be observed by all radio field Units:

- unless otherwise directed by SCC, radio Units shall only use the "repeat mode;"
- at the start of shift, report “in service” with SCC;
- when transmitting on the mobile radio, place the microphone as close to the mouth as possible. When transmitting on all other types of equipment keep the

microphone approximately one inch from the mouth;
- speak in a normal tone, making the voice as emotionless as possible, regardless of the situation-keep the voice to a monotone;
- pronounce words distinctly and rather slowly--the normal speaking rate should be between 40 to 60, words per minute;
- identify your Unit at the start and end of each transmission;
- except in an emergency, do not transmit during a "busy" tone which indicates the frequency is being used; and
- refer to the Department Official Code Book for message codes to use when transmitting.

Any transmission longer than 30 seconds should be broken at 30-second intervals, stopping transmission and waiting 2 or 3 seconds before resuming transmission. This interval provides for the following:

- allows the copying Station to assure the Unit that the message is being received or, if not receiving, allows time to ask for a repeat message; and
- allows any other Station with an emergency transmission to go ahead without waiting.

3-07/010.20 FALL BACK MODE

Use of Station transmitters for dispatch purposes or the use of "Fall back Mode" shall not be initiated without approval of the SCC Watch Commander. In the event that SCC cannot be contacted, authorization shall be obtained from the Station Watch Commander.

3-07/010.25 CONTROL AND INVENTORY OF RADIO EQUIPMENT

Unit Commanders are responsible for the development, implementation and enforcement of procedures for radio equipment, care, control and inventory. All portable radio equipment and accessories shall be stored in a locked location. Watch Commanders shall confirm, at least once per shift, that all assigned portable radio equipment and accessories are accounted for. Units that do not operate with 24-hour Watch Commanders, shall develop policies and procedures to ensure strict accountability for communications equipment.

Unit Commanders are responsible for implementation of, and adherence to, the battery maintenance and security program approved by CFMB. All batteries not attached and in use on radios shall be secured in a locked cabinet and only issued when a discharged battery is exchanged.

Units temporarily requiring additional radios for planned tactical or special operations shall forward their request to CFMB via the internet request form located on the CFMB

web page.

The CFMB shall be responsible for the assignment, control and maintenance of radio equipment and shall maintain a master inventory of all Department-owned radios. Radios are generally issued to individual Department members and will remain with them when they transfer to a new assignment. Members who transfer to an assignment with a different type of radio shall contact CFMB logistics to exchange radios. Members are responsible for notifying their Unit of equipment changes.

Units shall designate a “Radio Collateral Officer” who will be responsible for keeping that Unit’s radio inventory updated using the Department’s “MCM” inventory management system. All changes in assignment of radio equipment shall immediately be updated in the MCM system. Semi-annually, the Radio Collateral Officer shall submit a report to CFMB logistics indicating that the radio assignments for that Unit are complete and correct.

Department members shall only be issued one portable radio unless authorization is received by CFMB.

Uniformed personnel who are assigned portable radios with remote speaker-microphones, shall carry the radio in the issued holder. The radios shall not be removed from the holder for routine use nor shall the remote speaker-microphone be removed or disconnected from the radio.

3-07/010.30 RADIO CHANNEL USAGE

The Department's radio system operates under the command and control of the CFMB. Users must follow Department operating procedures and FCC rules.

Department radio channels are a shared resource. Any Unit may request that a non-dispatch channel be temporarily restricted for its use as the situation warrants. Most channels are available only in specific geographical areas; therefore, their assignment must be closely coordinated to ensure effective use. The SCC Watch Commander may restrict or alter channel assignments based upon type of operation, other concurrent operations, area of required coverage and priority.

The following information describes general channel usage:

Dispatch Channels: Stations are assigned to specific dispatch channels. These channels will be used for dispatching and communicating with Station Units. Dispatch channels shall be used only in the "repeat mode."

Local Tactical (L-TAC) Channels: Stations are assigned to specific local tactical channels. L-TAC channels will be used for tactical coordination within a Station area. Should the need for an additional tactical channel arise, one may be requested through

the SCC Watch Commander.

Area Tactical (A-TAC) Channels: Tactical/special operation channels which provide wide geographic area coverage. Use of these channels is restricted and requires concurrence from the SCC Watch Commander prior to their use.

Countywide Tactical (C-TAC) Channels: Tactical/special operation channels which provide countywide coverage. Use of these channels is restricted and requires concurrence from the SCC Watch Commander prior to their use.

Mutual Aid (M-AID) Channels: Provide a radio communications link to participating outside agencies. These channels are restricted and may be used only with the prior approval of the SCC Watch Commander.

Custody Channels (Two Simplex Channels): Reserved for use by Custody Divisions.
Court Services Channels (Two Simplex Channels): Reserved for use by Court Services Division.

Countywide SCC Access Channel: Provides access to SCC for database inquiries and relaying of information.

Emergency Channel: Countywide channel restricted solely to request emergency assistance.

Special Unit Dispatch (SUD) Channel: Countywide channel for use by Units that are not dispatched through the SCC.

Investigative (INV-1 to 7) Channels: Used by assigned Department investigative and special operations Units.

Secure Voice Channels: Reserved for high security operations. These channels shall not be used without prior approval of the SCC Watch Commander.

Portable Repeater Channels: Reserved for special events and operations. These channels will only function when used with a portable repeater and shall not be used without prior approval of the SCC Watch Commander.

The following listing describes the channel plan for this Department. Channels marked with an asterisk (*) are monitored on a full-time basis by the SCC.

480 MHZ Voice Radio System

Channel	Usage
Dispatch 1	Crescenta Valley/Altadena
Dispatch 2	West Hollywood

Dispatch 3	East Los Angeles
Dispatch 4	Century
Dispatch 5	Santa Clarita Valley
Dispatch 6	San Dimas/Walnut
Dispatch 7	Lomita/Avalon
Dispatch 8	Industry
Dispatch 9	Carson
Dispatch 10	Lost Hills/Malibu
Dispatch 11	Temple
Dispatch 12	Lennox/Marina del Rey
Dispatch 13	Norwalk/Pico Rivera
Dispatch 14	Lakewood
Dispatch 15	Lancaster Station
SCC Access	Metrolink/Court Services

L-TAC-1	West Hollywood/Lost Hills/Malibu
L-TAC-2	Lennox/Lomita/Avalon/Marina del Rey
L-TAC-3	Lakewood
L-TAC-4	Industry
L-TAC-5	Carson
L-TAC-6	East Los Angeles
L-TAC-7	San Dimas/Walnut/Temple
L-TAC-8	Altadena/Crescenta/Santa Clarita/Metrolink
L-TAC-9	Century
L-TAC-10	Norwalk/Pico Rivera
L-TAC-11	Lancaster Station
A-TAC-1	North Area Tactical
A-TAC-2	West Area Tactical
A-TAC-3	East Area Tactical
A-TAC-4	South Area Tactical
C-TAC-1	Countywide Tactical
C-TAC-2	Countywide Tactical
C-TAC-3	Countywide Tactical
M-AID-1	Mutual Aid, North County/SF Valley
M-AID-2	Mutual Aid, West Metropolitan Area
M-AID-3	Mutual Aid, East Metropolitan Area
M-AID-4	Mutual Aid, San Gabriel Valley
M-AID-5	Mutual Aid, Central Metropolitan Area
CUSTODY	Custody Channel (2 Simplex Channels)
COURT SER	Court Services (2 Simplex Channels)
SCC	Countywide SCC Access
EMERGENCY	Emergency Trigger Channel
SUD	Countywide Special Unit Dispatch
INV-1	Investigative, Countywide
INV-2	Investigative, North/Central
INV-3	Investigative, West

INV-4	Investigative, South
INV-5	Investigative, Southeast
INV-6	Investigative, Central
INV-7	Investigative, East
SV-1	Secure Voice 1, LA Basin/ SG Valley/N County
SV-2	Secure Voice 2, LA Basin/ SF Valley/Santa Clarita
PORT RPTR-1	Portable Repeater 1
PORT RPTR-2	Portable Repeater 2

470 MHZ DIGITAL RADIO SYSTEM

Channel	Usage
DATA-1	Data, Countywide
DATA-2	Data, CAS, LNX, MDR
DATA-3	Data, AVA, CVS/ALD, LMT, SCT, LHS/MAL
DATA-4	Data, ELA, TEM, WAL/SDM
DATA-5	Data, IND, PRV
DATA-6	Data, NWK, CEN SO
DATA-7	Data, LKD, WHD, CEN NO
DATA-8	Data, AVS

470 MHZ Voice/Paging Radio System

Channel	Usage
PAGING	Paging
TACTICAL	Countywide Tactical/Mutual Aid

MDT equipped Units shall use only the assigned data channel. Use of DATA-1 requires prior SCC approval.

3-07/010.32 USE OF DEPARTMENT FREQUENCIES BY OTHER GOVERNMENT ENTITIES

There are circumstances when it is beneficial to members of this Department to have radio inter-operability with other law enforcement and government agencies. The Department's radio frequencies are, however, a finite resource and only in those instances where inter-operability with other agencies is clearly in the Department's interest shall authorization to operate on Department frequencies be granted. In those circumstances, and when such an entity requests authorization to operate on Department radio frequencies, the following procedure shall apply:

- when any Department Unit receives a request to operate on Department radio

frequencies, the Unit Commander shall evaluate the request and, if he concurs, forward it to CFMB with a memorandum stating the Unit Commander's basis for concurrence. All requests from other government entities must be in writing and identify the reason for which operation on Department frequencies is necessary;

- the CFMB Unit Commander shall evaluate the request, prepare a memorandum with his findings and forward it, along with the original request and the memorandum from the Unit Commander who concurred with the request, to the Chief of TSD;
- the Chief of TSD shall review and forward the request to the Division Chief or Division Director whose Unit(s) will share the use of the frequencies with the requesting agency for evaluation. The completed evaluation shall be returned to the CFMB through the Chief of TSD;

  NOTE: Requests which involve inter-operability with multiple Department Units on multiple frequencies shall not be reviewed at the Unit Commander level. All such requests shall be forwarded by the Chief of TSD to the appropriate Division Chief(s) or Division Director. The completed evaluation shall be returned to the CFMB through the Chief of TSD.

- the CFMB shall be responsible for notifying the requesting agency in writing of the Department's findings. A frequency-sharing agreement, which is required by the Federal Communication Commission, shall be prepared by CFMB for those requests which are approved. Approved requests shall be valid for a period not more than one year, with reevaluation occurring annually in June.

  The frequency-sharing agreement, which identifies the specific terms and conditions of use, shall include, but not be limited to, the following:

  - number of radios authorized;
  - whether radios are mobile or portable;
  - which frequencies are to be used; and
  - call signs of the requesting agency;

- an automatic identification feature, compatible with the Department's communication system, for all radios; and
- frequency-sharing agreements shall be maintained on file at the CFMB.

3-07/010.35 REPORTING SYSTEM FAILURES/PROBLEMS

Any system problems or failures must be reported to SCC at once. The caller must provide the following information:

- radio or data frequency used;
- geographical location where the problem occurred;
- specific nature of the problem; and

- Station or Unit identifier.

The SCC access channel or any dispatch channel may be used to report radio system trouble.

3-07/010.40 LOST/STOLEN/DAMAGED RADIO AND CELLULAR TELEPHONE EQUIPMENT AND ACCESSORIES

When Department portable communications equipment or accessories are lost, stolen or damaged, the Unit at which it occurred shall:

- make an immediate phone notification to CFMB, Logistics;
- file an Incident Report (SH-R-49) and distribute as follows:
    - original to be imaged in the electronic archival system, SECDA;
    - one copy to the Auditor-Controller, Fixed Assets Unit;
    - one copy to accompany SH-AD-32A to the reporting Unit's Division Chief or Division Director; and
    - one copy to CFMB Systems Maintenance Section;
- send a SH-AD-32A, signed by the Captain, to the Division Chief or Division Director. The SH-AD-32A shall include:
    - type of equipment, i.e., portable radio, speaker/microphone. Full description, i.e., brand name, model, size, etc.;
    - County serial number and/or the inventory control number;
    - a brief description of the circumstances surrounding the loss or damage; and
    - the Unit Commander's finding on the cause of the loss/damage and a determination of negligence involved;
- after review by the Division Chief or Division Director, the SH-AD-32A shall be forwarded to the Chief of TSD, Attn: CFMB; and
- cellular telephone equipment capable of sending and receiving data that is lost or stolen must immediately be reported to Data Systems Bureau via the Help Desk to request a "wipe" of the device. Service on this equipment shall not be suspended or transferred until Data Systems Bureau confirms the data is clear or sufficient time has passed indicating the device is not active.

