Chapter 10 - Technology and Support Division

• 2-10/000.00 - Technology and Support Division

This chapter outlines the functions, responsibilities and jurisdiction of the Technology and Support Division.

• 2-10/005.00 - Functions and Responsibilities

The Technology and Support Division (TSD) is comprised of Communications and Fleet Management Bureau, Data Systems Bureau, Records and Identification Bureau, Scientific Services Bureau, and Office of Technology Planning.

This division supports the entire Department in the application of science, technology, and innovation services to public safety which includes: radio, cellular, and data communications; fleet maintenance and management; information technology, including operating secure networks, hardware, and data centers; official records and biometric identification; forensic sciences, including crime scene investigations; and other law enforcement technologies, such as automated license plate readers and fixed wearable camera systems. TSD's vision and strategy is to provide effective information technology solutions to improve the Department's business decision making ability, create innovative approaches to improve business processes, and enhance public trust through information transparency.

• 2-10/010.00 - Information Technology Governance

The Department employs centralized governance to managing all information technology (IT) projects as defined in section 2-10/015.10. The governance process ensures that all IT projects are properly identified, vetted, prioritized, and implemented in accordance to the Department's strategic goals and protocols.

The information technology governance is managed by the Department's Chief Information Officer, the Chief Technology Officer, and the Office of Technology Planning (OTP).

Effective IT governance will:

- Provide a strategic and centralized approach to addressing the Department's increasingly complex IT requirements;
- Provide a process to resolve issues of competing interest within the IT domain;
- Establish procedures for initiating new IT projects;
- Prioritize IT projects based on Department needs and available resources;
- Identify standards and protocols for Department IT solutions;
- Identify and track all current and developing IT programs to ensure system compatibility and nonâ€‘duplication of effort;
- Provide technical IT expertise/support as needed;
- Ensure the Department's IT efforts are coordinated with the Los Angeles County Chief Information

Office;
- Enforce adherence of the IT governance process;
- Grant approval for all IT projects;
- Ensure a unified Department effort in the development, implementation, vetting, and function of Department-wide IT projects;
- Ensure the Department's IT strategy and individual IT projects are coordinated with the County's strategic IT plan; and
- Report and track the status of IT projects.

• 2-10/010.01 - Department Chief Information Officer

The chief of Technology and Support Division (TSD) shall serve as the Department's Chief Information Officer with oversight responsibility to ensure that all technology programs and efforts are consistent with the Department's information technology (IT) goals. He or she shall be at the executive level of the Department and serves as the focal point for all IT projects and/or initiatives for the Department.

The Chief Information Officer's role is:

- To provide vision and leadership for developing and implementing IT initiatives; and
- To direct the planning and implementation of enterprise IT systems in support of business operations in order to improve cost effectiveness, service quality, and business development.

The Department's Chief Information Officer is responsible for:

- All aspects of the Department's IT and systems;
- Leading IT strategic and operational planning to achieve business goals by fostering innovation, prioritizing IT initiatives, and coordinating the evaluation, deployment, and management of current and future IT systems across the Department;
- Developing and maintain an appropriate IT organizational structure that supports the needs of the Department;
- Establish IT Department goals, objectives, and operating procedures;
- Approving, prioritizing, and controlling projects and the project portfolio as they relate to the selection, acquisition, development, and installation of major information systems;
- Defining and communicating policies and standards for acquiring, implementing, and operating IT systems;
- Ensuring IT systems operation adheres to applicable laws and regulations; and
- Promoting and oversee strategic relationships between internal IT resources and external entities, including agencies, vendors, and partner organizations.

• 2-10/010.02 - Technology Approval and Governance Board

The Technology Approval and Governance Board (TAGB) is comprised of the Sheriff, Undersheriff, and

assistant sheriffs. The Chief Information Officer [Technology and Support Division (TSD) chief] will serve as the executive director to the board.

The TAGB shall provide oversight of information technology investments by evaluating and approving proposed actions related to information technology (IT) risk, investment, and prioritization of projects and services. This board will deliver business value by aligning IT initiatives and operations to the current and future strategic objectives of the Department.

Additionally, this oversight ensures business units are effectively supported and have the technology they need to enable their goals.

Goals and responsibilities of the board are:

- To foster collaboration through shared accountability for IT investment, project, risk, and service decisions and performance;
- To foster IT success through shared accountability and established processes;
- To align funding and resource allocation through prioritization of IT projects in-line with the Department's strategic plan;
- To encourage continuous improvement of IT service performance and strategic use of IT by the Department;
- To establish Department-wide IT priorities, including new development and on-going maintenance;
- To facilitate collaboration among divisions with closely aligned requirements to ensure synergies and cost savings;
- To work in concert with the Chief Information Officer to determine feasibility and impact of IT initiatives to existing Department operations;
- To communicate directions or decisions throughout the organization;
- To evaluate the IT governance process at the end of each year to determine if changes are needed; and
- To approve the allocation of financial and personnel resources to support IT.

