2 0

FINAL CLOSE-OUT SECOND AND FINAL FOLLOW-UP INFORMATION TECHNOLOGY AUDIT:

SOCIAL SERVICES AGENCY COMPUTER GENERAL CONTROLS

AS OF APRIL 30, 2014

Our Second Follow-Up Audit found SSA took appropriate action to implement one (1) recommendation remaining from our original audit concerning IT security reviews. Since SSA completed two of three security reviews and is working towards completing the third, we are closing this recommendation for purposes of follow-up. Previously, five (5) recommendations were implemented or closed in our First Follow-Up Audit dated October 15, 2013.

Because all recommendations are implemented or closed, this report represents the final close-out of the original audit.

AUDIT NO: 1142-F2 (REFERENCE 1359) ORIGINAL AUDIT NO. 1142

REPORT DATE: MAY 29, 2014

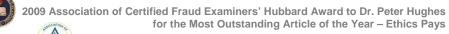
Director: Dr. Peter Hughes, MBA, CPA, CITP Senior Audit Manager: Michael Goodwin, CPA, CIA IT Audit Manager: Wilson Crider, CPA, CISA

RISK BASED AUDITING

GAO & IIA Peer Review Compliant - 2001, 2004, 2007, 2010

American Institute of Certified Public Accountants Award to Dr. Peter Hughes as 2010 Outstanding CPA of the Year for Local Government

GRC (Government, Risk & Compliance) Group 2010 Award to IAD as MVP in Risk Management



2008 Association of Local Government Auditors' Bronze Website Award





GAO & IIA Peer Review Compliant - 2001, 2004, 2007, 2010

Providing Facts and Perspectives Countywide

RISK BASED AUDITING

Dr. Peter Hughes Ph.D., MBA, CPA, CCEP, CITP, CIA, CFE, CFF, CGMA

Director Certified Compliance & Ethics Professional (CCEP)

Certified Information Technology Professional (CITP)

Certified Internal Auditor (CIA)

Certified Fraud Examiner (CFE)

Certified in Financial Forensics (CFF)

Chartered Global Management Accountant (CGMA)

E-mail: peter.hughes@iad.ocgov.com

Michael Goodwin CPA, CIA

Senior Audit Manager

Alan Marcum MBA, CPA, CIA, CFE

Senior Audit Manager

Hall of Finance & Records

12 Civic Center Plaza, Room 232 Santa Ana, CA 92701

Phone: (714) 834-5475 Fax: (714) 834-2880

To access and view audit reports or obtain additional information about the OC Internal Audit Department, visit our website: www.ocgov.com/audit



OC Fraud Hotline (714) 834-3608

Letter from Dr. Peter Hughes, CPA



Transmittal Letter



Audit No. 1142-F2 May 29, 2014

TO: Michael Ryan, Director Social Services Agency

FROM: Dr. Peter Hughes, CPA, Director

Internal Audit Department

SUBJECT: Second and Final Close-Out Follow-Up

Information Technology Audit: Social Services Agency Computer General Controls, Original Audit No. 1142, Issued February 19,

2013

We have completed a Second and Final Follow-Up Audit of Social Services Agency Computer General Controls. Our audit was limited to reviewing, as of April 30, 2014, actions taken to implement the **one (1) recommendation** remaining from our First Follow-Up Audit report dated October 15, 2013. We conducted this Second Follow-Up Audit in accordance with the *FY 13-14 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and Board of Supervisors (BOS).

The results of our Second Follow-Up Audit are discussed in the **OC Internal Auditor's Report** following this transmittal letter. Our Second Follow-Up Audit that found SSA took appropriate action towards implementing the one (1) recommendation remaining from our original audit concerning IT security reviews. Because SSA has completed two of three planned security assessments and is working with Xerox toward completing the third assessment, we are **closing this recommendation.** Previously, five (5) recommendations were implemented or closed in our First Follow-Up Audit. Because all recommendations are implemented or closed, this report represents the **final close-out of the original audit**.

Each month I submit an **Audit Status Report** to the BOS where I detail any material 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 audit will be included in a future status report to the BOS.

Other recipients of this report are listed on the OC Internal Auditor's Report on page 3.

Table of Contents



Second and Final Close-Out Follow-Up Information Technology Audit: Social Services Agency Computer General Controls Audit No. 1142-F2

As of April 30, 2014

Transmittal Letter	i
OC Internal Auditor's Report	1

OC Internal Auditor's Report



Audit No. 1142-F2 May 29, 2014

TO: Michael Ryan, Director

Social Services Agency

FROM: Dr. Peter Hughes, CPA, Director,

Internal Audit Department

SUBJECT: Second and Final Close-Out Follow-Up Information Technology Audit: Social

Services Agency Computer General Controls, Original Audit No. 1142, Issued

te Hughes

February 19, 2013

Scope of Review

We have completed a Second and Final Close-Out Follow-Up Audit of Social Services Agency Computer General Controls. Our audit was limited to reviewing actions taken, as of April 30, 2014, to implement the **one (1) recommendation** remaining from our First Follow-Up Audit report dated October 15, 2013.