Equipment that is lost, stolen or damaged beyond repair may be replaced if CFMB has sufficient inventory to replace the equipment.

If an immediate replacement item is needed, the Chief of TSD shall make the determination whether a loan item will be issued pending the delivery of a replacement item. However, if a loan item is not available, the Division where the loss occurred may be required to provide the necessary funds to purchase the replacement equipment.

- Units with damaged equipment may be required to provide the necessary funds to repair the equipment; and/or

- post or damaged cellular equipment shall be replaced and funded by the requesting Unit. If negligence is determined, the employee may be responsible per MPP section 3-03/060.00.

3-07/020.00 RADIO BROADCASTS

An occurrence of concern to any or all groups of field Units shall be transmitted as a "broadcast." A broadcast may be transmitted simultaneously on more than one frequency at the discretion of the SCC Watch Commander. Field Units should designate the area they desire to receive the broadcast.

Commonly used the broadcasts include the following:

- emergency crime broadcasts;
- missing child broadcasts;
- found child broadcasts; and
- Countywide alert broadcasts.

3-07/020.05 EMERGENCY CRIME BROADCASTS

Units requesting clearance for an emergency broadcast shall use the following sequence of information for the broadcast:

- crime;
- location;
- time of occurrence;
- number of suspects, subjects, etc;
- vehicle description (year, make, model, color and license number);
- last seen (direction taken; on foot or in vehicle);
- description of suspects (sex, race, age, height, weight, color hair, color eyes, oddities and clothing);
- weapons used; and
- what obtained (money, merchandise, etc.).

3-07/020.15 MISSING AND FOUND CHILD BROADCASTS

If the subject is of critical age (16 years of age or under), a broadcast shall be initiated by the handling Unit. If the subject is over the critical age, but there are extenuating circumstances involved (suicidal, mentally ill, diabetic, retarded, in need of medical attention, etc.), the field Unit shall determine the need for a broadcast. The basic information for broadcasts shall include:

- reporting Unit;

- name of missing child (last, first and middle);
- address;
- physical description and any outstanding features;
- mental condition (retarded, etc.);
- clothing description;
- time and locate on last seen; and
- probable destination (if given).

A "Found Child" broadcast must be issued if the subject is found and a "Missing child" broadcast has been made. If no missing broadcast was issued and subject is found, only the concerned Station shall be notified.

3-07/020.20 SILENT ALARM RADIO CALLS

Silent burglary or robbery alarm radio calls may originate at SCC or the Station of jurisdiction. They are priority calls requiring one Unit to handle the call and one or more Units to assist the handling Unit. Units responding to a silent alarm call shall:

- acknowledge receipt of the message and give an estimated time of arrival (ETA);
- proceed immediately to the location of the alarm when assigned to handle or assist in handling the call;
- notify SCC upon arrival at the location; and
- advise monitoring Station of conditions at location after investigation. When advising that no further assistance is needed (Code 4), give the name and address of business and whether or not a crime has occurred. Example: (Station name, Unit number) Code 4, Bank of America, Fifth and Main. No 211; (Unit number).

3-07/020.25 PHYSICAL DESCRIPTIONS

Descriptions of persons named in radio broadcasts shall be given in the following sequence:

- name (last, first, middle and suffix);
- alias (AKA);
- date of birth (DOB);
- sex;
- race;
- age;
- height;
- weight;
- hair;
- eyes;
- identifying physical imperfections, marks, etc.; and

- description of clothing (from head downward).

3-07/030.00 ACQUISITION AND USE OF RADIO TRANSMITTERS

Personnel, including Reserves, posse members, mountain rescue team members, and law enforcement explorers, shall not use radio transmitters capable of transmitting on licensed Sheriff's frequencies unless the transmitters have been issued by the County or have been approved by the Department. Units shall notify CFMB prior to purchasing or accepting donations of any radio equipment of any type and receive approval of the equipment.

All equipment capable of transmitting any radio signal of any kind, whether purchased by individuals or acquired through donations, shall be examined by the Communications Solutions of CFMB, who shall:

- examine equipment for compatibility;
- examine modifications to transmitter circuitry;
- examine repairs made to radios by non-County personnel;
- examine auxiliary transmitter equipment, such as extra microphones or encoding devices;
- perform other examinations as may be deemed necessary to protect the integrity of the Sheriff's radio system; and
- determine if the equipment must be licensed per Federal Communication Regulations.

3-07/040.00 FUNCTIONS OF SHERIFF'S COMMUNICATIONS CENTER (SCC)

Major functions of SCC are outlined in the following subsections. For "Sigalert" procedures, refer to the Case Assignment and Reporting Volume.

3-07/040.05 RELAY OF RADIO MESSAGES

SCC, when acting in its primary capacity as the relay center for radio communications between Department Units, receives the message for transmission from the Station of jurisdiction via the Mobile Digital Communications System, MDCS. The exact message is then relayed over one of several frequencies to the concerned mobile Unit.

In this capacity, SCC does not dispatch, command or control the Unit's communication, but merely relays the communication.

There is a direct voice channel "Hot Line" between each Station and the Sheriff's dispatcher assigned to that Station. An alternate voice line that can be used as a backup to the Hot Line is an automatic ring circuit "Cold Line." When the Cold Line rings at SCC,

it is answered by a communication operator.

3-07/040.10 INTERCOMMUNICATIONS WITH OTHER AGENCIES

SCC coordinates requests for assistance from other agencies and relays calls received by these agencies to Sheriff's Stations having jurisdiction. This intercommunication is accomplished by direct phone lines with the following agencies:

- Fire Department;
- Los Angeles Police Department (LAPD); and
- California Highway Patrol (CHP).

3-07/040.15 PRESS NOTIFICATION - CODE "20"

SCC relays all requests for press notification of newsworthy incidents in accordance with Department policy.

3-07/040.20 WARNING SYSTEMS

SCC is the control point for the following warning systems:

- Emergency Alert System (EAS)
- this local system provides a means wherein a direct flow of information regarding a local major disaster can be transmitted to the public via radio and TV. Input to the EAS is accomplished through Sheriff's Headquarters Bureau or the SCC Watch Commander; and
- National Warning Systems (NAWAS)
- SCC is the primary warning point within the County for the North American Air Defense Command. This system is used for attack warnings, disasters and tsunami (seismic sea wave) warnings and is tested each shift.

3-07/040.25 CALIFORNIA LAW ENFORCEMENT RADIO SYSTEM (CLERS)

SCC is the local communication point for this state-provided radio system by which police agencies may communicate point-to-point on a statewide basis. Several local police agencies have equipment on this system. SCC will relay for nonparticipating police agencies.

3-07/040.30 FIELD CHECKS

SCC is the contact point between mobile field Units and major state and federal

computerized data banks for purposes of field checks of vehicles, wanted persons, firearms and property. This service is for non – MDT/MDC equipped mobile field Units only - Stations and headquarters Units shall use normal channels of access to these computers. Data required should be spoken slowly and distinctly.

3-07/050.00 REQUESTS BY RADIO

Requests for service or backup by a field Unit should include the purpose of which it is needed, e.g., car trouble, a search, for traffic control, for transportation, etc. A routine request may change to an emergency situation at any time. Emergency requests, except for the following subsections, are outlined in the Miscellaneous Line Procedures chapter and in the Radio Communications Procedural Manuals.

3-07/050.05 AMBULANCE REQUESTS

A Unit making this emergency request shall identify itself and give the location to which the ambulance should be dispatched. SCC, via ring-down line, will advise the Fire Dispatch Center of the request the number of ambulances required and the location. An exception to this is the City of Lynwood, where requests will be relayed to Century Station.

3-07/050.10 FIRE AND/OR RESCUE EQUIPMENT REQUESTS

A Unit making this emergency request shall identify itself and give the location to which the fire equipment should respond. Requesting Unit shall state the type of fire so that the Fire Department may respond with the proper equipment. Requesting Unit shall also state type and purpose of rescue equipment needed, e.g., cave-in; inhalator needed, etc.

3-07/060.00 L.A. COUNTY DISASTER COMMUNICATIONS SERVICE

The Disaster Communications Service (DCS) is established and maintained under the authority of L.A. County Code. The L.A. County Sheriff is the designated Chief of this service. Space, personnel and equipment are provided at the following locations:

- County Emergency Operations Center, Sheriff's Emergency Operations Bureau (CEOC); and
- nineteen decentralized districts--one at each Sheriff's Station, including Catalina Island.

3-07/060.05 ORGANIZATION

Volunteer amateur radio operators enrolled in the 19 districts and County Emergency

Operations Center comprise the largest and most active Radio Amateur Civil Emergency Services (RACES). This group is mobilized in case of:

- war-caused emergencies;
- local disasters, e.g., earthquakes, major forest fires or riots;
- National disasters; and
- mountain, desert or water rescues.

Department staff and district communications officers are appointed to supervise and direct the volunteers. Their duties and responsibilities are outlined in detail in established operations manuals.

3-07/060.10 EQUIPMENT

The following equipment is available through the DCS and is designed to establish required communications circuits during initial stages of a disaster:

- Sheriff's Mobile Command Post;
- generator Truck - a companion power supply vehicle; and
- one van - equipped with Department and amateur transmitters and receivers.

3-07/060.15 ACTIVATION

Activation of all or any portion of the DCS can be accomplished through the following chain of command of North Patrol Division:

- Chief, North Patrol Division;
- Area Commander in charge of Emergency Operations Bureau (EOB);
- Unit Commander, EOB; and
- EOB Sergeants, DCS.

3-07/070.00 PAGING SYSTEM

Requests for pagers for assignment to specific individuals, or for a Unit's pool use, shall be directed to the respective Division Chief or Division Director for review and approval. The request shall indicate the specific requirement for the paging service and the number of pagers needed. If the pager is for assignment to an individual, his name, position and Unit of assignment shall be noted.

Pagers shall be issued to those individuals who are assigned to a unique position that requires the ability to be contacted by methods other than telephone or radio.

3-07/070.05 ISSUANCE AND CONTROL OF PAGERS

The CFMB shall be responsible for the issuance, control and maintenance of pagers and shall maintain a master inventory of all Department owned pagers. This Bureau shall forward a roster of assigned pagers to each respective Unit as part of the semi-annual cell phone audit.

Unit Commanders are responsible for the pagers issued to their Unit for pool use. Unit Commanders shall maintain a current list of all pagers assigned to their Unit, including those assigned to individual positions and shall be responsible for verifying CFMB's inventory roster of all pagers within their Unit. If an individually assigned pager is reissued to another employee, the CFMB must be notified immediately.

3-07/080.00 TELEPHONE SYSTEM

Telephone systems – including both analog and Voice Over Internet Protocol (VOIP) and services for this Department are provided and maintained by the Data Systems Bureau.

3-07/080.02 RESPONSE TO A FAILURE IN THE TELEPHONE SYSTEM

The following procedures shall be followed in the event of a large scale failure in telephone and 9-1-1 services within the Sheriff's Department jurisdiction:

If the station is unable to accept 9-1-1 telephone calls due to equipment failure, station evacuation, or other cause, the station shall notify SCC by calling (323) 881-8100, and the station that serves as the fallback Public Safety Answering Point (PSAP) 9-1-1 responsibilities shall be transferred to a station that is outside of the affected area.

In a large scale failure, alternate routes of communication shall be established, providing citizens with the ability to request required assistance.

Contact the Sheriff's Communication Center (SCC) via radio and advise them of the problem. They will set up an alternate line at SCC for citizens to call and will advise Sheriff's Headquarters Bureau to post Emergency Alert Announcements with local television and radio stations. This will allow people with unaffected land lines or cell phones to contact the Department if the station phones are inoperable.

Contact the Station's Disaster Communications Service Volunteers (DCS) via the Station's Emergency Coordinator. These are Home Amateur (HAM) radio operators that can set up their equipment at fire stations, shopping centers, hospitals, and other locations to facilitate communications to and from the station or SCC.

If assistance from additional personnel is required, the affected station should follow the Departmental guidelines for initiating the Emergency Mobilization Plan.

3-07/090.00 INCOMING CALLS

Procedures for handling emergency and routine incoming calls are outlined in the subsections which follow. All calls shall be answered promptly, efficiently and courteously. Personnel shall properly identify themselves by Unit and name when answering all incoming telephone calls.

3-07/090.05 BUSINESS AND 9-1-1 TELEPHONE SYSTEMS

For the purposes of the subsections which follow, the Department's telephone systems are defined as the "business system" and the "9-1-1 emergency system."

3-07/090.10 EMERGENCY INCOMING CALLS - BUSINESS SYSTEM

Emergency calls directed to a Station complaint desk, received on the business system, shall take precedence over all other business system calls. Any routine call in progress shall be placed on "hold" until each new incoming call is answered to determine if it is an emergency call.