Goals and responsibilities of the executive director are:

- To advise TAGB on the long-term technology strategic plan and ensure alignment with business strategic goals;
- To provide cost analysis and long-term sustainability of IT investments reports for TAGB approval;
- To provide technology project portfolio to TAGB for approval and prioritization; and
- To make recommendations on project approach, direct on effective resource management, and seek approval for funding and prioritization.

• 2-10/010.03 - Office of Technology Planning

The Office of Technology Planning (OTP) serves as a clearinghouse and advisory group for all Department information technology (IT) projects. OTP is an integral component of the Department's information technology governance process.

The Chief Technology Officer oversees all the functions of the OTP which is comprised of the following offices:

- Chief Data Office (CDO)
- Project Management Office (PMO)
- System Architecture Office (SAO)

Each office is an integral piece of the OTP to provide customer service to Department business units.

• 2-10/010.04 - Chief Technology Officer

The Chief Technology Officer reports directly to the Chief Information Officer. The Chief Technology Officer's role is:

- Manage the Office of Technology Planning (OTP) operation;
- Work with executive management to nurture the organization through the use of technological resources; and
- Manage and have oversight on information technology (IT) governance implementation, project management, data management, and system architecture.

The Chief Technology Officer is responsible for the following:

- Development of the Department's long-term IT strategic plan;
- Ensure all technology practices adhere to best practice standards;
- Perform as the IT advisor to the Department's Chief Information Officer;
- Perform as the liaison between the Department and the Los Angeles County Chief Information Office to ensure collaboration and consistency with County technology polices;
- Oversight with County approved technology agreements; and
- Manage the related IT matters through the Chief Officer/Chief Executive Officer process.

• 2-10/010.05 - Chief Data Office

The Chief Data Office (CDO) provides data oversight and management, enterprise data governance, and Department-wide data stewardship for technology and business-related projects. The CDO is managed by the Chief Data Officer. They report directly to the Chief Technology Officer and executive leadership to ensure data is being developed as a viable resource for current and future needs both inside and outside of specific information technology (IT) systems.

The Chief Data Officer is responsible for the following:

- Acts as the principle data trustee for the Department;
- Develops and implements data standards, practices, and technologies which build the foundation to create an Enterprise Information Management Program;
- Works closely with the Chief Information Officer and business subject matter expert (SME) to develop

data quality metrics, measures, and practices to improve the Department's data and to protect sensitive information;
- Develops, organizes, and implements data management standards, policies, and practices that outline and enforce rules of engagement, decision rights, and the accountabilities for the effective management of information assets to support the mission of the Department;
- Oversees enterprise entity repository, data catalog, and publishing primary identifiers;
- Reaches out to industry, academics, other branches of government, and the public to promote the Department’s data and data services;
- Attend events to promote the Department’s data;
- Develops collaborations that further development of data products and services that speed communication products and innovations to market;
- Manages open government data activities;
- Evaluates, designs, and implements common technologies and information management best practices that maximize County investments and reduce project and operating costs;
- Responsible for data reform and modernization for "fact-based, data-driven” decision-making; and
- Collaborates with the Department's and County's various information sharing projects and initiatives to create an information management strategy and to create data standards that facilitate information sharing and management.

• 2-10/010.06 - Project Management Office

The Project Management Office (PMO) is managed by the Project Management Officer, who reports directly to the Chief Technology Officer and executive leadership. The PMO provides project oversight, project control, and project support for technology related projects and pilots. The PMO will ensure the Department is investing in the right technology, realizing the promised (or expected) benefits, and monitoring successful implementation within the timeframe and budget allocated.

The primary mission of the PMO is:

- To ensure sustainable governance for project portfolio structure and project status oversight, including post-development lifecycle oversight;
- To ensure system compatibility amongst the various information technology (IT) solutions;
- To prevent duplication of effort;
- To provide a consistent approach to project initiation, approval, monitoring and reporting;
- To improve efficiencies within the IT domain;
- To develop IT system standards/protocols; and
- To assess new IT projects to determine their value and impact on the Department’s operation.

