Internal Audit Report 2017-314

Riverside County Probation Department, Follow-up Audit

Report Date: March 27, 2017

Office of Paul Angulo, CPA, MA
Riverside County Auditor-Controller
4080 Lemon Street, 11th Floor
Riverside, CA 92509
(951) 955-3800

www.auditorcontroller.org

COUNTY OF RIVERSIDE
OFFICE OF THE
AUDITOR-CONTROLLER

County Administrative Center
4080 Lemon Street, 11th Floor
P.O. Box 1326
Riverside, CA 92502-1326
(951) 955-3800
Fax (951) 955-3802

Paul Angulo, CPA, MA
Riverside County Auditor-Controller

Frankie Ezzat, MPA
Assistant Auditor-Controller

March 27, 2017

Mark Hake
Chief Probation Officer
Riverside County Probation Department
3960 Orange Street, Suite 600
Riverside, CA 92501

Subject: Internal Audit Report 2017-314: Riverside County Probation Department, Follow-up Audit

Dear Mark Hake:

We have completed the first follow-up audit of Riverside County Probation Department. Our audit was limited to reviewing actions taken as of January 4, 2017, to correct the findings noted in our original audit report, Internal Audit Report 2014-008, dated September 22, 2014.

We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain reasonable assurance that our objective, as described in the preceding paragraph, is achieved. Additionally, the standards require that we conduct the audit to provide sufficient, reliable, and relevant evidence to achieve the audit objectives. We believe the audit provides a reasonable basis for our opinion.

The original audit report contained five recommendations, all of which required implementation to help correct the reported findings. Based on the results of our audit, we found that of the five recommendations:

- Two recommendations were implemented.
- Three recommendations were partially implemented.

Details of the findings from the original audit and the status of the implementation of the recommendations are provided in this report. For an in-depth understanding of the original audit, please refer to Internal Audit Report 2014-008 at www.auditorcontroller.org/Divisions/InternalAudit/InternalAuditReports.

AUDITOR CONTROLLER
COUNTY OF RIVERSIDE

Internal Audit Report 2017-314: Riverside County Probation Department, Follow-up Audit

We appreciate the cooperation and assistance provided by the staff of the Riverside County Probation Department during this follow-up audit. Their assistance contributed significantly to the successful completion of the audit.

Paul Angulo, CPA, MA
Riverside County Auditor-Controller

By: René Casillas, CPA, CRMA
Interim Chief Accountant

cc: Board of Supervisors
Executive Office
Grand Jury

Table of Contents

Information Security

Finding 1: Business Impact Analysis

Riverside County Probation Department (Probation) did not complete a business impact analysis for systems that support "highly available information" because they were not aware of the requirement. As a result, "highly available information," Probation requires in daily operations, may not be available in a timely manner.

Recommendation 1

Probation should ensure a business impact analysis is completed as required by Riverside County Information Security Information Management Standard.

Current Status: Partially Implemented

We were not provided with documentation confirming a business impact analysis was completed. After the original audit, Riverside County Information Technology Department (RCIT) was contracted to provide information technology support to Probation. Currently, Probation is working with RCIT to determine who will perform the business impact analysis.

Finding 2: Information Technology Devices Vulnerability

The equipment inventory listing (servers and workstations) obtained from the department did not agree with the listing extracted from the Information Security's Office (ISO) scanning software. The scanning software only captures equipment that are both connected and powered on.

Probation identifies which equipment is included or excluded from the scheduled monthly vulnerability scans. The Internet Protocol (IP) addresses of equipment that need to be scanned are defined in the ISO scanning software list of "Included Assets;" otherwise, they are defined in the ISO scanning software list of "Excluded Assets."

Our comparison of both equipment listings as of October 2013 revealed 91 of 790 (12%) devices consisting of 18 laptops, 69 desktop computers, and four servers were not scanned for vulnerabilities in October 2013; of these, six (7%) were not shown in the ISO scanning software report of "Included Assets" or "Excluded Assets," while 85 (93%) were shown in the ISO scanning software list of "Included Assets." Further, two desktop computers and 10 servers were scanned which were not on the department listing.

Probation indicated that these laptops were not usually connected to the network while two of four servers were excluded from the scan because they contain juvenile and adult clients' information. The rest of equipment was not scanned in October 2013, presumably because they were not connected and powered on.

Vulnerability management is a critical component of any security infrastructure because it enables proactive detection and remediation of security vulnerabilities.

Recommendation 2

Probation should ensure that equipment is powered on during the monthly vulnerability scanning schedule or perform an ad-hoc vulnerability scan for any equipment powered off.

Current Status: Partially Implemented

Probation is working with RCIT to determine who will retain responsibility for ensuring all computer assets are scanned during the monthly vulnerability scan.

Recommendation 2.1

Probation should ensure that new IP addresses/ranges of equipment are submitted to ISO and recorded in ISO scanning software list of "Included Assets" to ensure all equipment are scanned for vulnerabilities.

Current Status: Partially Implemented

Probation is working with RCIT to determine who will retain responsibility for ensuring updated listings of IP addresses assigned to computer assets are provided to individuals performing the monthly vulnerability scans.

Records Management

Finding 3: Written Procedures

Probation does not have written procedures on handling requests of department personnel information via "subpoenas." According to the department, all requests received by the front desk personnel are submitted to and approved by the human resource coordinator. Also, during our review, the department started developing a request log system, and indicated that they will develop written procedures on handling "subpoenas."

By not having up to date written procedures for the processing of personnel information requests, the risk of inadvertent disclosures of confidential or personally identifiable information outside the scope of the request increases and may result in personnel issues.

Recommendation 3

Probation should develop written procedures on handling personnel file information requests, including specific guidance for court requests such as "subpoenas."

Current Status: Implemented

Probation developed written procedures for handling requests of department personnel information via subpoenas. Procedures should reduce the possibility of unintentionally disclosing any confidential or personal information.

Finding 4: Untimely Record Destruction

Probation incurred unnecessary costs for retaining records beyond their required retention period. Employee hiring and selection records created during the period of 1980 to 2007 (PER 100, *Application and Selection Records*) and employee disciplinary records from January 1, 1997, to April 15, 2007, (PER 200, *Corrective and Disciplinary Actions*) were eligible for destruction in February 2008. Probation authorized the destruction of records on May 8, 2012. These official records should have been destroyed in February 2008 upon adoption of the County of Riverside General Records Retention Schedules (GRRS) but were not due to an oversight on the part of management.

Retaining records beyond the required retention period incurs unnecessary storage costs and exposes Probation to potential costs related to information requests.

Recommendation 4

Probation should establish policies and processes, including the assignment of accountability, for the review of their records on a periodic basis, and authorize the destruction of records in accordance with their County of Riverside Departmental Records Retention Schedules (DRRS) and the GRRS.

Current Status: Implemented

Probation developed and is utilizing written procedures for records retention management and disposition of records. Probation's records are periodically reviewed and properly authorized for destruction.