When calls for emergency service or assistance are received by a Unit other than the Unit having jurisdiction, all necessary information shall be obtained and the information relayed to the concerned Unit or agency immediately. This procedure is in accord with the Department policy of not transferring calls of an emergency nature, received on the business system and giving all possible assistance to the caller.

If there is any question of jurisdiction or when available information indicates that our emergency service can arrive sooner than that of the agency having jurisdiction, a Unit of this Department and necessary allied emergency equipment shall be dispatched.

If the call involves a traffic accident within the jurisdiction of the California Highway Patrol (CHP), handle in accordance with the provisions outlined in the Traffic chapter of this manual.

The incident and action taken shall be entered in the dispatch system and a tag number assigned so that the incident will be recorded.

3-07/090.15 THE 9-1-1 EMERGENCY TELEPHONE NUMBER SYSTEM

Without exception, only emergency calls shall be taken on the 9-1-1 line. Do not transfer a non-emergent 9-1-1 call to a business line. This procedure does not remove the caller from the incoming 9-1-1 telephone trunkline, though appearances would tell you

otherwise. Should a non-emergent call be received on this line, transfer the caller to the 9-1-1 nuisance line recording and the caller will be informed that 9-1-1 is to report emergencies only.

Station complaint desk personnel answering 9-1-1 lines shall:

- do so without delay - the line should not ring more than twice before being answered;
- answer: "9-1-1. What is the emergency?";
- if "Foreign Exchange" appears on the Automatic Location Identification (ALI) display unit above the caller's address, the Deputy shall look at the address carefully. "Foreign Exchange" should alert the Deputy that the call is originating outside the Station area. If an emergency, the Deputy shall determine which police or Sheriff's Station has jurisdiction and immediately transfer the call;
- immediately transfer calls reporting incidents of smoke/fire to Fire Dispatch. Do not interrogate the caller. All calls reporting the same smoke/fire incident shall be transferred, not terminated;
- immediately transfer calls reporting injury traffic accidents to Fire Dispatch, regardless of jurisdiction. Calls reporting injury traffic accidents within Station jurisdiction, including contract cities, may be placed in conference with Fire Dispatch to obtain all necessary information;
- remain on the line until the transfer is complete; and
- transfer or terminate all calls expeditiously to free the 9-1-1 lines.

A 9-1-1 call that has been transferred to the Station complaint desk shall not be transferred a second time. All necessary information shall be obtained and relayed to the concerned Unit or agency immediately.

When a 9-1-1 line is answered and the call is disconnected prior to determining its nature or completing a transfer, Deputies shall utilize available resources to determine an appropriate response.

3-07/090.20 ALARM COMPANY CALLS

Coordination of emergency procedures with alarm companies necessitates rapid identification, reporting, and response. The following procedures shall apply to silent alarm calls:

- the alarm company should identify the emergent nature of the call by stating "silent robbery/burglary alarm report;"
- the Station switchboard operator receiving this identification shall immediately connect this call with the Station complaint desk via the emergency line. If the emergency line is busy, the call shall be placed on another line to the desk and a Station PA broadcast made identifying the line and the nature of the call; and
- the complaint Deputy or other available desk personnel shall answer the call

immediately and dispatch the necessary Units to handle.

3-07/090.25 ROUTINE INCOMING CALLS

Establishing and maintaining good public relations shall be a primary goal of all Department members handling incoming telephone calls. All personnel shall adhere to the following procedures:

- give proper identification when answering the telephone, stating unit of assignment and name;
- handle the call yourself, when possible, unless the caller asks to speak to a specific person;
- when necessary to refer the caller to another unit, explain the reason and provide caller with the correct number before transferring the call;
- if caller has already been transferred, offer to obtain requested information and return the call or obtain an accurate source of information for the caller;
- return calls promptly, notifying caller of action being taken or results of your efforts to obtain correct information; and
- use message forms when taking messages; record the following information:
    - called person's name;
    - caller's name and affiliation;
    - date and time of call;
    - message; and
    - receiver's name.

Telephone Demeanor

The public's perception of our organization is directly impacted by our courtesy and thoroughness during daily telephone contacts. All personnel shall utilize the basics of effective telephone communications:

- greet the caller with a professional tone;
- listen closely;
- be helpful;
- empathize; and
- avoid Department/police jargon.

By utilizing these five easy steps, the Department will present a professional image and promote better customer service.

Procedure

All personnel who answer incoming telephone calls shall greet the caller by identifying themselves and stating their unit of assignment. Below are examples of standard greetings that may be adapted for every unit on the Department:

Data Systems:
"Records Management, Mr./Ms./Mrs. Smith, how may I help you?"

"Good afternoon, Records Management, Mr./Ms./Mrs. Smith, can I help you?"

Homicide Bureau:

"Detective Smith, Homicide Bureau, how may I help you?"

"Homicide Bureau, Mr./Ms./Mrs. Smith, can I help you?"

Lakewood Station:

"Deputy Smith, Lakewood Station, how may I help you?"

"Good morning, Sheriff's Station, Mr./Ms./Mrs. Smith, can I help you?"

Telephone Demeanor Audits

To ensure compliance with Department policy, random audits will be conducted. The result of these audits will be reported to the Office of the Undersheriff or concerned Assistant Sheriff on a monthly basis. A copy of these results will also be sent to each Unit audited. Unit Commanders are responsible for commending employees who performed in accordance with this policy. Unit Commanders shall take appropriate administrative action regarding employees who demonstrated substandard performance in an area covered by the audit.

3-07/100.00 OUTGOING CALLS

County phones shall normally be used for County business only. Members making outgoing business calls shall give proper identification and state the reason for the call when the person or Unit being called is reached. Members making any personal calls shall reimburse the County via personal check payable to the Sheriff's Department.

Busy signal verification shall only be used in an emergency, as the Department is charged for these verifications.

3-07/100.05 TOLL OR LONG-DISTANCE CALLS

Toll or long-distance calls from County phones shall be placed utilizing the authorized long distance telecommunications network.

Toll or long-distance calls from a non-County phone should be handled as follows:

- completed via the authorized long distance telecommunications network;
- charged to a County calling card; and
- paid for by the employee placing call and a claim for reimbursement made.

Telephone calls from most Department facilities are automatically routed by the County long distance provider. Local area calls (Los Angeles and fringe areas bordering the County) are routed without an authorization code requirement. Telephone calls directed outside of the local area require an authorization code.

Depending upon the class of service, the authorization code will enable the user to make long distance calls ranging from Southern California only, to worldwide coverage. Employees of the Department who routinely make long distance calls to locations outside the County should be issued an authorization code/card.

All requests for telephone authorization codes should be submitted to CFMB. CFMB shall be notified when employees are transferred. Monthly usage reports will be reviewed by the user's supervisor for authorized use.

Calling Range Privilege (CRP)

002 50 United States
003 50 United States, DDD* Mexico and Canada and IDDD International capabilities)**
010 Southern California (Outside LATA 5)
011 California State
013 50 United States, DDD* Mexico and Canada

* direct distance dialing (DDD) refers to those calls that can be dialed directly without the assistance of a telephone operator.

** No one below the rank of Commander should be assigned this CRP absent specific articulable requirements.

Authorization Codes are issued as follows:

Calling Range Privilege (CRP)	Rank/Equivalent/Civilian Position
011	Deputy
013	Sergeant
013	Lieutenant
013	Captain
003	Commander or above

Any class of service upgrade requires the approval of a Division Chief or Division Director.

Use of Calling Cards

From a County facility with MCI network access:

- enter the phone number as you normally would. When you hear the tone, enter your authorization code. Your call will be completed.

3-07/100.20 TELEPHONE CALLING CARDS

Calling cards will be issued to those employees who have need to make frequent official calls from non-County phones. Due to service charges, the necessity of such calls should receive serious consideration before completing. Personal calls shall not be made with the County issued calling card.

Requests for new calling cards, changes to existing calling cards, or deletion of calling cards should be made to the Unit Calling Card Coordinator who will relay the request to CFMB.

3-07/100.25 CELLULAR PHONE ASSIGNMENT, USAGE, MAINTENANCE AND MANAGEMENT

Several classifications of Department employees are assigned a cellular phone for use in the course of their Department business. The following is a list of Department classifications and positions whose incumbents are authorized the use of a permanently assigned cellular phone:

- sworn Department executives and civilian Directors responsible for command in the Executive Offices, Office of Administrative Services and other Department Divisions, facilities, Stations and Bureaus;
- sworn investigators and their supervisors who are on active on-call status and who are subject to immediate response, wherein the assignment and use of a cellular phone is deemed necessary and appropriate by the employee's Unit Commander. Unit Commanders shall closely monitor the assignment of cellular phones to individuals in this classification. Only those employees who are frequently called out after hours shall be assigned a cellular phone. Unit Commanders are encouraged to assign Department hand-held radios to those employees who have a lesser likelihood of call-out or who may be called out in the event the active on-call investigator is unavailable; and
- sworn or civilian employees who are entrusted with unique Departmental resources or specialized equipment, wherein the use of a cellular phone enhances their ability to respond and deploy these resources or equipment. Additionally, some employees travel outside the effective range of the Department radio network (i.e., Statewide Transportation, Fugitive Detail, Crime Lab technicians, etc.); because of this, cellular phone assignment may be appropriate. The concerned Unit Commander shall closely evaluate the need for cellular phone

assignment in these cases.

Department Units with multiple users or pool cellular phones shall assign a supervisor to ensure compliance with a standardized Department tracking system designed to manage and audit the use of each phone. The tracking system entails the use of the Multi-Use Cellular Phone Usage log.

Purchase of cellular phone instruments is the responsibility of individual Units. Cellular phones that are considered additions (not replacement units) require the approval of the concerned Division Chief or Division Director and the Chief of Technical Services Division. Vehicle installation (if applicable), maintenance, and activation of all Department cellular phones shall be the responsibility of the Communications and Fleet Management Bureau (CFMB). CFMB will also maintain a complete inventory of Department cellular phones, specifying the Unit of assignment of each phone and, if appropriate, the name of the assigned employee. All changes in cellular phone assignment, including a phone's removal from service, shall be reported to CFMB. CFMB also maintains a utility and tactical pool of cellular phones to support special operations or other unique needs. The temporary loan of one of these phones, not to exceed 30 days, may be granted by the CFMB Unit Commander.

Fiscal Administration, Administrative and Training Division, is responsible for the acceptance and appropriate distribution of monthly cellular phone bills to individual Units. The concerned Unit Commander shall be responsible for:

- reviewing each bill to determine if charges are appropriate. In the event that employee personal calls are identified, the Unit Commander shall ensure that the responsible employee reimburses the Department for the cost of these calls. The employee shall forward the appropriate amount for reimbursement, in the form of a personal check or a money order, to the Special Accounts Section of Sheriff's Fiscal Administration within 30 days of bill receipt; and
- notifying Fiscal Administration, in writing, of billing inconsistencies or discrepancies.

Twice each year, on January 1 and July 1, Unit Commanders shall review the allocation of cellular phones at their Unit. They shall question the continued necessity of each phone in service, utilizing standards such as:

- frequency of use;
- availability of other communications equipment in lieu of cellular phones;
- percentage of employee personal use versus Department use; and
- the possibility of converting individually assigned cellular phones to pool phones.

In conjunction with the July allocation review, Unit Commanders shall complete an annual certification of cellular phone use for their Unit. This review shall be forwarded to the Director of Administrative and Training Division by July 30 of each year. This certification will specify the following:

- number of “active” cellular phones assigned to the Unit;
- summary of the Unit’s cellular costs; and
- Unit Commander’s statement of necessity, covering each phone in use.

3-07/100.30 INMATE TELEPHONE MONITORING SYSTEM

The Inmate Telephone Monitoring System (ITMS) is a computer database capable of maintaining secured data storage, live monitoring and temporary storage of recorded inmate telephone calls initiated from Los Angeles County Sheriff’s Jail Facilities, Courthouse Holding Facilities, Patrol Station Holding Cells and Probation and Juvenile Detention Facilities throughout Los Angeles County.

The Inmate Telephone Monitoring System is divided into two sections, the Administrative (Non-Investigative) Section and the ITMS Investigative Section.

The Administrative Section is located in Correctional Services Division, within the Inmate Services Unit. This section is overseen by a ITMS Project Director, ITMS Project Manager and/or designee. It shall be the responsibility of the Administrative Section to alleviate maintenance issues, oversee the daily management of the inmate telephone services contract in Los Angeles County Jails and detention facilities and to manage the revenue derived from the telephone system.

The ITMS Investigative Unit is managed by an individual holding the rank of Lieutenant assigned to Detective Division - Homicide Bureau. It shall be the responsibility of the ITMS Investigative Unit to authorize use, issue user accounts and manage system access by all Department and non-Departmental personnel.