The Project Management Officer is responsible for the following:

- Reviews Department IT project proposals to ensure optimum effort, adherence to established standards, and compliance to County procurement guidelines;
- Facilitates the establishment of IT project management guidelines, processes, and standards;

- Facilitates the establishment of performance measures and project status/reporting tools;
- Compiles and reviews IT requests for information (RFI), requests for proposal (RFP), and statements of work (SOW) prior to submission;
- Organizes technical experts into a project review team to help the project manager complete a successful project;
- Acts as liaison with the Los Angeles County's Chief Information Office;
- Acts as liaison with the Los Angeles County's Information Systems Advisory Body (ISAB);
- Maintains the Department's IT inventory, project portfolio, and the County-mandated Business Automation Plan (BAP);
- Reports directly to the chief of Technology and Support Division;
- Recommends and develops a strategic IT plan and other IT-related administrative reports with the Department's Chief Information Officer; and
- Coordinates technology activities performed in all parts of the Department to avoid redundancies.

• 2-10/010.07 - System Architecture Office

The System Architecture Office (SAO) works in support of the Department's Chief Information Officer and reports to the Chief Technology Officer to develop strategic plans for the coordinated development, implementation, and maintenance of current and emerging information technology (IT) solutions.

The SAO is responsible for the following:

- Provides overall enterprise architecture oversight, enterprise-wide strategic planning, acts as a clearing house for innovation to support technology related projects and pilots, and interacts with vendors for both innovation and business fit needs.
- Makes recommendations on the development of IT strategic planning, tracking technical trends, new projects research, adopting and driving emerging technologies, managing enterprise architecture, vendor management, and evaluation of in-house development vs. outsourcing;
- Legacy application modernization, and system consolidation;
- Implement architectural standards;
- Identifies and tracks Department technology programs and provides a central knowledge base of efforts and technologies;
- Provides support to the Chief Technology Officer, Chief Data Officer, and Project Management Officer with regards to IT strategic architectures as they relate to new and emerging IT projects being submitted for consideration;
- Reviews and makes recommendations on products, services, and technical architectures that support data within the Department;
- Identify an end-to-end approach for information management from intelligent data capture, to master and data quality management;
- Adopt a strategic approach to IT architecture, as well as develop and implement data sharing policies and standards; and
- Identify opportunities to reduce information sharing project and operating costs using adopted data sharing and exchange standards, practices, and technologies.

• 2-10/015.00 - Information Technology (IT) Projects Defined

An Information Technology (IT) project is defined as:

- any process or implementation of hardware and/or software that is connected, by any method, to the Sheriff's Data Systems Network or software that analyzes, retrieves stores or transmits data across any Sheriff's data or voice communication system;
- any process or implementation of hardware and/or software that is operated by the Department to support criminal justice efforts throughout the Los Angeles County region or with other agencies outside the region;
- computer hardware, networking software, data cabling, bandwidth and new applications of existing LASD technologies or data that is utilized on a Unit or Bureau-Level;
- nonâ€'Department owned data, network, audio or video system that is designed, managed, or maintained by Department personnel (Federal, State, or public domain);
- conversion of data, computer programming, information storage and retrieval and data transmission;
- any IT device requiring installation, maintenance or technical support from any of the Department's IT units at any time during the life of the project; and
- any Departmental data connection with any other agency or department.

• 2-10/015.10 - Mandatory Reporting and Approval of Information Technology (IT) Projects

All proposed information technology (IT) projects must be submitted to the Technology and Support Division's Office of Technology Planning (OTP) prior to acquisition, development, enhancement, or implementation. No IT project will be funded, implemented, or available for use without having been first vetted through the information technology governance process. This includes those projects wherein the funding originates from grants and/or other specialized accounts. All IT projects are subject to the following governance process:

- The division/executive sponsor of an IT project or their representative shall submit the project proposal to the chief of Technology and Support Division (TSD);
- The OTP and requesting division's project manager will review and discuss the project's purpose, readiness, and direction;
- OTP will assemble a team of IT technical experts in order to conduct a technical analysis and review to support business needs;
- During this process, OTP will review possible alternatives, if any, and will prepare recommendations for the chief of TSD; and
- Upon final approvals, the OTP will facilitate the project development, as needed.

Any deviation from this policy will require a memorandum from the unit commander to the chief of TSD explaining the justification for bypassing the IT governance process.

• 2-10/020.00 - Jurisdiction

While the services provided by Technology and Support Division are primarily designed to support Departmental operations, many of its functions and services now extend outside of the Department. Official records are available to personnel of other public agencies. Among these systems, Technology and Support Division operates the Justice Data Interface Controller (JDIC) for the Criminal Justice System of the County with the exception of the Los Angeles Police Department and California Highway Patrol, the Countywide Warrant System (CWS), the Automated Fingerprint Identification System, which is used by all local law enforcement agencies, and law enforcement information sharing systems and efforts.

