FIRST FOLLOW-UP INFORMATION TECHNOLOGY AUDIT:

SHERIFF-CORONER COMPUTER GENERAL CONTROLS AS OF AUGUST 14, 2015

Audit Number 1353-F1 (Reference 1541) Report Date: October 22, 2015
ORANGE COUNTY
AUDITOR-CONTROLLER
INTERNAL AUDIT

Eric H. Woolery, CPA
Orange County Auditor-Controller

Toni Smart, CPA                              Director, Internal Audit
Michael Goodwin, CPA, CIA                   Assistant Director
Wilson Crider, CPA, CISA                    IT Audit Manager

12 Civic Center Plaza, Room 200
Santa Ana, CA 92701

Auditor-Controller Web Site
www.ac.ocgov.com
TO: Sandra Hutchens  
Sheriff-Coroner


We have completed our First Follow-Up Information Technology Audit of Sheriff-Coroner Computer General Controls as of August 14, 2015. Our final report is attached for your review.

I submit an Audit Status Report quarterly to the Audit Oversight Committee (AOC) and a monthly report to the Board of Supervisors (BOS) where I detail any critical and significant audit findings released in reports during the prior month and the implementation status of audit recommendations as disclosed by our Follow-Up Audits. Accordingly, the results of this Follow-Up Audit will be included in future status reports to the AOC and BOS.

Toni Smart, CPA, Director  
Auditor-Controller Internal Audit Division

Attachments

Other recipients of this report:  
   Members, Board of Supervisors  
   Members, Audit Oversight Committee  
   Eric H. Woolery, Auditor-Controller  
   Frank Kim, County Executive Officer  
   Mark Denny, Chief Operating Officer  
   Don Barnes, Assistant Sheriff, Administrative Services Command, Sheriff-Coroner  
   Brian Wayt, Senior Director, Administrative Services Command, Sheriff-Coroner  
   Kirk Wilkerson, Director, Support Services, Sheriff-Coroner  
   Ed Lee, Administrative Manager, Information Systems Bureau, Sheriff-Coroner  
   Jerry Soto, Administrative Manager, Information Systems Bureau, Sheriff-Coroner  
   Charles Ko, Database & Security Administrator, Sheriff-Coroner  
   Noma M. Crook, Director, Financial/Administrative Services, Sheriff-Coroner  
   Foreperson, Grand Jury  
   Robin Stieler, Interim Clerk of the Board of Supervisors  
   Macias Gini & O’Connell LLP, County External Auditor
# Table of Contents

*First Follow-Up Information Technology Audit: Sheriff-Coroner Computer General Controls Audit No. 1353-F1 (Reference 1541)*

As of August 14, 2015

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmittal Letter</td>
<td>i</td>
</tr>
<tr>
<td>Internal Auditor's Report</td>
<td></td>
</tr>
<tr>
<td>SCOPE</td>
<td>2</td>
</tr>
<tr>
<td>BACKGROUND</td>
<td>2</td>
</tr>
<tr>
<td>RESULTS</td>
<td>2</td>
</tr>
</tbody>
</table>
TO: Sandra Hutchens  
Sheriff-Coroner

FROM: Toni Smart, CPA, Director  
Auditor-Controller Internal Audit Division


SCOPE
We have completed a First Follow-Up Audit of Sheriff-Coroner Computer General Controls. Our audit was limited to reviewing actions taken as of August 14, 2015, to implement four (4) recommendations from our original audit.

BACKGROUND
The original audit found IT general controls were adequate and identified four Control Findings to enhance the Sheriff-Coroner’s computer general controls. 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. Sheriff-Coroner/Information Systems Bureau 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.

RESULTS
Our First Follow-Up Audit indicated that the Sheriff-Coroner implemented one recommendation and is in process of implementing three recommendations. Based on our First Follow-Up Audit, the following is the implementation status of the four original recommendations:

1. **Security Settings May Be Improved** (Control Finding)  
Sheriff-Coroner should consider changing the security settings to meet best practices.

   **Current Status:** Implemented. Our original audit reviewed Sheriff-Coroner network security settings and determined the settings could be improved to lessen the risk of an unauthorized access to the OCSD network. Our First Follow-Up Audit found the Sheriff-Coroner revised the network security settings to better align with access security best practices. Because network security settings were revised to meet best practices, we consider this recommendation implemented.
2. **Change Control Policies and Procedures Need to be Developed** *(Control Finding)*

Sheriff-Coroner should develop policies and procedures to address: vendor supplied passwords, embedded passwords, development environment, changes to network devices, personal and public domain software, and patch management.

**Current Status:** In Process. Our original audit determined adequate policies and procedures were not documented to address the items previously noted.

Our First Follow-Up Audit found that Sheriff-Coroner is in the process of developing an IT Operations Manual that will address among other items: vendor supplied passwords, embedded passwords, development environment, changes to network devices, personal and public domain software, and patch management. Because the IT Operations Manual is currently in draft form, we consider this recommendation in process.

**Planned Action:** The policies and procedures are in process of being developed and incorporated into the “Network and Security Services” section of the new IT Operations Manual. The project is on schedule to meet the 12 month estimated completion.

3. **Computer Operations Policies and Procedures Need to be Developed** *(Control Finding)* The Sheriff-Coroner should document and maintain its computer operation policies and procedures.

**Current Status:** In Process. Our original audit determined adequate policies and procedures were not documented to address the items previously noted.

Our First Follow-Up Audit found that Sheriff-Coroner is in the process of developing an IT Operations Manual that will address among other items: administrative procedures, application development & support, desktop services, network services and project management. Because the IT Operations Manual is currently in draft form, we consider this recommendation in process.

**Planned Action:** Sheriff-Coroner Information Systems Bureau is in the process of developing the new IT Operations Manual which covers operations, planning, network infrastructure, security services, help desk, administrative procedures, CLETS (California Law Enforcement Telecommunications System) administration and training areas. This project is on schedule to meet the 12 month estimated completion.

4. **Contingency Plans Need to be Updated and Tested** *(Control Finding)*

The Sheriff-Coroner should develop a plan for testing its disaster recovery and contingency plans on a regular basis.

**Current Status:** In Process. Our original audit determined the Sheriff-Coroner had not updated or tested its IT related business contingency plans within the last year.

Our First Follow-Up Audit found that Sheriff-Coroner is in the process of developing an IT Operations Manual that will address among other items: disaster recovery plan, backup and recovery procedures, incident response, emergency operations center activation, and disaster recovery plan testing. Because the IT Operations Manual is currently in draft form, we consider this recommendation in process.
**Planned Action:** Sheriff-Coroner Information Systems Bureau is in process of implementing an IT disaster recovery project. It will include remote disaster recovery sites with critical applications running on their local hardware. In addition, they are developing the disaster recovery test plan to regularly validate the recovery and contingency plan. This project is on schedule to meet the 24 month estimated completion.

We appreciate the assistance extended to us by Sheriff-Coroner personnel during our Follow-Up Audit. If you have any questions, please contact me directly at 834-5442 or Michael Goodwin, Assistant Director at 834-6066.