The ITMS Investigative Unit Lieutenant will establish a liaison with the ITMS Administrative Section and ITMS Project Manager of the Los Angeles County Probation Office, regarding any investigative issues.

GENERAL PROCEDURES

ITMS access is available to all LASD Detective Personnel including designated personnel from the Administrative Section, Custody Division, Detectives from allied Law Enforcement agencies and personnel from the District Attorney’s Office, with the approval of their respective Unit Commander or Department Administrator.

Reporting of all ITMS maintenance issues discovered by the ITMS Investigative Unit, will be promptly reported to the Administrative Section for resolution. ITMS users shall not make direct or indirect contact with the contractual provider for any issue regarding the ITMS.

Access to the ITMS by Private Attorneys, Court Appointed Attorneys or members of the

Office of the Public Defender and or Private Investigators, will be by court order only.

The ITMS Investigative Unit will conduct quarterly ITMS audits. Accounts deemed inactive for more than 90 days will be deactivated. The ITMS Investigative Unit Lieutenant can revoke access to the ITMS upon founded violations of the ITMS Access Request Agreement.

The ITMS Investigative Unit will offer analytical support to Sheriff's Department personnel. The ITMS Investigative Unit will maintain a training program and will provide necessary training to users.

All downloaded ITMS data and records generated as a result of a systems search, are deemed confidential and may be legal evidence. All downloaded data and records deemed to be pertinent to an investigation shall be handled, retained, and stored in accordance with Los Angeles County Sheriff's Department evidentiary procedures.

All court orders and subpoenas for ITMS data, records or recordings will be processed by the ITMS Investigative Unit. ITMS Investigative Unit personnel and or representatives from the contracted telephone service provider, will be available for courtroom testimony.

Privileged communications between inmates and their attorney, religious advisor, and physician will not be knowingly or intentionally downloaded without a search warrant, court order or consent of all involved parties, in compliance with Penal Code Section 636 (a). Telephone numbers of members of the Los Angeles Bar Association, Los Angeles County Public Defender's Offices and attorney's telephone numbers provided by the court appointed conflict panel (Attorneys) have been entered into the ITMS / contracted telephone service provider database, to prevent the recording of telephone calls to these numbers.

If during the monitoring of inmate communications, Law Enforcement personnel discovers evidence of criminal activities involving officer safety issues, conversations involving criminal threats of harm to witnesses or victims, information regarding jail security issues at any facility or information pertaining to attorney's telephone numbers and or the recording of any privileged communication, this information shall be reported to the ITMS Investigative Staff immediately.

The ITMS Investigative Unit will make efforts to make notification to Detectives regarding the simultaneous monitoring of inmates by other detectives. It will be the responsibility of the detectives to contact each other to resolve investigative conflicts.

All users are responsible for adhering to the Los Angeles County Sheriff's Department's electronic communications policy, as set forth in the following Manual of Policy and Procedures sections:

- 3-07/210.00, Permissible Use: Employees are expected to abide by the standards of conduct delineated in other volumes, chapters, and sections of the Manual of

Policy and Procedures as they may be applied to the use of electronic communications, use and release of information;
- 3-07/210.25, Security: Only the authorized owner of the logon person (USER ID's) is permitted to use the ID. Employees are responsible for keeping their passwords secret. Employees shall not share common USER ID's and passwords for any computer system; and
- 3-07/220.00, Prohibitions: Assist in providing access to unauthorized persons to any data, software, programs, computer system, or computer network.

3-07/110.00 COUNTY TELEPHONE DIRECTORY CHANGES

Information concerning changes to the current Department section of the County Telephone Directory shall be reported to the Department telephone coordinator, CFMB.

Instructions and the method of reporting errors are found in the "General Information" section of the County telephone directory.

3-07/120.00 JUSTICE DATA INTERFACE CONTROLLER SYSTEM (JDIC)

The Justice Data Interface Controller (JDIC) is operated and maintained by Data Systems Bureau.

JDIC is a regional law enforcement data communications system consisting of a centrally located message switching computer and a network connecting criminal justice agencies throughout the County. The primary function of JDIC is to provide County law enforcement agencies instant access to local, state and federal data files and to permit them to send and receive official administrative messages to one another throughout the County, State, and Nation.

3-07/120.10 PARTICIPATING AGENCIES

Agencies participating in the Sheriff's JDIC system include:

- all Sheriff's Stations, Bureaus and major facilities;
- District Attorney's Office;
- Superior Courts;
- Probation Department; and
- local, state, and federal law enforcement and criminal justice agencies within Los Angeles County.

Refer to the JDIC system "HELP," for a directory of all participating agencies and their terminal identifiers listed in "Help/1" and "Help/12."

3-07/120.15 MESSAGES - TYPES, TRANSMISSION, AND RECEPTION OF

JDIC is the state designated County control agency for transmission of point-to-point administrative messages and broadcasts as well as computer data file access for Sheriff's facilities and other Los Angeles County justice agencies.

Message types:

- Department orders, notices and announcements;
- bulletins directed to agencies participating in the JDIC network;
- broadcasts originating within the JDIC network for transmittal to in-County, State, and Federal agencies or to out-of-County agencies via CLETS and out-of-State agencies via NLETS;
- crime broadcasts originating from law enforcement agencies within the County; and
- Sheriff's Department administrative broadcasts.

A JDIC user anywhere on the network can transmit and receive messages to or from:

- any participating Station, Bureau or facility;
- any law enforcement agency participating in the JDIC network;
- any in-County local, State, or Federal law enforcement or criminal justice agency participating in the California Law Enforcement Telecommunications System (CLETS) network;
- any out-of-State criminal justice agency participating in the Nation Law Enforcement Telecommunications System (NLETS); and
- with proper security, any JDIC terminal can access:
    - Department of Motor Vehicles' data file;
    - Department of Justice (DOJ) data files;
    - FBI National Crime Information Center (NCIC) data files; and
    - County Internal Services Department's Justice Computer Center (JCC) data file.

3-07/120.20 REPORTING EQUIPMENT TROUBLE

If trouble is encountered while operating JDIC equipment, the operator shall contact JDIC Computer Operations and give the following information:

- Department name and phone number;
- address and location of equipment;
- JDIC equipment mnemonic; and
- nature of trouble.

The operator shall follow the instructions of the JDIC Computer Operations personnel in

order to resolve the problem.

3-07/130.00 LOCAL BROADCASTS

The JDIC system has the capability to transmit messages to one or more locations, broadcast groups, or to all Sheriff's Stations and police departments on the network simultaneously. Members of this Department shall cause messages to be transmitted to their appropriate destination according to message classification.

JDIC messages are classified as follows:

- Point-to-Point Messages - these are single address messages directed specifically to another agency or to a particular Sheriff's Station or facility. The message is of importance only to the agency addressed;
- Joint Messages - these are multiple address messages. They are directed to two or more agencies. They are of importance only to those agencies addressed. JDIC allows users to address a message from one up to a maximum of 20 agencies. The message must be readdressed and retransmitted if this maximum is exceeded; and
- JDIC Broadcast Group Messages - these are messages sent to specific agencies within particular JDIC broadcast groups. The message is of importance to all agencies within the broadcast group addressed.

  Broadcast groups and agencies within each group are found in the JDIC system "HELP" broadcast group directory in "Help/4",

The following general instructions shall apply to all broadcast messages transmitted from any Sheriff's Department terminal:

- messages shall be brief and concise;
- messages containing statute code violations shall specify both the statute code section as well as its correct legal description. Statute codes alone are not permitted; and
- messages shall be directed only to those agencies/facilities which have a need to receive the information contained in the message.

There are two types of local broadcasts:

- announcements, - these include Department orders, notices, and other administrative messages; and
- crime Broadcasts.

3-07/130.05 ANNOUNCEMENT - FORMAT

Department announcement broadcasts shall adhere to the following format:

- the first line shall contain the address of the location where the message is to be sent;
- SHERIFF'S DEPARTMENT BROADCAST shall appear in the left position of the second line;
- ANNOUNCEMENT shall appear in the extreme right position of the second line;
- the Station/Bureau/facility name shall appear on the third line immediately beneath ANNOUNCEMENT;
- the Unit name shall appear on the fourth line immediately beneath ANNOUNCEMENT;
- the fifth line shall indicate to whom the message is directed, e.g., TO: ALL PERSONNEL, etc.;
- the sixth line shall remain BLANK;
- the seventh line shall state the subject of the message, e.g., SUBJECT: TRANSFERS, PROMOTIONS, etc.;
- the eighth line shall remain BLANK;
- the text of the message shall begin on the ninth line;
- the line following the end of the text shall remain BLANK; and
- the Sheriff's name and title shall appear in the extreme left position of the last line. The operator's initials, followed by SNDG, shall appear in the extreme right position of the last line.

3-07/130.10 CRIME BROADCAST FORMAT

The information listed below shall be included in all crime broadcasts, if unavailable the operator shall indicate that the information is unknown. Each information category shall be preceded by an appropriate heading which describes the type of information being provided. A blank line shall separate each category of information. Local crime broadcasts shall be presented in the following format:

- SHERIFF'S DEPARTMENT BROADCAST shall appear in the extreme left position of the first available line after the message has been addressed to the location(s) to where it is to be sent;
- Crime - type of crime. Statute codes used alone are unacceptable. An appropriate legal description of the charge shall be included;
- Date/Time - date and time crime occurred;
- Victim - victim's or business' name;
- l - address and city where crime occurred;
- Suspect - physical description and clothes description. Name, age, DOB and residence address, if known;
- Weapon - type and appearance, if used;
- Vehicle - year, make, type, color, any damages and license plate number of suspect’s vehicle;

- Loss - amount of loss and brief description of identifiable objects;
- MO - mode of operation (modus operandi) method of entry, speech, conduct, etc., of suspect. Particular attention shall be given to the unique aspects of the crime;
- Attn: - any agency or detail that may have particular interest in the crime, e.g., ATTN: Norwalk Sheriff's Station suspect lives in your area; ATTN: All Burglary Details, etc.; and
- Refer - name and title of Bureau/Station Commander, Bureau/Station name, detail, telephone number, and file number.

3-07/130.15 ROBBERY BROADCAST FORMAT

Robbery broadcasts shall be initiated or approved by the following persons:

- Watch Sergeant for broadcasts resulting from a patrol Unit investigation;
- Station Detective Watch Commander for broadcasts resulting from follow-up investigation; and
- Detective Division investigation Units.

The following heading shall be used to standardize robbery broadcasts:

- Robbery/Market (small grocery store, liquor store, gas station, drug store, bank - name the type of business that sustained the loss, not the clerk or employee's name);
- Robbery/Bank Messenger (name of business or type of business for which employee may be transporting money to or from a bank);
- Robbery/Strong arm (location of robbery should be included in text of message; for example, "paper boy attacked by suspect on street corner"); and
- Robbery/Purse Snatch (location of robbery can be included in text of message; for example, "victim attacked from the rear while walking on sidewalk").

A standard robbery broadcast format shall be used for the following types of robbery broadcasts:

- Robbery/Business, Bank messenger, strong arm or Purse Snatch;
- Wanted – Robbery;
- In Custody –Robbery; and
- Supplement - Wanted - Robbery.

The information listed below shall be included in all Robbery Broadcasts. If it is not, it shall be indicated that the information is unknown. If the information is not known, the operator shall indicate that it is unknown. Each information category shall be preceded by an appropriate heading which describes the type of information being provided. A blank line should separate each category of information.

- Robbery/Business (name the type of business involved):

    - Victim - name of business, address, city, date and time of crime;
    - Suspect - physical description, clothes description, appearance;
    - Weapon - type and appearance;
    - MO - mode of operation (modus operandi) method of entry, conduct, speech, written or spoken orders, etc.;
    - Loss - amount of cash or valuables; description of identifiable objects,
    - Vehicle - Year, make, type, color, any damages and license plate number of suspect's vehicle; and
    - Refer - name of detective handling case, Station or Unit and URN;
- Wanted - Robbery/Business (include felony warrant number in heading):
    - Suspect - name, age, DOB, physical description, distinguishing marks, appearance, residence address, release dates, CII, FBI or County booking number;
    - Weapon - type and appearance;
    - Vehicle - year, make type, color, any damage and license plate number of suspect's vehicle;
    - Attn: - jurisdiction where suspect may visit relative, address of relative, receptiveness of relative to police contact; and
    - Refer - name of detective handling case, Station, or Unit and URN;
- In Custody-Robbery/Business (name the type of business involved):
    - Suspect - name, age, DOB, physical description, distinguishing marks, appearance, residence address, release dates, CII, FBI or County booking numbers;
    - Weapon - type and appearance;
    - Vehicle - year, make, type, color, any damage and license plate number of suspect's vehicle; and
    - Refer - name of detective handling case, Station or Unit and URN.