• 2-10/030.00 - Communications and Fleet Management Bureau

Communications and Fleet Management Bureau provides for quality communications vehicles, and vessels in a cost-effective manner to support the operations of the Department. The bureau is comprised of eight primary units:

- Communications Center/Radio Room:
- Fleet Management Unit;
- Interoperability Section;
- Mobile Solutions Section;
- Communications Solutions Section;
- MDCS Training Unit;
- Data Solutions Section; and
- Information Technology Section.

Disaster Communications Service Unit which is managed by the Communication Center/Radio Room.

This Bureau is responsible for:

Communication Center/Radio Room

- Delivery of radio communicating services;
- Computer Aided Dispatch (CAD) system specialists;
- Alarm system central monitoring for Los Angeles County facilities (aka “Manitou Alarms”);
- Emergency Alert System (EAS) activations;
- AMBER alerts;
- Coordination of “Alert LA” activations (shared responsibility with EOB);
- Assignment of radio call numbers;
- Custody of voice and digital radio transmission records;
- Initiating voice interoperability system for LARTCS (Los Angeles Regional Tactical Communications System);
- Tactical radio channel management;
- After hour’s notification for Department vehicle tow; and
- Monitoring and coordinating of “3SI” tracking and “ETS” systems.

Fleet Management Unit

- Budgeting for replacement of vehicles, vessels and related equipment;
- Preparing specifications for the lease or purchase of vehicles, vessels, accessories and equipment;
- Pre-purchase evaluating and testing of equipment;
- Prioritizing and expediting equipment repairs;
- Reporting of statistics on fleet operations;
- Maintaining vehicle inventory records;
- Maintaining vehicle take home authorization records;
- Maintaining fuel supply and usage records;
- Functioning as liaison between Sheriff's Department, and vehicle/vessel maintenance contractors;
- Coordinating the assignment and replacement of vehicles and vessels; and
- Conduct annual inspections of station/unit fleet.

Interoperability Section

- LARTCS (Los Angeles Regional Tactical Communications System) program;
- LARICS (Los Angeles Regional Interoperability Communication System) program management;
- Mutual aid coordination and memorandum of agreements with outside agencies;
- CAL-SEIC coordination;
- Operational coordination of Department Mobile Interoperability Units (MCU);
- Coordinating and responding on FCC matters and policy; and
- Tactical communications responses.

Mobile Solutions Section

- Mobile Digital Computer (MDC) program management;
- Evaluation and implementation of new mobile technologies; and
- In-car video.

Communications Solutions Section

This section provides support in four major areas: oversight of the Department’s communications infrastructure and systems engineering, radio services (repair and maintenance), cellular phone and radio inventory control, and telecommunications. These responsibilities include Department vehicles, Sheriff’s stations, other County facilities and communications sites.

- Identifying and resolving communications problems;
- Budgeting for the Department’s communications infrastructure costs;
- Planning and facilitating assistance with portable radios and cellular telephone communications for special events and other Department needs;
- Coordinating the planning, purchasing, installation and maintenance of communications sub-systems in liaison with other County entities (i.e., Internal Services Department, Sheriff’s facilities, etc.);
- Radio programming;

- MDT support (limited to repair and replacement of MDT's);
- Department issued calling cards;
- Issuance, billing, and tracking of cellular devices;
- Repair, replacement and maintenance of all mobile communications equipment for the entire Department, to include but not limited to; voice and data radios (portable and mobile), mobile digital terminals (MDT's), mobile digital computers (MDC) first point of contact for repairs, siren controls, base stations, etc.;
- Testing and evaluation of new communications related equipment, such as new mobile and portable radios, MDT's, and other communications systems;
- Develop, fabricate, and test special and experimental electronics equipment;
- Develop, test, and implement Sheriff's voice radio channel plans for all portable, mobile and base station radios; and
- Managing the Department Service Order Account (DSO) and Service Level Agreement (SLA) as it relates to the communications infrastructure, maintenance, new projects, expenditures, and billing.

MDCS (Mobile Digital Communications System) Training

- Training personnel in the use of the Computer Aided Dispatch (CAD) equipment, to include station desk operations (complaint, dispatch, and watch deputy), mobile computing, and E-911 answering equipment;
- Develop and provide training for MCU participants;
- Conduct annual inspections of station/unit desk operations;
- Training for patrol school, security assistants, and security officers;
- Assist in evaluation of equipment for station desk and patrol use;
- Assist HelpDesk resolution of issues related to CAD, MDT, and MDC;
- Adding and verifying users to MDT/MDC systems;
- Research, develop, and deploy elearning (LMS) products related to CAD, MDT, MDC, and other CFMB products;
- Liaison with JDIC and other Data Systems Bureau training elements; and
- Function as Bureau LMS Coordinator.