Background

Our original audit of Social Services Agency's (SSA) Computer General Controls evaluated the following: 1) adequacy of SSA's security-related personnel policies; 2) adequacy of user access and physical access controls to provide reasonable assurance that computer resources are protected from unauthorized personnel and environmental hazards; 3) adequacy of SSA's systems development and change control policies to help ensure only authorized programs and authorized modifications are implemented, and errors are not introduced into programs when they are developed or subsequently modified; 4) whether an adequate segregation of duties exists within the IT organization; and 5) adequacy of policies/procedures for disaster recovery and business continuity to mitigate service interruptions.

The original audit identified **six (6) Control Findings** to enhance processes and controls by conducting annual security reviews; removing user access timely; maintaining user access forms; installing a surveillance system in the computer room; improving access controls to the computer room; and enabling the password complexity setting.

Results

Our Second Follow-Up Audit found SSA took appropriate action towards addressing the one (1) recommendation. As such, we are **closing this recommendation for purposes of follow-up**. The following is the implementation status of the six (6) original audit recommendations:

1. Annual Security Reviews Not Performed (Control Finding)

We recommend that SSA ensure system security reviews are performed at least annually.

<u>Current Status</u>: **Closed (Second Follow-Up Audit).** Our Second Follow-Up Audit found that SSA used Xerox to conduct security assessments on two of the three functional areas of the SSA environment, including the SLA3 servers hosted by Xerox at the OC Data Center and the SSA network. SSA received a quote from Xerox to complete a security assessment in the third functional area that includes all personal computers and SSA hosted servers; however, the initial quote was not acceptable to SSA. CEO/IT is working with Xerox and SSA to negotiate a more reasonable cost for this service.

OC Internal Auditor's Report



Because SSA completed security assessments in two areas and has assured us that is working with Xerox and CEO/IT to negotiate a cost for the third security assessment, we consider this recommendation closed for purposes of follow-up.

2. <u>User Access Removal Not Within Policy Timeframes</u> (Control Finding)

We recommend that SSA implement procedures and/or additional communications to ensure supervisors are notifying SSA Information Technology of separated users within 24 hours of their separation.

<u>Current Status</u>: **Implemented (First Follow-Up Audit).** SSA revised its employee separation policy and procedures to ensure employee access is removed in a timely manner. We verified the procedures were implemented by obtaining related email correspondence and confirming in monthly separation reports that SSA Information Technology is notified of separated users within 24 hours. Because SSA revised its employee separation policy and procedure, we consider this recommendation implemented.

3. <u>User Access Request Forms Prior to 2006 Were Not Retained</u> (Control Finding)

We recommend that SSA revise their procedures and ensure that user access request form documentation is on file and retained for all active users.

<u>Current Status</u>: **Implemented (First Follow-Up Audit).** SSA revised access procedures to ensure all access request forms are retained. We selected a sample of ten (10) recently hired employees to verify an access request form was on file, and no exceptions were noted. Because SSA revised its access request policy and procedures to retain all access request forms, and no exceptions were found in our test sample, we consider this recommendation implemented.

4. Computer Room Not Alarmed (Control Finding)

We recommend that SSA consider installing a camera surveillance system for the room housing SSA's computing resources at 888 Main Street building.

<u>Current Status</u>: **Closed (First Follow-Up Audit).** SSA evaluated options including motion sensors and video cameras for the computer room and concluded that the additional benefit does not justify the cost given the existing layers of physical security that include Sheriff presence during business hours and key card access to the elevator and the outer door to the server room. SSA recently installed a key card reader for the server room door. Internal Audit agrees with SSA's analysis; therefore, we consider this recommendation closed.

5. Combination Door Lock Not Changed Periodically (Control Finding)

We recommend that SSA replace the computer room door/combination lock with a new door and County card reader as planned.

<u>Current Status</u>: **Implemented (First Follow-Up Audit).** SSA replaced the computer room door with a card reader. Because corrective action was taken, we consider this recommendation implemented.

OC Internal Auditor's Report



6. Password Complexity Setting is Disabled (Control Finding)

We recommend that SSA change the network password complexity setting to "enabled."

<u>Current Status</u>: **Implemented (First Follow-Up Audit).** We verified that SSA enabled password complexity in their network security settings. Because SSA enabled password complexity, we consider this recommendation implemented.

We appreciate the assistance extended to us by Social Services Agency personnel during our Follow-Up Audit. If you have any questions, please contact me directly at 834-5475 or Michael Goodwin, Senior Audit Manager at 834-6066.

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Michael B. Giancola, County Executive Officer
Mark Denny, Chief Operating Officer
Carol Wiseman, Director, SSA Administrative Services
Grady Howe, Deputy Director, SSA Information Technology Services
Hugo Ortega, Manager, SSA Information Technology Services
Foreperson, Grand Jury
Susan Novak, Clerk of the Board of Supervisors
Macias, Gini & O'Connell LLP, County External Auditor