3-07/140.00 DEPARTMENT OF JUSTICE SYSTEM (DOJ)

The California Law Enforcement Telecommunications System (CLETS) is maintained by the Department of Justice (DOJ) and provides administrative and broadcast message service to law enforcement and criminal justice agencies within the state. CLETS also provides law enforcement agencies the ability to send and receive messages throughout the 50 United States via the National Law Enforcement Telecommunications System (NLETS).

3-07/140.05 CLETS AND NLETS MESSAGE CLASSIFICATION

CLETS and NLETS messages are classified according to their destination, as follows:

- Point-to-Point Messages - these are single address messages directed specifically to another agency;
- Joint Messages - these are multiple address messages directed to two or more

agencies;

- CLETS Area Bulletins - these are messages sent to one or more of three broadcast areas within California;
    - many agencies do not participate in the bulletin service. It should not be assumed that a message addressed to a bulletin area will be received by all agencies within that area. If a message is thought to be of specific interest to one or more agencies within a bulletin area, a point-to-point administrative message should also be sent;
- NLETS State APBs - these are messages sent to one or more (maximum of five at one time) areas within the Continental United States;
- NLETS National APBs - these messages are sent to all states within the continental United States;
    - NLETS APB messages are first sent to the state control agency within the state to which the message is addressed. The state control agency may or may not rebroadcast the message to other agencies within their state. If a message is thought to be of specific interest to one or more agencies within the APB area, a administrative point-to-point message should also be sent to the agency or agencies.

3-07/140.10 GENERAL INSTRUCTIONS

The following general instructions apply to all messages transmitted from any Department JDIC terminal to CLETS or NLETS:

- area broadcasts shall not be used when point-to-point or joint messages will serve the same purpose;
- messages shall be brief and concise;
- messages containing statue code violations shall specify both the numerical code section as well as its correct legal description. Statute codes alone are unacceptable;
- all CLETS broadcast messages shall be sequentially numbered, commencing at 2400 hours daily, by each originating terminal;
- the time of transmission, date, originating agency identifier (ORI) and operator's initials shall appear as the final entry in all CLETS and NLETS messages. The hour of the day shall be represented in military (24-hour) time;
- NLETS messages shall be carefully addressed and directed only to those states or regions having a particular interest in the information broadcast. Do not use abbreviations in NLETS messages and never use California Penal or other statute codes when sending messages to other states; and
- messages shall be directed only to those agencies or bulletin areas which have a specific need to receive the information contained in the message.

3-07/140.15 CLETS AND NLETS RESTRICTIONS

CLETS and NLETS bulletins may not include any of the following:

- excessive listings of unidentifiable serialized and non-serialized items, except those that contain unique markings;
    - serialized property should be entered into the Automated Property System rather than listed in CLETS and NLETS bulletins. NLETS does not allow any property under observation broadcasts;
- misdemeanors - crime broadcasts;
- runaway juveniles;
- traffic warrants;
- failure-to-provide wants (270 PC);
- missing persons bulletins;
    - CLETS does allow missing persons bulletins for life or death situations. NLETS, however, does not allow missing persons bulletins under any circumstances. Missing persons shall be entered in the Missing Persons System;
- political notices - of any nature;
- notices regarding retirements, seminars, training, meetings, social functions, pistol meets, TV or radio programs, membership solicitations, holiday greeting, etc.;
- recruitment of personnel;
- death notices, except sworn personnel and executive level officials on active duty status; and
- profane language - for any purpose.

In addition to the above restrictions, NLETS National APB bulletins may not contain:

- attempt to locate messages;
- messages regarding wanted subjects or vehicles;
- road and weather reports;
- messages in which complainant is interested only in recovery of property; e.g., property under observation broadcasts; and
- administrative information regarding vehicle registration or driver's license expiration dates, etc.

3-07/140.20 CLETS MNEMONICS

CLETS mnemonics are utilized to route messages to the following agencies:

- all State agencies participating in the CLETS Network, including those located within the County;
- any municipal or County law enforcement or criminal justice agency that participates in the CLETS Network; and

NOTE: The Department of Justice prohibits sending point-to-point and joint

messages via the CLETS Network to County or municipal agencies located within the same County.

- all Federal agencies located within the state that participate in the CLETS Network.

CLETS mnemonics are found in the CLETS-CJIS Manual, published by the California State Department of Justice.

3-07/140.25 NLETS ORIGINATING AGENCY IDENTIFIER

NLETS originating agency identifiers (ORI) are utilized to route messages to law enforcement or criminal justice agencies in another state. Originating agency identifiers are found in the NLETS ORI Directory, published by the U.S. Department of Justice.

CLETS prohibits sending any message to agencies within the state via the CLETS Network using NLETS ORIs.

3-07/140.30 CLETS AND NLETS BULLETIN/MESSAGE FORMAT

JDIC provides two customized screens (formats) to assist operators in addressing and constructing CLETS and NLETS messages. Operators should refer to on line JDIC System "HELP" for general instructions regarding format use.

The information shall be included in CLETS and NLETS crime bulletins. If unavailable, the operator shall indicate that the information is unknown. Each category shall be preceded by a standardized descriptive heading. A blank line should separate each category of information. See section 3-07/130.10 for bulletin format. When using this format, eliminate "Sheriff's Department Broadcast," and begin on the first available line after the destination agency name.

All other types of CLETS and NLETS bulletins/messages shall adhere to the following format. They shall begin on the first available line after the destination agency name:

- Subject - subject of the message;
- text of the message;
- Attn: - agency, detail, etc. or individual who may have a particular interest in the message; and
- Refer - name of individual sending message, file#, agency name, Unit, address, city, zip code, operator’s initials and telephone number.

3-07/140.35 STANDARDIZED SUBJECT

Standardized subjects titles have been established by DOJ for CLETS bulletins. They shall be used whenever possible. This convention admits entry of a primary and secondary subject. For example:

- primary subject;
    - assault;
- secondary subject;
    - in custody;
    - wanted;
    - deadly weapon;
    - intent to murder; and
    - intent to rape.

Two primary subjects may be used for the purpose of clarification. Example: Robbery - Kidnaping.

Operators must refer to the CLETS-CJIS Manual to ensure that their crime bulletin entries contain the proper standardized subject titles. When primary or secondary subjects other than those listed in the CLETS Manual are employed, they shall conform to CLETS policy as closely as possible.

3-07/140.40 SUPPLEMENTATION/CORRECTION

To add information or correct a CLETS or NLETS message, the following applies:

- Supplementation - when operators wish to add supplemental information to a message previously broadcast the secondary subject, shall be titled "SUPPLEMENT," For example: Aggravated assault – Supplement; and/or
- Correction - when operators wish to correct information contained in a message previously broadcast, secondary subject shall be titled "CORRECTION." For example, armed robbery - correction.

Any transmission that changes the status of a message previously broadcast shall include:

- the date, time, call letters and message number of the original and all subsequent messages;
- subject (title) of the original message;
- intended change of status - supplementation or correction;
- name of suspect; alias;
- all available reference numbers, such as:
    - file or case number;
    - booking numbers;
    - report number; and
    - FBI and CII numbers (if known);

- any "Attn:" previously cited;
- description and status of any property or vehicles mentioned in previous messages; and
- repeat of report number in reference line.

3-07/150.00 LAW ENFORCEMENT COMPUTER INFORMATION SYSTEMS

Several computerized data files have been developed for law enforcement and criminal justice agencies. These data files can be accessed through the JDIC Network and provide a variety of information of interest to law enforcement.

When using any of the computer files available through JDIC, this Department shall adhere to the policies, practices, and procedures established for these systems. The policies instituted for each system are discussed in that system's user's manual. A list of available user's manuals is provided in a later section of this chapter.

3-07/150.05 INFORMATION ACCESS AND DISSEMINATION

Department members shall adhere to all applicable restrictions pertaining to the use and dissemination of information obtained from a particular data file. Generally, information obtained from criminal justice information systems is restricted to law enforcement and criminal justice agencies for official business only. (See the Miscellaneous Administrative Procedures chapter of this manual for special regulations concerning the Dissemination of Criminal Record Information).

For the purposes of this chapter, access to and/or dissemination of information contained in criminal justice information systems is accomplished through the use of communications equipment. Unauthorized or unofficial use of Departmental communications equipment is prohibited. Refer to the subsection entitled "Use of Communications Equipment" in the Policy and Ethics chapter of this manual for additional information concerning this regulation.

3-07/150.10 LEGAL REQUIREMENTS - RECORD ENTRY

The California Penal Code section 11108 and/or California Vehicle Code section 10551 requires that every law enforcement agency immediately enter certain types of information into the appropriate data base:

- all serial numbers of vehicles, vehicle parts or license plates reported as stolen, lost or recovered;
- all serialized property reported as stolen, lost, found, recovered or under observation property; and
- all serial numbers of boats and boat parts reported as stolen and recovered.

Unit Commanders shall ensure that their personnel follow legal these requirements.

All information entered into criminal justice information data files must be based upon an Incident or Supplemental Report. The report must be available at all times in order that "hits" on the data base record can be confirmed. Any changes to information contained in the original Incident or Supplemental Report, must be made so that it agrees with the report.

3-07/150.15 DATA BASE USER'S MANUALS

Criminal justice information system data files require that record entries, updates and certain inquiries contain specific types of information. JDIC structures all messages to conform to the formal requirements of each data file; however, operators must enter required information in a manner consistent with the edit values of the data file in use.

Operators are referred to the appropriate user's manual for a detailed discussion of data base terminology, functions, record retention criteria, special instructions, mandatory versus optional information and valid codes.

User's manuals for criminal justice information system data files are:

- Department of Motor Vehicle (DMV) - refer to the DMV Manual for CLETS Inquiry;
- California Justice Information System (CJIS) - refer to the CJIS Manual and Automated Criminal History System User's Guide;
- National Crime Information Center (NCIC) - refer to the NCIC Operating Manual and Code Manual;
- Automated Justice Information System (AJIS) - refer to the Automated Justice Information System Terminal Operator's Manual, arresting agency table, charge table and release custody table;
- Juvenile Automated Index (JAI) - refer to the Juvenile Automated Index Terminal Operator's Instruction Manual; and
- Los Angeles Countywide Warrant System - refer to Countywide Warrant System Users Manual.

3-07/150.20 CALIFORNIA JUSTICE INFORMATION SYSTEM (CJIS)

The California Justice Information System (CJIS) is maintained by the California Department of Justice. CJIS provides inquiry and record entry capability for authorized local, state and federal criminal justice agencies. CJIS is composed of:

- Automated Boat System (ABS) - ABS maintains information regarding stolen, lost, repossessed, embezzled or stored boats and boat parts;
- Automated Firearm System (AFS) - AFS information is divided into two groups: law

enforcement records and historical records. Law enforcement records include stolen, evidence, found, institutional registration, lost, under observation, retain for official use, and destroyed firearm information. Historical records include buy, consignment, dealer record of sale, serial number assigned or restored, license to carry concealed weapon, pawn, voluntary registration and sold at auction firearm information;

- Automated Property System (APS) - APS maintains information regarding stolen, lost, found, under observation and evidence held property. The stolen bicycle file is a sub-file of APS. Stolen credit card and pawn or buy information is also available;
- Criminal History System (CHS) - CHS maintains complete records on active criminals within the state, including past activity within the criminal justice system. Information contained in CHS records include name, aliases, monikers, physical descriptors, identifying numbers, registration information, probation and/or parole summary, arrest, convictions, arrest and convictions, arrest and conviction disposition, arresting agency and arresting agency file number;
- A "No Hit" in CHS does not mean a criminal history record does not exist. A record may exist in the manual file (see section 3-07/160.00);
- Stolen Vehicle System (SVS) - SVS maintains several types of records associated with vehicles. SVS defines a vehicle as a device by which a person or property may be propelled, moved or drawn, except: devices used exclusively in water; propelled by human power; and devices used exclusively on stationary rails or tracks;
    - Information in SVS records pertain to stolen, felony, wanted person, missing person, stored, impounded, lost and repossessed vehicles, stolen vehicle parts and stolen or lost license plates;
- Wanted Person System (WPS) - WPS maintains information on persons for whom an arrest warrant has been or will be (within 48 hours) issued. The warrant may be for felony or misdemeanor charges or any bench warrant. WPS is a pointer system only. The contributing agency must be contacted to verify the validity of the warrant. WPS requires that contributing agencies be willing to transport the person if he is apprehended;
- Missing and Unidentified Persons (MUPS) - MUPS is a file of reports about missing persons from California agencies. The Unidentified Persons File is a file of reports about unidentified persons (living and deceased) and body parts from California and surrounding states. All missing and unidentified persons reports are cross checked daily and contributing agencies are notified of possible matches;
- Restraining Order System (ROS) - ROS is a pointer system which pertains to domestic violence restraining orders entered into the state automated system by law enforcement agencies on individuals who have committed an act of domestic violence and have been served with a restraining order; and
- Supervised Release File (SRF) - SRF is an on-line file designated to provide the street officer with an index to subjects on active parole, probation, required to register as a sex or arson offender or considered a career criminal.