Data Solutions Section

- Advance Surveillance and Protection Unit (ASAP) program management;
- Bureau reserve/volunteer program management;
- Quality assurance programs; and
- Advanced planning.

Information Technology Section

- Maintaining, evaluating, enhancing, upgrading, and replacing components of the Mobile Digital (Data/Voice) Communications System (MDCS);
- Computer Aided Dispatch (CAD) system management;
- Data center liaison;

- Technical advisory and support;
- Video alarms program management;
- Bureau website;
- Console Switch Interface system management;
- CSI WAN Management; and
- NG911 coordination.

• 2-10/035.00 - Station/Bureau Desk Operations Standards and Guidelines

Central Coordinating Authority/Responsibility

- Communications and Fleet Management bureau shall have central coordinating authority for all hardware, software, and communication devices installed in station desk areas regardless of funding source. This includes any audio, visual, data, or other IT equipment or software that may be installed in the station desk area (temporary or permanent) visible to the watch deputy and dispatcher. This is done to maximize officer safety, provide for a standardized physical layout of equipment for personnel, standardize workflow, and establish a standard baseline for cost estimates of future technology projects;
- As a central coordinating authority for desk operations, Communications and Fleet Management Bureau shall be consulted prior to any installation, modification, or alteration of anything related to desk operations. No technology item regardless of funding may be placed in the desk area without prior approval from Communications and Fleet Management Bureau; and
- These projects are still subject to guidelines set forth in MPP section 2-10/015.10, Mandatory Reporting of Information Technology (IT) Projects.

Station/Bureau Desk Operations Training

- Communications and Fleet Management Bureau shall have the central coordinating authority for training related to all facets of technological assets deployed at the desk. To maximize officer safety, service to the public, and maintain a standard of operation across the Department, any training related to station desk operations shall be vetted through Communications and Fleet Management Bureau.

Station/Bureau Desk Operations workflow Management

To maximize officer safety and standardize workflow, any potential increase in workload for station dispatchers and watch deputies (such as monitoring non CAD, CSI, Vesta, or GST systems) shall be vetted by Communications and Fleet Management Bureau.

• 2-10/040.00 - Data Systems Bureau

Data Systems Bureau plans, develops, coordinates and manages Information Technology (IT) for the Department - including systems and data connections supporting or interfacing with county, state, and federal criminal justice agencies.

This bureau ls responsible for:

- managing the IT infrastructure - consisting of servers, computers, terminals, networks and network equipment, software, applications, databases, and peripheral equipment;
- developing and implementing security measures and IT standards to ensure Departmental information and systems work efficiently and securely; and
- ensuring the IT infrastructure and IT usage meet mandated local, state, and federal standards.

Mainframe Systems Support

- providing maintenance services for the Department's large mainframe-base law enforcement systems (Automated Jail Information System, Countywide Warrant System, and Transportation Management Automation System); and
- providing the Department and participating agencies with an on-line and batch system to track individuals through the criminal justice process from the time of arrest or remand through release.

Sheriff's Data Network

- providing a high-speed data communications infrastructure which interconnects all Department sites;
- providing a mature, stable and robust network which will furnish a means by which all Units can access services and applications that are required to perform vital Department functions;
- providing liaison with the County and State Coordinators for Public Safety Answering Points and Wireless 9-1-1 telephone operations;
- providing liaison with the California Law Enforcement Telecommunication System Advisory Committee;
- ensuring systems meet California Justice Information Systems (CJIS) guidelines;
- managing systems/services including, but not limited to the following:
    - network connections and interfaces with other criminal justice agencies;
    - Department Voice over Internet Protocol (VoIP) telephone systems;
    - Department telecommunication equipment and lines, including data circuits, analog voice lines, and 9-1-1 equipment and lines;
    - Closed Circuit Television (CCTV);
    - Department e-mail;
    - office automation;
    - personal computer and file server support; and
    - help desk and computer training.

Systems Development Section

- providing various levels of technical staff support in the acquisition and/or development of new automated systems within the Department. More than 65 systems are maintained by staff;
- enabling rapid on-line access to the Regional Allocation of Police Service (RAPS) to report patrol activity for the purpose of providing the Department executives, Contract Law Enforcement Bureau, and Station Administrators with statistical data relevant to particular policing jurisdictions. RAPS serves as a management tool for deployment of Patrol Personnel, analysis of individual Unit performance, budgetary justifications and reporting to contract cities regarding levels of police services; and
- providing a Performance Recording and Monitoring System that is an integrated database for administrative investigations and service comment forms. It also includes a system to flag instances that

meet predefined criteria and thresholds. PRMS was originally comprised of three modules that automated the business processes of Internal Affairs Bureau, Civil Litigation, and Pitchess Motions. PRMS consolidates the information kept in these independent databases into an integrated database that serves as a Department-wide decision support system in matters related to risk management and service reviews.

