Internal Audit Department

ORANGE COUNTY

AUDIT HIGHLIGHT JANUARY 13, 2015

INFORMATION TECHNOLOGY AUDIT
SHERIFF-CORONER
COMPUTER GENERAL CONTROLS
Audit No. 1353

WHY THIS AUDIT IS IMPORTANT

The Orange County Sheriff-Coroner Department (S-C) is a large, multi-faceted law enforcement agency served by approximately 4,000 sworn and professional staff members and over 800 reserve personnel. **Sheriff-Coroner/Information Systems Bureau** is managed by an IT Manager, who reports to the Support Services Director. The S-C Information Systems Bureau consists of approximately fifty (50) staff providing the following functions: Field Base Reporting (FBR) Project Manager, IT Project Manager Enterprise Applications, Infrastructure, and IT Project Manager CRM Applications. The S-C utilizes a number of systems including:

- ✓ Sheriff's Data System (SDS)/Automated Jail System (AJS),
- ✓ Enhanced Law Enforcement Telecommunications Emulator (ELETE),
- ✓ BMC Remedy AR Systems (Help Desk/Asset Inventory Reporting),
- ✓ Records Management System (RMS), and
- ✓ Computer Aided Dispatch (CAD) backup.

These systems store and process sensitive/confidential data including law enforcement operations involving criminal investigations, jail operations, undercover and forensic work. In addition, these systems interface with other key statewide and Department of Justice law enforcement systems. Therefore, restricting access to the systems and their data is a key priority.

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. If general controls are weak, they severely diminish the reliability of controls associated with individual applications. The audited IT general controls were found adequate.

WHAT THE AUDITORS FOUND

Successes

Our audit found that: (1) **adequate** security-related personnel policies have been developed; (2) **adequate** user access and physical access general controls were present to provide reasonable assurance that computer resources are protected from unauthorized personnel; (3) **adequate** configuration management, including change management, has been developed; (4) **adequate** segregation of duties exists within the IT organization; and (5) **adequate** policies and procedures for disaster recovery/business continuity have been substantially developed to help mitigate service interruptions and protect computing resources from environmental hazards.

Our audit identified **four (4) Control Findings** for security settings, change management policies and procedures, computer operations policies and procedures, and contingency planning.