3-07/150.25 AUTOMATED MANAGEMENT INFORMATION SYSTEM (AMIS)

The Automated Management Information System (AMIS) is managed by the State Department of Motor Vehicles (DMV). The system provides access to the Driver's License file and Vehicle Registration file:

- DMV Driver's License file - contains individual's physical description, year of license expiration, special conditions regarding the status of the license, legal actions against the driver, abstract of court proceedings and record of subject's accidents; and
- DMV Vehicle Registration file - contains name and address of owner (registered and legal), description and current legal status of vehicle.

3-07/150.30 NATIONAL CRIME INFORMATION CENTER (NCIC)

The National Crime Information Center (NCIC) is maintained by the Federal Bureau of Investigation (FBI) in Washington, D.C. NCIC provides inquiry and record entry capability for authorized local, state and federal criminal justice agencies.

Many of the NCIC files are corollaries of CJIS and all inquiries are first routed to CJIS. If the desired information is available in CJIS, the message to NCIC is intercepted and CJIS information will be returned to the requestor. If information is not available in CJIS, the original message will automatically be forwarded to NCIC. The only exception to the above are inquiries to the Criminal History System. Criminal History inquiries may be routed directly to NCIC.

NCIC is composed of fourteen files, each of which contains information regarding:

- Stolen Boat File - stolen or embezzled boats. NCIC does not allow entry of lost, repossessed or stored boats. It also does not allow entry of boat parts or boat trailers. NCIC requires that stolen boats with out-of-state registration be entered to the stolen boat file;

- Gun File - stolen and recovered (abandoned, seized or found) firearms;

- Article File - stolen property. NCIC will not accept property records which are reported lost, found, evidence, under investigation, pawn or buy;

    The criteria for entry into the NCIC Stolen Article File are limited to individual property items valued at $500 or more or multiple (group) property items totaling $5,000 or more in one theft. Office equipment (typewriters, copy machines, etc.) and color television sets may also be entered, regardless of value. Additionally, any item of property may be entered at the discretion of the reporting agency, if:

        - the circumstance of the theft indicates that there is a possibility of interstate movement; and/or
        - the seriousness of the crime indicates that such entry should be made for investigative purposes.

- Criminal History Files - NCIC maintains three files which provide criminal history information:

    - the Automated Identification Division System (AIDS) is updated by the FBI from manual records supplied by states which do not participate in the Interstate Identification Index (III). This file is not complete, as several states do not submit criminal history information to it;
    - the III provides information necessary to directly access participating states' criminal history files; and
    - the Federal Offender File (FOF) provides federal arrest, disposition and custody/supervision information.

  Much of the information in these files is similar to the CJIS Criminal History System;

- Stolen Vehicle File - stolen or embezzled vehicles, (only if an arrest warrant has been issued for the suspect), vehicle parts, aircraft, and vehicles used in a felony. For NCIC purposes, a vehicle is any motor-driven conveyance, except a boat, designed to carry its operator. Trailers are also contained in this file;

- Stolen License Plate File - this file is used to store information regarding stolen license plates;

- Wanted Person File - persons with outstanding federal warrants, warrants for felonies or serious misdemeanors. The Wanted Person File is a pointer system only. The contributing agency must be contacted to verify the validity of the warrant. Contributing agencies must be willing to extradite the person from at least one state other than the contributing agency's state;

- Missing Person File - a person of any age who is missing and:

    - under proven physical/mental disability or is senile; thereby, subjecting himself or others to personal and immediate danger;
    - in the company of another person under circumstances indicating that his physical safety is in danger;
    - the circumstances indicate that the disappearance was not voluntary, e.g., abduction or kidnaping; and
    - declared unemancipated as defined by the laws of his state of residence and does not meet any of the entry criteria set forth above;

- Securities File - serial numbered identifiable securities which have been stolen, embezzled, counterfeited or are missing. This file does not include personal notes, checks, credit cards or coins. Securities for the purposes of this file include the following:

    - currency (Federal Reserve Notes, Silver Certificates, U.S. Notes, Canadian Notes, etc.);
    - documents which are evidence of debt (Treasury issued bills, bonds and notes; municipal and corporate bonds; debentures; other non-personal notes, etc.);
    - documents which represent subscription rights (stock warrants, stock rights);
    - other types traded in United States securities exchanges (except for commodities futures);
    - postal and other types of money orders;
    - traveler's checks;
    - warehouse receipts;
    - savings certificates;
    - bank drafts; and
    - interest coupons on stocks and bonds;

- Foreign Fugitive File - FFF records are maintained by the International Criminal Police Organization (INTERPOL). The inclusion of foreign fugitive data in the NCIC System provides a warning to U.S. law enforcement officers who might confront the fugitive so that they may use appropriate caution, provides assistance in locating and arresting foreign fugitives and helps provide for the public safety. Inquiries are not made directly into this file, but positive responses are provided when your message is processed through the NCIC Wanted Persons File;

- Unidentified Persons - the intent of this file is to assist investigators in the identification of unidentified found bodies, parts and of unidentified living persons;

- U.S. Secret Service Protective File (USSS) - USSS is a file designed to aid the U.S. Secret Service in protecting the President and other authorized protectees. It provides investigative leads on the whereabouts of those individuals who may pose a threat to a protectee and an individual's criminal activity which may be related to one of the protectees;

- Originating Agency Identifier (ORI) - ORI is a unique number assigned by the FBI/NCIC to every law enforcement or criminal justice agency that is serviced by NCIC. This file contains the agency name, address and telephone number; and

- Alcohol Tobacco and Firearms (ATF) Violent Felon File - ATF contains records on individuals who have three or more previous convictions for a violent felony or serious drug offense and are barred by Federal law from possessing a firearm or ammunition.

3-07/150.35 LOS ANGELES REGIONAL CRIME INFORMATION SYSTEM (LARCIS)

- Los Angeles County Regional Information System (LARCIS) - LARCIS maintains summary information on crimes and incidents based on activity by type. The LARCIS record contains type of offense, date and location of the incident, names of persons associated with the incident and vehicle license numbers. This system replaced the Event Index (EI) effective 01/01/2000.

3-07/150.36 CONSOLIDATED CRIMINAL HISTORY REPORTING SYSTEM

CCHRS provides the Los Angeles criminal justice community with complete, timely, and accurate criminal history information in an understandable format. The CCHRS database contains arrest and case disposition information about subjects who have been processed by the Los Angeles County criminal justice system. Subject information, including names, addresses, identifiers, and physical descriptions are stored in the database. Arrests and arrest charges, cases and case charges, dispositions, sentences, probation/parole, and warrant data is also available. This source data is provided by the following computer systems: AJIS, APS, CWS, JAI, PDS, PIMS, PHI, and TCIS. County data is supplemented with data from State justice agencies, ACHS, and DMV. Only authorized users have access to this information. Data in the database extends as far back as 1977, when data was first entered into the Personal History Index (PHI) system. CCHRS replaced PHI effective 01/01/2000.

3-07/150.40 AUTOMATED JUSTICE INFORMATION SYSTEM (AJIS)

The Automated Justice Information System (AJIS), managed by the Department, provides current information on the status of inmates in the custody of this Department, LAPD and several municipal police departments. AJIS issues booking numbers and maintains detailed information, e.g., physical description, charge, court dates, inmate locations, total bail and fines, expiration and release dates and special handling codes.

3-07/150.45 COUNTYWIDE WARRANT SYSTEM (CWS)

The Countywide Warrant System (CWS), managed by the Department, maintains information on persons for whom a felony, misdemeanor or traffic warrant has been issued. CWS also contains felony want information. Unlike the CJIS and NCIC wanted persons systems, CWS provides a Warrant Information Sheet (WIS for identification and warrant booking purposes).

3-07/150.50 AUTOMATED WORTHLESS DOCUMENT INDEX (TANGO)

The Automated Worthless Document Index (TANGO) managed by the Los Angeles Police Department, maintains local information related to forged and stolen checks, credit cards, money orders, airline tickets, etc. TANGO records contain names, addresses, phone numbers, identification and account numbers and driver's license numbers that appear on worthless documents.

3-07/150.55 JUVENILE AUTOMATED INDEX (JAI)

The Juvenile Automated Index (JAI) managed by the Los Angeles County Probation Department maintains information on juveniles contacted by contributing agencies within Los Angeles County for infractions of local, County, state or federal laws. The file also contains contact reports regarding neglected and dependent juveniles.

JAI records contain the following:

- juvenile's name, address, sex, date of birth and race;
- the parents', stepparents' or guardians' names;
- nature of the offense, date it occurred and name of agency processing the incident;
- previous contacts by other agencies;
- information regarding the following types of disposition:
    - application for Juvenile Court Petition;
    - application for Transfer to Probation Officer;
    - application for referral to Probation Department for non-court investigation; and
    - transferred to California Youth Authority;
- Probation Information - consists of PDJ number, area office, DPD number, detention location, current probation status and probation disposition;
- DPSS Information - consists of the Children's Services worker file number, DPSS officer, office location and 652 disposition;
- District Attorney Information - consists of the filing charges, reasons for petition rejection or referral and office location; and
- Superior Court/County Clerk Information - consists of the number, date and court locations of all court orders. When available, future court dates, whether a petition or any charges were dismissed or sustained, the reason for dismissal, warrants, findings from fitness resumption hearings, minor's attorney's name and final disposition.

3-07/160.00 NON-AUTOMATED STATE INFORMATION FILES

There are several manual files maintained by the State Department of Justice which provide information of interest to law enforcement. Access to this information is obtained

by mail, telephone or JDIC administrative message directed to the Department of Justice.

- mail requests are addressed as follows:

  Department of Justice
  Bureau of Identification
  P.O. Box 13417
  Sacramento, California 95813
  Attn: Unit Name

- Administrative Message requests are sent via JDIC, utilizing the "CLETS Administrative" format. The message is addressed to CLETS mnemonic "YME," Attn: Unit Name,

  The text of the message shall contain sufficient descriptors to assist in retrieval of the requested information; and

- telephone requests may be directed to each Unit, Monday through Friday, 0800 to 1630 (see telephone numbers in subsequent subsections); or the DOJ Command Center at (916) 227-3244, after hours, on weekends and holidays, unless otherwise indicated. The Command Center should only be contacted in emergent situations.

3-07/160.05 SEX AND NARCOTIC REGISTRANT UNIT

The Department of Justice maintains a central statewide alphabetic name file of persons who have been convicted of specific sex offenses (see 290 PC) and narcotic offenses (see 11590 H&S). Inquiries to the file may be requested by using one or a combination, of the following variables:

- CII number, name, age, race, weight, height, hair, eyes, sex, offense code, address, city, county, registering agency, date of registration (month and year), and termination of registration (month and year narcotic files only),

  Additionally, the County is broken down into grid coordinates. As an example, DOJ could search in L.A. County all registrants residing within map page 736, Grid Square J1, of the "Thomas Brothers Street Guide;" and

- messages and correspondence are sent Attn: Records and Identification Bureau, Registration Unit.

3-07/160.10 CHILD ABUSE UNIT

The Department of Justice maintains a central statewide file regarding child abuse and

neglect cases. The file contains and provides reports of child beating, child neglect, assaults on children, death reports of children, incest and child molestation where a member of the family is involved. The file contains the names of suspects, parents, victims, babysitters and other children mentioned in the reports.

- messages and correspondence are sent Attn: Child Abuse Unit, Special Services; and/or
- Telephone: (916) 227-3285.

3-07/160.15 COMMAND CENTER - RECORD INQUIRY UNIT

The Department of Justice Command Center is a manual expedite Unit whose primary function is to provide manual criminal history file information to law enforcement and criminal justice agencies on a timely and continual basis. The Unit is manned 24 hours per day, 7 days per week.

The manual criminal history file contains the same information as the CJIS Criminal History System (see section 3-07/150.20). Records are maintained on individuals whose first arrests occurred prior to 1972. Any subsequent arrests for these persons only will be recorded in the manual file, not the Criminal History System. Prior to contacting the Command Center, the subject should be checked against the CHS.

Operators are referred to the Department of Justice Record Inquiry Manual for further instructions.

- messages and correspondence are sent Attn: Name Check, Special Services; and
- telephone: (916) 227-3244.