Law Enforcement Information Sharing Program

The Law Enforcement Information Sharing Program (LEISP) handles the business and technical needs required to capture, organize, and share crime data and information, both within the Sheriff's Department and outside law enforcement agencies.

- the LEIS Section is responsible for the overall business and technical operations of the entire LEISP unit, along with the implementation of law enforcement applications such as COPLINK, LASDashboard and records management systems. A Help Desk is staffed to handle inquiries related to these applications as well as LARCIS (Los Angeles Regional Crime Information System), the current Records Management System for LASD;
- the Crime Analysis Program (CAP â€' formerly Management Information Services MIS) is responsible for:
    - mandated state and federal crime;
    - supervision of the collection of the Department's crime data;
    - prepare specialized crime studies and statistical reports;
    - handles all ad hoc requests for crime information;
    - the oversight and approval of all aspects of Geographical Information Systems (GIS) within the Sheriff's Department, including development of boundary layers, determination of mapping standards, and GIS software licensing;
    - the creation and maintenance of reporting districts, arresting agency identifiers, and statistical codes and the related automated system tables;
    - data proprietor of the Regional Allocation of Patrol Services (RAPS) system; and
    - directs all crime analysis services, including selection, training, and supervision of all crime analysts as well as development and implementation of new crime and intelligence services.
- the Crime Assessment Center (CAC) analyzes crime throughout the entire county, without regard to jurisdictional boundaries; and
- the Advanced Surveillance and Protection (ASAP) unit specializes in closed circuit video surveillance (CCTV), Automated License Plate Recognition (ALPR) systems, Acoustical Gunshot Detection Systems and Advance Command Center Integration. It oversees the procurement, installation, and maintenance of these systems.

Custody Automation

Jail issues, including medical and mental health, classification, overcrowding, erroneous release, and over detention, have been addressed from a technology perspective. A series of systems projects, both short-term and long-term, were identified to address the Custody issues. Major systems being implemented or maintained are:

- Jail Hospital Information System (JHIS) - JHIS provides complete, accurate, and accessible clinical

documentation to Medical Services. Using a customized version of hospital software package, an on-line medical record is available from any Custody facility. The system supports all the major functions of Medical Services, including patient care management, laboratory, radiology, pharmacy, mental health, dietetics, and other major processes. JHIS is fully integrated with AJIS.

- Jail Information Management System (JIMS) - JIMS is a multi-faceted development project that was designed to address short-term needed system fixes while concurrently proceeding down an orderly development path towards a replacement Automated Jail Information System (AJIS).

Data Center Administration

The Data Center Administration Unit is responsible for physically hosting in a secure, climate controlled environment all elements of the Department's data processing and Information Technology infrastructure, including Sheriff's Data Network and Records and Identification Bureau equipment. Data Center Administration is further responsible for the ongoing management and operational support, at the hardware and operating system level, of all Department-wide computer systems. Many of these systems are considered mission-critical and must be available on a 7-days-a-week, 24-hours-a-day basis. To effectively manage these systems, Data Center Administration maintains multiple Departmental Data Centers in geographically separate areas.

• 2-10/050.00 - Records and Identification Bureau

Records and Identification Bureau (RIB), comprised of both sworn and professional personnel, provides a crucial service for the Department. Its core responsibilities focus on the archival, retention, and release of the Department's records, totaling over 19 million crime reports and booking jackets stored in the Sheriff's Electronic Criminal Documents Archive (SECDA). Additionally, RIB oversees essential services such as fingerprint identification, warrants, subpoenas, and the registration of arson offenders through its Public and Law Enforcement Services (PALES) and Compliance and Specialized Services (CSS) Sections.

Compliance and Specialized Services (CSS) Section encompasses the following subsections and performs the following functions:

Countywide Warrant Processing:

- Manages the Countywide Warrant System (CWS).
- Enters, reactivates, and recalls Juvenile warrants in CWS.
- Enters, reactivates, and recalls Adult Mental Health warrants in CWS.
- Enters, reactivates, and recalls Adult/Juvenile Protective Custody warrants.
- Enters, reactivates, and recalls some Civil Bench warrants.
- Creates and recalls Grand Jury Indictments.
- Disseminates Second Abstracts via teletype.

- Serves as the point of contact for National and Local Law Enforcement for warrant information.
- Analyzes legislation and proposals concerning warrant entries.