3-07/160.20 OTHER STATE CRIMINAL HISTORY REQUESTS

Requesting criminal history information from other states within the Continental United States who do not participate in the NCIC Interstate Identification Index (see section 3-07/150.30) requires the utilization of the "JDIC RAPS2 Criminal History Record/Supplemental Info Request" format. The text of the message must contain sufficient descriptors to identify the subject to assist in the retrieval of the requested record. Identifying numbers should be included, if known. The check box for "NLETS criminal destination" field(s) must be filled if the request is for other than California destinations.

3-07/200.00 DATA NETWORKS, EXTERNAL DATA INTERFACES, AND DATA STORAGE

The Sheriff's Data Network (SDN), external data links, and data storage are under the administration of Data Systems Bureau. Hereafter, these are collectively referred to as the Department's Information Technology (IT) resources.

The SDN is a high speed network connecting all Sheriff's Department facilities and participating Los Angeles County municipal police departments. The SDN provides connectivity between desktop computers throughout the Department, as well as connection to other networks such as the Internet, LA Net, CLETS, and the Statewide Integrated Narcotics System. The SDN currently provides access to a wide range of applications, such as AJIS, LARCIS, CWS, CCHRS, RAPS, FMS, Cal Gangs (Formerly GREAT), CWTAPPS, JDIC and the Department's Intranet Server. For an up-to-date list of applications available on the SDN, contact the Central Help Desk.

For further information, refer to the standards found on the Intranet under Policy/ Standards/Guides on Data Systems Bureau's Intranet web page.

3-07/200.10 ELECTRONIC COMMUNICATIONS

The following sections of the Department's Manual of Policy and Procedures set forth the LASD policies for electronic communications including activity involving the Internet, Sheriff's Data Network, Justice Data Interface Controller (JDIC), local area networks, individual personal computers, and access to data stored in local, state, and federal computer systems. Electronic mail and faxes, which are transmitted over both the Internet and Sheriff's Data Network, are subject to all provisions of this policy. Data Systems Bureau is responsible for the administration of electronic communications via the Internet, Sheriff's Data Network, and JDIC.

3-07/210.00 AUTHORIZED PERSONS

Access to Department IT resources on behalf of the Department is limited to Department employees, Reserves, Volunteers, County employees, participating police agency employees, contractors and subcontractors and their employees conducting Department business, and others authorized by Data Systems Bureau. Hereafter in this policy, authorized persons will be referred to as authorized persons. Unauthorized persons, including inmates, shall not be permitted to access or otherwise utilize computers or network equipment unless under the direct instruction and supervision of an employee authorized to permit that access.

3-07/210.05 PERMISSIBLE USE

The use of any Department IT resource is restricted to those activities related to Department business. Use of computers and electronic communications by employees is authorized in support of the law enforcement mission of the Department and the

administrative functions that support that mission. Authorized persons shall adhere to this policy as well as the guidelines set forth in the County Electronic Data Communications and Internet Policies.

Authorized persons are expected to abide by the standards of conduct delineated in other volumes, chapters and sections of the Department's Manual of Policy and Procedures as they may be applied to the use of electronic communications and use and release of information.

3-07/210.10 SYSTEM USE

Authorized persons are expected to use electronic communications and network systems with a high degree of professional and personal courtesy. Authorized persons must ensure that the tone and content of electronic communications are business-like and exclude inflammatory remarks or inappropriate language. If it is an issue that could cause embarrassment, it does not belong on e-mail.

Although users of any Department electronics communication system or network have no rights of privacy, authorized persons shall not forward or otherwise disclose the contents of electronic messages with the intent to embarrass or otherwise harm the sender. This does not prohibit the receiver of e-mail from divulging the contents of electronic communications to an authorized persons' supervisor or to Department management.

Authorized persons who receive an electronic communication intended for another person shall attempt to notify the sender as soon as possible of the error.

Authorized persons who are authorized users of e-mail are responsible for reading their electronic mail in a timely manner, no less than once a day, or notifying their supervisor that they are unable to read e-mail. To enhance security and ensure that shared computers are available to all authorized persons, users shall logoff their computer when away from their workstation and at the end of the work shift.

All computers connected to the Sheriff's Data Network must remain "on," at all times, in order to permit after-hours maintenance, updates, and security upgrades. Authorized persons who have workstations which are used one or two shifts per day should logoff at the end of the day and leave the machines running.

Users of portable devices that connect to the Sheriff's Data Network should refer to the standards found on the Intranet under Policy/Standards/Guides on the Data Systems Bureau's Intranet web page.

3-07/210.15 PRIVACY

Authorized persons do not have any expectation of privacy when using computer and

network systems. All electronic files and e-mail in Department systems are considered the property of the Los Angeles County Sheriff's Department and may be accessed without the employee's permission.

The Department reserves the right to engage in monitoring electronic communications such as e-mail, faxes, computer files and networks, including the inspection of files created by authorized persons and stored in Department systems, to ensure that the public resources are appropriately used for County-related business. Monitoring may be for reasons including investigations, audits, employee supervision, and system maintenance.

Department authorized persons employees who are authorized access to the Internet will be monitored to ensure that Internet access is used for Department business.

Data Systems Bureau administrators may view the contents of electronic messages and files during the administration of the network computers.

Electronic communications and data may be subject to disclosure to third parties in response to the "Public Records Act" or other lawful court orders.

3-07/210.20 CONFIDENTIALITY

The Department cannot control the final disposition of electronic communications once they have been delivered. Authorized persons should be cautioned that any electronic message may be forwarded or printed without the sender's knowledge.

3-07/210.25 SECURITY

Only Department authorized persons or other persons authorized by Data Systems Bureau may access the Department IT systems. Those authorized will be assigned a logon identification code (i.e., USERID or ID). Only the authorized owner of the ID is permitted to use the ID. Those assigned an ID will also be required to select a password. Authorized persons shall not disclose their computer passwords to another person, except as required under this policy. Authorized persons are responsible to keep their passwords secret and to change them if compromised. Any electronic communications sent using an authorized persons' USERID and password is prima facie evidence the employee assigned the USERID and password generated the communications.

Authorized persons shall not share common USERIDs and passwords for any computer system, except as required for training or as specifically authorized by Data Systems Bureau. Any person who has knowledge of individuals who are sharing common USERIDs and passwords shall immediately notify their Unit Commander, in writing, with a copy to Data Systems Bureau. Authorized persons shall have only one network, e-mail, and fax account unless authorized by Data Systems Bureau. Only Data Systems

Bureau shall authorize IT systems access and USERIDs.

Passwords must adhere to the standards set forth in the Security Standards, which may be found on the Intranet under Policy/Standards/Guides on the Data System's Bureau Intranet web site.

In order to prevent unauthorized access to the Department IT systems or mis-use of information maintained by the Sheriff's Department, authorized persons must comply with the IT policies, standards, and guidelines which may be found on the Intranet under the Policy/Standards/Guides on the Data Systems Bureau Intranet web site.

Authorized persons shall immediately report to their Unit Commander, in writing, any violations of electronic communications policy as set forth in the Manual of Policy and Procedures, section 3-07/210.25, section 3-07/210.55, and section 3-07/250.00.

3-07/210.30 COMPUTER SOFTWARE AND FILES

Data Systems Bureau is responsible for selecting the standard desktop software suite for all Department computers and for administration of the software on computers connected to the Sheriff's Data Network (see section 3-07/230.00.). All authorized persons shall use the selected desktop suite unless critical functionality is not available through the suite.

Authorized persons are required to keep the personal information section (properties) of the e-mail address book up-to-date. This includes title, work address, Unit of assignment, work location, work phone number, and fax number. Optional items include mobile phone number and pager number.

Security software, including but not limited to: anti-virus, anti-spam, and firewall solutions are a critical component of the multi-layered security structure protecting the Department. Given this criticality, Data Systems Bureau is responsible for selecting and configuring security software for all computers. Unless a specific exemption or modification is authorized by Data Systems Bureau, all authorized persons shall use the authorized software, use the authorized configuration, and ensure the software is kept current.

Authorized persons are prohibited from installing or maintaining unlicensed software on any Department computer. Authorized persons who wish to install licensed software on a Department computer must have authorization from their Unit Commander and Data Systems Bureau. The software installation and record of the installation will be the responsibility of Data Systems Bureau. Authorized persons are required to provide a copy of the software license to Data Systems Bureau prior to the installation.

Licensing agreements for some software applications permit Department members to install the software on their home computers. For a list of these applications, contact the Central Help Desk.

It is strongly recommended that users store files in their personal folder in the Unit file server. These files will be "backed up" daily to prevent loss of information. They cannot be accessed by other users and offer the highest degree of individual security. Any files stored on the local drive ("C" drive) of the computer are not secure against access by other users and will not be backed up to prevent loss of information. During routine maintenance, computers may be replaced or hard drives erased without notice to the user. Data contained on the local drive ("C"drive) of these machines/hard drives will be lost to the user.

The Department reserves the right to access and disclose the contents of employee-created electronic files and messages when a legitimate business need arises and without the permission of the employee.

3-07/210.35 APPROVED ACCESS

All salaried Department employees shall have a Sheriff's Data Network account and electronic mail address subject to revocation.

Department members may have access to the Internet. Authorization may be terminated upon the employee's transfer to another Unit or at any time by their Unit Commander.

Department members may have access to the Sheriff's Data Network from remote sites using a special security identification procedure. Employees authorized access will be provided with a Virtual Private Network (VPN) access token for access to the Sheriff's Data Network. The tokens are the property of the Sheriff's Department and will be returned to Data Systems Bureau upon transfer to another Unit or upon the request of Data Systems Bureau. Access privileges will be reviewed annually. Unit Commanders may request remote access for their employees by sending a memorandum to the concerned Division Chief or Division Director (see section 3-07/230.00).

Access to database systems is authorized by the concerned system administrators. Access to the Sheriff's Data Network does not grant authorization to any database system. Contact the Unit which has system proprietorship in order to request access.

Individuals needing access to the files of another, when the employee is unavailable, must obtain approval from the concerned employee's Unit Commander. Upon authorization, Data Systems Bureau will provide and record the access given.

3-07/210.36 APPROVED ACCESS – NON-COUNTY PURCHASED COMPUTERS, SMART PHONES, AND OTHER PERSONAL DEVICES

For the purposes of the policy, all non-County owned computers, smart phones (including

BlackBerrys), and remote e-mail devices shall be termed “personal devices.”

Department employees may have a non-County purchased personal device connected to the Sheriff’s Data Network (SDN) provided that:

- access is approved by the Technical Services Division Chief;
- the remote access device has been approved by Data Systems Bureau; and
- the remote access device is configured to the established operational and security standards set by Data Systems Bureau.

Connecting a non-County purchased personal device to the SDN is strictly voluntary. All purchases, licenses, and configurations must be completed at the employee’s expense.

In order to maintain security of the Sheriff’s Data Network, authorized persons are prohibited from modifying the operational or security standards established by Data Systems Bureau on the non-County purchased personal device.

Data Systems Bureau may revoke access to the Sheriff’s Data Network at any time for violation of Department policy or breaches of security.

In the event a security issue arises, Data Systems Bureau may, without notice, remotely disable the non-County purchased personal device and erase all data contained on it in order to ensure the protection of the authorized person, data, and network.

Use of a non-County purchased personal device connected to the Sheriff’s Data Network is subject to the same policies and regulations as a County owned communication device. There is no “personal use” exemption.

There is no expectation of privacy for data passing through the Department’s network. All data is subject to review and audits.

The specific procedure to request a non-County purchased personal device to be connected to the Sheriff’s Data Network is described in detail in the Data Systems Bureau’s Intranet web page. For this and other information, refer to the Policy/ Standards/Guide on the Sheriff’s Data Network web page.

3-07/210.40 ENCRYPTION

Authorized persons may use encryption features provided by Department-approved software. Authorized persons shall not use their network password for files saved using this feature. When authorized persons choose to use encryption for personal files, they must divulge the encryption passwords to their supervisor. Authorized persons may not install or use any encryption software not specifically authorized by the Data Systems Bureau.

3-07/210.50 SPACE ALLOCATION

Authorized persons will be allocated limited space for the storage of their files. Authorized persons are encouraged to delete or remove data stored in Department computers as soon as practical. When maximum storage capacity is reached, authorized persons will be advised to remove files. Failure to do so will result in files being removed by system administrators without notice.

Authorized persons who need to exchange a high volume of information via e-mail should place the information in a “shared” folder and have permissions set so that the interested parties may have access to the folder over the network. See your local systems administrator for instructions on setting up shared folders or contact the Central Help Desk.

3-07/2I0.55 INTERNET ADDRESS

All Internet addresses (IP) for Department computer equipment will be assigned by Data Systems Bureau. No person shall utilize an Internet address without specific authorization from Data Systems Bureau.