Fingerprint Services:

- Conducts analytical fingerprint comparisons for local, state, and federal law enforcement agencies (excluding the Los Angeles Police Department), Department of Motor Vehicles and the Coroner's Office. Provides support for countywide warrant investigations and conduct identifications of unknown and deceased individuals using fingerprint and biometric records.
- Manually registers and maintains fingerprint information in the Automated Biometric Identification System (ABIS) for future comparisons.
- Ensures timely identification notifications are sent to booking locations and investigative units countywide.
- Conducts visual inspections and consolidates fingerprint-based records of subjects with duplicate SID numbers and MAIN numbers; and forwards this information to various agencies, including the California Department of Justice (DOJ).
- Maintains electronic, digital, and hard copy fingerprint files.
- Provides court testimony for fingerprint identifications and methods used for identification.
- Analyzes friction ridge images to determine the source of record with multiple identification numbers.
- Assists local law enforcement agencies with information corrections, coordinating with the DOJ.
- Provides information to jail staff regarding booking transactions and DOJ identification responses.
- Provides certified copies of fingerprint bookings and photographs to local, state, and federal law enforcement agencies.

Public and Law Enforcement Services (PALES) Section encompasses the following subsections and performs the following functions:

Applicant Processing:

- Provides local summary criminal history information to authorized city, county, state, and federal agencies for employment, permit, or licensing purposes.
- Provides copies of crime reports and booking jacket records to authorized agencies for the mentioned purposes, charging fees per California Penal Code section 13300(f).

Subpoena Control:

- Responds to criminal, civil, and administrative subpoenas, court orders, pre-sentences, prior convictions, and miscellaneous certification requests.

- Provides records in accordance with statutes and civil/criminal court rules.

Records Inquiry (Non-Law Enforcement):

- Responds to requests for police or accident reports, custody/booking information, or local summary criminal history information from authorized agencies, victim attorneys, and private individuals.

- Prepares various letters and provides crime reports and booking jacket information to relevant agencies.

Records Inquiry (Law Enforcement):

- Works exclusively with law enforcement agencies, California State Prisons, District Attorneys, and City Attorneys for criminal investigations, housing recommendations, and prosecutions.

- Disseminates information to facilitate investigations and prosecutions.

Sealing:

- Remove data from electronic Departmental databases to comply with legal requirements for sealing and destruction of adult and juvenile arrest records.

Public Services:

- Provides full-service public counter.

- Offers a range of criminal history-related services to private individuals and attorneys.

- Provides Livescan Fingerprint services, register arson offenders, and collect fees for these services in compliance with state law and County ordinances.

Additionally, RIB undertakes Special Projects as needed.

• 2-10/060.00 - Scientific Services Bureau

This Bureau is comprised of specialized sections with responsibilities as follows:

Biology Section

Laboratory Services

- identification of body fluids including blood, saliva and semen;
- determination of possible donors of evidentiary body fluid stains utilizing DNA testing

methods; and
- Combined DNA Indexing System (CODIS): Entry of DNA profiles in a database for search against profiles from known donors and other criminal cases.

Crime Scene Investigation

- Traceâ€'Biology Team - investigation of crimes against persons and some property crimes, including examination for and collection of biological evidence, trace evidence, impression evidence; conduct general evidence searches; and perform crime scene reconstructions.

Blood Alcohol Testing Section

Laboratory Services

- analysis of blood, urine, and beverage samples for alcohol concentration. Maintenance of breath alcohol testing instruments and instrument accuracy records. Train breath alcohol instrument operators. Provide expert testimony in DUI cases.

Controlled Substances Section

Laboratory Services

- examination and identification of solid dose controlled substances, including the examination of large drug seizures which require an appointment with the respective laboratory; and
- examination and identification of solid dose controlled substances and other evidence associated with the illicit manufacture of controlled substances.

Crime Scene Investigation

- Clandestine Laboratories Team – investigation of clandestine drug laboratories.

Evidence Control Section

- transports evidence between Bureau facilities and Stations, municipal police departments, and Central Property;
- accepts and releases evidence submitted to the Bureau; and
- maintains chain of custody records for evidence submitted to the Bureau.

Firearms Identification Section

Laboratory Services

- identification of bullets and cartridge cases to specific firearms; identification of type of firearm based upon expended bullets and/or cartridge cases; determination and function testing of full automatic firearms and silencers, determination of distance; serial number restoration; gunshot residue examination; and tool mark comparison; and
- National Integrated Ballistics Information Network (NIBIN) – entry of fired bullet and cartridge case information for search a National database.

Crime Scene Investigation

- Firearm Team – search for, collect, and interpret firearm and tool mark-related evidence to include bullet and cartridge case search and recovery, trajectory determinations, possible bullet strikes, and possible tool mark impressions. Provide expertise for the safe handling of unusual firearms.