3-07/220.00 PROHIBITIONS

Authorized persons shall not add, alter, copy, damage, delete, move, modify, tamper with or otherwise use or affect any data or software, computer, computer system, or computer network in order to either:

- devise or exclude any scheme or artifice to defraud, deceive, destroy or extort;
- Wrongfully control or obtain money, property, or data;
- disrupt or cause the disruption of computer or network services, or deny or cause the denial of computer or network services to an authorized user of a Department computer, computer system, or computer network; and
- assist in providing access to unauthorized persons to any data, software, programs, computer system, or computer network.

Unless specifically authorized by Data Systems Bureau, Authorized persons shall not install, connect to, move, change, modify, disconnect, or tamper with any data circuit, router, switch, hub, data jack, data cable, server, or other data communications equipment or software or assist any unauthorized person in gaining access to data circuits, routers, switches, hubs, data jacks, data cables, servers, or other data communications equipment or software.

Authorized Persons shall not do any of the following without the required authorization:

- access or allow access to another to obtain, alter, or prevent access to stored electronic communications or data;
- use electronic communications to capture or open electronic communications of another, or access files without permission of the owner;
- damage hardware, software, or other communications equipment or interfere with functionality;
- attempt to breach any security measures on any electronic communications system, or attempt to intercept any electronic communication transmission;
- modify or delete any file, folder or system audit, security, or ownership records or time stamp with the intent to misrepresent true system audit records;
- access the files belonging to another for non business purposes;
- use someone else's USERID, password or access another person's files, or retrieve stored communications without authorization;
- modify the hardware or software configuration on any computer;
- use electronic communications to transmit (upload) or receive (download):
    - any communication violating any applicable laws, regulations, or policies;
    - proprietary or confidential Department information;
    - chain letters; and
    - material that would be offensive to a reasonable person;
- transmit any electronic message in violation of file size restrictions;
- use Department computer equipment or network to send or receive electronic communications for non-Department business;
- use computers, networks, or electronic communications to infringe on the copyright or other intellectual property rights of the County or third parties;
- send or receive commercial software in violation of its license agreement;
- copy personal files, programs, or images into any Department computer without authorization from their Unit Commander;
- send anonymous messages or represent themselves as someone else, real or fictional, or send messages or images which are defamatory, fraudulent, threatening, harassing, sexual or contain derogatory racial or religious content;
- establish any hidden or misidentified links on any web page;
- send or forward messages which have been altered in order to deceive the receiver as to the original content;
- use Department computers, networks, software, or electronic communications for personal financial, commercial, political, or other personal use;
- use electronic communications to intimidate, embarrass, cause distress, or otherwise force unwanted attention upon others or to interfere with the ability of others to conduct Department business or create a hostile work environment;
- use electronic communications in competition with commercial services to individuals or organizations outside the Department;
- use electronic communications for the purposes of gambling, including but not limited to, lotteries, sports pools, and other personal wagering; and
- give out employee personal information such as home address and/or telephone numbers.

3-07/220.20 CALIFORNIA DEPARTMENT OF JUSTICE ADMONISHMENT

As an employee of the Los Angeles County Sheriff's Department, you may have access to confidential criminal record and/or Department of Motor Vehicles record information which is controlled by statute. Misuse of such information may adversely affect the individual's civil rights and violates the law. Penal Code Section 502 prescribes the penalties relating to computer crimes. Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code Sections 11140 - 11144 and 13301 - 13305 prescribe penalties for misuse of criminal history information. Government Code Section 6200 prescribes the felony penalties for misuse of public records and CLETS information. Penal Code Sections 11142 and 13303 state:

> "Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."

California Vehicle Code Section 1808.45 prescribes the penalties relating to misuse of Department of Motor Vehicles record information.

Any employee who is responsible for such misuse is subject to disciplinary action. Violations of this law may also result in criminal and/or civil actions.

3-07/230.00 DATA COMMUNICATIONS MANAGEMENT

Data Systems Bureau is responsible for overall access and administration of electronic data communications policy and procedures for traffic occurring over the Sheriff's Data Network, the Justice Data Interface Controller (JDIC) to the Internet, and to any other Department-authorized data interfaces. In this role, Data Systems Bureau will:

- review and approve requests for access to the Sheriff's Data Network or JDIC. Requests for such access should be made to the Central Help Desk;
- review and act on all requests to receive e-mail. Requests for e-mail should be made to the Central Help Desk;
- review and act on requests from LASD users to install new equipment, hardware or software connected to the Sheriff's Data Network. Such requests should be made to the Central Help Desk;
- review and select the Department's Internet provider and generate and maintain documentation where the provider is, other than the County's Internal Services Department;
- review requests and provide remote access to the Sheriff's Data Network for individual Department members. Requests for such access must be submitted on office correspondence (SHAD 32) from the requestor's Unit Commander to the

concerned Division Chief or Division Director. Requests must include the need for remote access;

- specify the software required for usage with computers connected to the Sheriff's Data Network and ensure its usage on all such computers;
- establish the standards for all Department IT resources including personal computers, printers, scanners, and network equipment for the Department;
- establish and purchase the standard software suite for Department computers, including desktop and network operating systems, virus scanning, e-mail, faxes, word processing, spreadsheet, graphics, database, and network management software; and
- review and act on requests to use encryption technology by Department members and ensure its use by only those approved to do so. Requests to use encryption technology must be submitted on office correspondence signed by the requestor's Division Chief, Division Director, or above, and directed to the Captain of Data Systems Bureau.

3-07/240.00 CENTRAL HELP DESK

The Central Help Desk is the main point of contact for questions and issues relating to information technology and related equipment. Issues may be reported to the Central Help Desk via telephone, e-mail, or preferably, through an Intranet site accessible through the Sheriff's Department Network – http://myhelpdesk/.

3-07/250.00 LASD USER AUTHORIZATION AND ACKNOWLEDGMENT OF POLICIES AND GUIDELINES

Authorized persons will be responsible for reading and signing the Sheriff's Department "User Acknowledgment of Electronic Communications Policy" form before obtaining authorization to access the Sheriff's Data Network. The Department form requires a counter signature by the user's supervisor at the rank of Sergeant or higher. An authorized persons may request authorization to access the Sheriff's Data Network by submitting the request as described under the manual section entitled, Data Communications Management (section 3-07/230.00), and attaching the signed user acknowledgment form.

User Acknowledgment of Electronic Communications Policy

I understand that the Los Angeles County Sheriff's Department requires each user, who has access to automated data communications, be responsible for adhering to its electronic communications policy sections as set forth in the Manual of Policy and Procedures, section 3-07/200.10 through section 3-07/250.00 inclusive. I have received a copy of these sections of the Manual of Policy and Procedures.

I understand that I must not have an expectation of privacy when using County electronic communications and acknowledge that my electronic communications may be monitored at any time by authorized employees.

By signing this form, I agree to abide by all policies, including State statutes relating to electronic communications and use of information, and understand that I will be held accountable for my actions and that disciplinary actions may result from not abiding by these policies. I also agree to give authorized persons, including supervisors, auditors, and investigators access to my equipment, software, and files at reasonable times for the purposes of investigating compliance.

User Name (PRINT)	User Signature	Date

As a supervisor, by my signature, I acknowledge my responsibility to have provided the electronic communications policies, section 3-07/200.10 through section 3-07/250.00 inclusive, to the above user. I also acknowledge that I am responsible for ensuring that the above user, whom I supervise, has read and understands this policy.

Supervisor's Name (PRINT)	Supervisor's Signature	Date

3-07/260.00 INFORMATION TECHNOLOGY – POLICIES, STANDARDS, AND SECURITY

Information Technology has become a core component within the Sheriff's Department, to enhance the Department's crime fighting mission, to share vital information among Units and among various criminal justice agencies, and to improve efficiency in administrative duties.

Hereafter, in this policy, standards shall include Information Technology policies, standards, guidelines, and procedures.

Establishing standards in both equipment and procedures will enable the Department to:

- share information within the Department, with other criminal justice agencies, and with anti-terrorism task forces;

- efficiently operate the Department's growing Information Technology infrastructure by ensuring individual implementations are the best suited for our mission and compatible throughout the Department;
- allow technical personnel to become proficient in standard technologies;
- improve migration to new technologies through an ability to coordinate a migration throughout the Department; and
- improve security by creating an environment wherein an effective multi-layered security system can be implemented.

Security has also become a vital part of Information Technology. As criminal justice agencies have expanded their use of technology, intrusion attempts have also increased. It is critically important to integrate multi-layered security in the entire Information Technology infrastructure.

3-07/260.10 STANDARDS

Data Systems Bureau is responsible for selecting standard hardware, software, and configurations for use within the Sheriff's Department, and is also responsible for coordinating those selections with the standards established for the County. These standards may be found on Data Systems Bureau's Policy/Standards/Guides web page.

All technology procurements must meet current standards, except as specifically exempted by Data Systems Bureau. In order to better standardize and secure the Information Technology infrastructure, all technology procurements must be reviewed by Data Systems Bureau and receive a Data Systems Bureau Approval Code. Further information may be found on Data Systems Bureau's Policy/Standards/Guides web page.

3-07/260.20 SECURITY

The Sheriff's Department shares information and operates systems that support both Department members and numerous other agencies. Accordingly, Data Systems Bureau is responsible for establishing security standards for the Department that meet Department, County, State, and Federal requirements. Security standards affect users, hardware, software, and configurations.

All authorized persons are required to meet the security standards, except as specifically exempted by Data Systems Bureau. Specific information regarding current standards, including needed security software and/or configurations, may be found on the Data Systems Bureau's Policy/Standards/Guides web page or by contacting the Central Help Desk.

3-07/260.30 ACCESS TO ELECTRONIC COMMUNICATIONS AND ACCESS RECORDS

For the purpose of this section, “electronic communications and access records” includes all such records maintained or managed by the Sheriff’s Department. It includes, but is not limited to:

- e-mails;
- internet access records, including any electronic transactions conducted using the Department’s internet access;
- records of electronic requests sent through the Justice Data Interface Controller (JDIC); and
- records or electronic requests sent through systems maintained by the Department.

The order does not mandate maintenance of any records of electronic communications, nor does it modify or supersede any rule, regulation, or law regarding the retention of those records. This order only establishes a procedure to request and process access to such electronic communications records that are maintained or managed by the Sheriff’s Department.

Request for access to electronic communications and internet access records may be made by any Division Chief or Division Director or person of higher rank. The request must include the following:

- name and rank of the requestor (concerned Division Chief ,Division Director or higher);
- name and rank of the investigator authorized to receive the record(s);
- name(s) and employee number(s) for the record(s) requested;
- type of record(s) requested;
- dates of the record(s) requested; and
- reason for the request. If the reason is for investigation, the request should include an IAB number, WCSCR number, POE number, and/or an URN. Valid reasons may also include inquiries, administrative reviews, and/or audits.

<u>Additional Persons Authorized to Initiate Requests for Electronic Records</u>

Based on a need for immediate response and/or an anticipated volume of requests, the following are exempted from the requirement for Division Chief, Division Director, or higher authorization. Under these exceptions, the designated person may make the request directly to the Data Systems Bureau Unit Commander or designee.

- Homicide Bureau: if investigations require immediate access to electronic records to pursue a homicide investigation, an on-duty Homicide Lieutenant may authorize the request. The Homicide Lieutenant must provide justification for the immediate need;
- Internal Affairs Bureau (IAB): if investigators require access to electronic records to pursue an internal administrative or criminal investigation, the IAB Captain or

Lieutenant may authorize the request. The requestor must provide an IA investigation number, URN, or other justification;

- Internal Criminal Investigations Bureau (ICIB): if investigators require access to electronic records to pursue an internal administrative or criminal investigation, the ICIB Captain or Lieutenant may authorize the request. The requestor must provide an IA investigation number, URN, or other justification;
- Civil Litigation Unit (CLU): if investigators require access to electronic records in anticipation or preparation for a claim or lawsuit involving the Department, the Risk Management Bureau Captain or Lieutenant may authorize the request. The requestor must provide identifying information about the claim or lawsuit; and
- Other emergency requests: other emergency requests may be authorized by the Unit Commander of Data Systems Bureau or designee upon presentation of sufficient explanation to justify the emergency.

Upon retrieval, an electronic copy of the requested records shall be made. The copy shall be released to the identified investigator. This copy may be maintained as long as needed for the investigation, inquiry, audit, or review. Any purge date on the original record shall not be changed without Data Systems Bureau Unit Commander's approval, however, a verified copy shall be maintained until released for deletion by the requestor, or his/her agent.

Once retrieval has been completed, handling personnel shall notify the following:

- requestor;
- investigator authorized to receive the record(s); and
- Data Systems Bureau Unit Commander or designee.

All incoming requests and retrievals shall be logged by the Data Systems Bureau including all information required for the request.