Latent Print Section

Laboratory Services

- comparisons of friction ridge impressions to exemplar(s) of known persons for the purpose of making identifications and non-identifications;
- Automated Fingerprint Identification System (AFIS) – entry of latent finger and palm prints for search against a database of known finger and palm prints; and
- chemical processing – develop latent prints on evidence items utilizing chemicals, alternate light sources and digital imaging.

Crime Scene Investigation

- Major Crimes – investigation of crimes against persons such as homicides, rapes, robberies, or other crimes to include crime scene documentation, processing for latent prints, and casting of shoe and tire impressions. Crime scene documentation includes but is not limited to photography, aerial photography, video, sketches, diagrams, and three-dimensional laser scanning;
- Clandestine Laboratories – respond to clandestine laboratories to photograph and process evidence for latent prints; and
- Property Crimes – process property crimes or other crimes for latent prints where photography, videography or diagraming is not required.

Photo/Digital Imaging Section

- provides professional imaging services including processing, printing, storing, and maintain archives of film negative and digital images;
- complete public relations and/or evidence related digital photographic projects; and
- conduct studio photography of evidence, personnel, and Bureau operations.

Polygraph Section

- administers polygraph examinations in criminal investigations and pre-employment evaluations.

Quality Assurance and Training Section

- maintains the Bureau's international ISO/IEC 17025 accreditation program by conducting annual audits of accredited sections, ensuring court testimony monitoring, administering the proficiency testing program, issuing and following through on appropriate Corrective Action Requests, and calibrating and maintaining critical measuring devices;
- oversees the Bureau's Health & Safety Program by conducting appropriate audits, providing

appropriate training and certification;
- oversees the Bureau's volunteer/intern program; and
- coordinates all aspects of the Bureau's external training program.

Questioned Documents Section

Laboratory Services

- provides a comprehensive range of document examination services which include but are not limited to – handwriting, printing, typewriting, inks, charred paper, and obliterated and altered documents.

Toxicology Section

Laboratory Services

- analysis of blood and urine samples for drugs in evidence samples and employee random drug testing samples; and
- analysis of food and product tampering cases and cases of suspected poison.

Trace Evidence Section

Laboratory Services

- identification and/or comparison of trace evidence, including: hairs, fibers, paint, tire and footwear impressions, physical matches, tear gas and pepper spray, general chemical unknowns, gunshot residue (GSR), ignitable liquids and explosive residues.

Crime Scene Investigation

- Traceâ€'Biology Team - see Biology section; and
- Fire Debris / Explosives Team - investigation of crimes of arson or explosive evidence.

• 2-10/070.00 - Communications Equipment

Communications and Fleet Management Bureau has responsibility for communications equipment of all types. Requests to purchase, survey, install, alter, extend, remove, or any other request in regard to any Department JDIC, MDT/MDC, CAD, portable or mobile voice radio, public address system, intercom, or other electronic devices (such as GPS monitors, video feeds, etc.) shall be requested on a SH-AD-32A through the Department Chief Information Officer (CIO) – Chief of Technical Services Division.

This includes any and all installations of any items in the Station desk area.

Units are specifically prohibited from altering in any way the CAD, GST, VESTA, CSI, and any and all fallback radio equipment. Unit Commanders are responsible for ensuring the standard equipment assembly (CAD, CSI, GST, VESTA, and fallback radios) as installed by Technical Services Division is not altered in any way.

To maximize officer safety and efficiency, unit Dispatchers and Watch Deputies shall ensure that all Station

desk hardware and software is functional, operational, and all required users are logged on with the proper credentials. Specifically, they shall ensure that the CAD, CSI, 9-1-1 (VESTA), and GPS viewing units are functional, operational, and users are logged on with proper credentials.

The Station Dispatcher shall check the GST Viewer at least twice per shift as well as maintain constant vigilance to ensure that all GPS equipped units assigned to his or her Station are logged on and visible. If specific GPS equipped units are not visible to the Dispatcher on the GST Viewer, he or she shall contact the unit and ascertain the reason. If the Dispatcher and unit are not able to resolve the issue to become “visible” on the Dispatcher’s viewer, the unit shall contact the Central Help Desk for assistance. If the issue cannot be resolved at that level, the vehicle should be removed from service pending a response by technicians.

If the viewer is not functioning properly, the Dispatcher shall troubleshoot the issue to resolution according to training. If the issue is unable to be resolved at his or her level, he or she shall call the Central Help Desk and ensure a trouble ticket is generated.

Requests for telephones, additional directories and/or modifications of existing telephone equipment, shall be prepared on a Department Supply Requisition. Upon completion, send the form to the Telephone Coordinator, Communications and Fleet Management Bureau.

Any exceptions to this policy must be expressly in writing and kept on file at the Unit only after review by Communications and Fleet Management Bureau and Technical Services Division Chief.