Internal Audit Department

ORANGE COUNTY
6th Largest County in the USA

INFORMATION TECHNOLOGY AUDIT:

SOCIAL SERVICES AGENCY COMPUTER GENERAL CONTROLS

Key Control Audit

As of December 31, 2011

We audited selected computer general controls over the administration and use of the Social Service Agency's (SSA) computing resources by reviewing applicable policies and procedures, conducting interviews, and testing of selected controls. SSA administers a budget of $747 million, a staff of 3,800, and has fiduciary responsibility for approximately $2.3 billion in expenditures paid directly by the State to clients and service providers.

Based on the audit, the IT general controls were found adequate, including:

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 and environmental hazards;**
3) **Adequate systems development and change control policies and procedures have 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.**

In addition, we identified six (6) Control Findings for performing annual security assessments, and improving user access and physical access to SSA's computing resources.

AUDIT NO: 1142
REPORT DATE: FEBRUARY 19, 2013

Director: Dr. Peter Hughes, MBA, CPA, CITP
Deputy Director: Eli Littner, CPA, CIA
Senior IT Audit Manager: Autumn McKinney, CPA, CIA, CISA
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

2009 Association of Certified Fraud Examiners' Hubbard Award to Dr. Peter Hughes for the Most Outstanding Article of the Year – Ethics Pays

2008 Association of Local Government Auditors' Bronze Website Award

2005 Institute of Internal Auditors' Award for Recognition of Commitment to Professional Excellence, Quality, and Outreach

Independence • Objectivity • Integrity

ORANGE COUNTY BOARD OF SUPERVISORS' Internal Audit Department

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

Eli Littner **CPA, CIA, CFE, CFS, CISA**
Deputy Director
Certified Fraud Specialist (CFS)
Certified Information Systems Auditor (CISA)

Michael Goodwin **CPA, CIA**
Senior Audit Manager

Alan Marcum **MBA, CPA, CIA, CFE**
Senior Audit Manager

Autumn McKinney **CPA, CIA, CISA, CGFM**
Senior Audit Manager
Certified Government Financial Manager (CGFM)

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 **February 19, 2013**

TO: Dr. Michael Riley, Director
Social Services Agency

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: Information Technology Audit:
Social Services Agency
Computer General Controls

We have completed an Information Technology Audit of the Social Services Agency - Computer General Controls as of December 31, 2011. We performed this audit in accordance with our *FY 2011-12 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and the Board of Supervisors. Our final report is attached for your review.

Please note we have a structured and rigorous **Follow-Up Audit** process in response to recommendations and suggestions made by the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS). Our **first Follow-Up Audit** will begin at six months from the official release of the report. A copy of all our Follow-Up Audit reports is provided to the BOS as well as to all those individuals indicated on our standard routing distribution list.

The AOC and BOS expect that audit recommendations will typically be implemented within six months and often sooner for significant and higher risk issues. Our **second Follow-Up Audit** will begin at six months from the release of the first Follow-Up Audit report, by which time **all** audit recommendations are expected to be addressed and implemented. At the request of the AOC, we are to bring to their attention any audit recommendations we find still not implemented or mitigated after the second Follow-Up Audit. The AOC requests that such open issues appear on the agenda at their next scheduled meeting for discussion.

We have attached a **Follow-Up Audit Report Form**. Your agency should complete this template as our audit recommendations are implemented. When we perform our first Follow-Up Audit six months from the date of this report, we will need to obtain the completed document to facilitate our review.

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

As always, the Internal Audit Department is available to partner with your staff so that they can successfully implement or mitigate difficult audit recommendations. Please feel free to call me should you wish to discuss any aspect of our audit report or recommendations. Additionally, we will request your department complete a **Customer Survey** of Audit Services. You will receive the survey shortly after the distribution of our final report.

ATTACHMENTS

Other recipients of this report are listed on the **OC Internal Auditor's Report** on page 5.

Table of Contents

Information Technology Audit:
Social Services Agency
Computer General Controls
Audit No. 1142

As of December 31, 2011

OC Internal Auditor's Report

Audit No. 1142 **February 19, 2013**

TO: Dr. Michael Riley, Director
Social Services Agency

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: Information Technology Audit: Social Services Agency
Computer General Controls

Audit Highlight

SSA administers a total budget of $747 million in appropriations and $684 million in revenues, with a Net County Cost of $63.4 million. SSA also has fiduciary responsibility for approximately $2.3 billion in expenditures paid directly by the State to clients and service providers.

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 and environmental hazards; 3) adequate systems development and change control policies and procedures have 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. We identified **six (6) Control Findings** for performing annual security assessments, and improving user access and physical access to SSA's computing resources.

OBJECTIVES

In accordance with our *FY 2011-2012 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and Board of Supervisors, we conducted an Information Technology Audit of the Social Services Agency - Computer General Controls. Our audit was conducted in conformance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. The objectives of our audit were to:

1. Evaluate the adequacy of SSA's security-related personnel policies;
2. Evaluate the adequacy of user access and physical access general controls to provide reasonable assurance that computer resources are protected from unauthorized personnel and environmental hazards;
3. Evaluate the adequacy of SSA's systems development and change control policies and procedures 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. Evaluate whether an adequate segregation of duties exists within the IT organization; and
5. Evaluate the adequacy of SSA's policies and procedures for disaster recovery/business continuity to help mitigate service interruptions.

RESULTS

Objective #1: Our audit found that adequate security-related personnel policies have been developed. No findings were identified under this objective.

Objective #2: Our audit found that adequate user access and physical access general controls were present to provide reasonable assurance that computer resources are protected from unauthorized personnel and environmental hazards. In addition, we identified **six (6) Control Findings** for performing annual security assessments, and improving user access and physical access to SSA's computing resources.

Objective #3: Our audit found that adequate systems development and change control policies and procedures have been developed. No findings were identified under this objective.

Objective #4: Our audit found that adequate segregation of duties exists within the IT organization. No findings were identified under this objective.

Objective #5: Our audit found that adequate policies and procedures for disaster recovery/business continuity had been substantially developed to help mitigate service interruptions. No findings were identified under this objective.

The following table summarizes our findings and recommendations for this audit. See further discussion in the *Detailed Findings, Recommendations and Management Responses* section of this report. See *Attachment A* for a description of Report Item Classifications.

Finding No.	Finding Classification - see Attachment A	Finding	Recommendation	Concurrence by Management?	Page No. in Audit Report
1.	Control Finding	Annual system security reviews are not being performed.	SSA should ensure system security reviews are performed at least annually.	Yes	8
2.	Control Finding	User access is not being removed within 24 hours of employee separation.	SSA should implement procedures and/or additional communications to ensure supervisors are notifying SSA IT of separated users within 24 hours of their separation.	Yes	8-9
3.	Control Finding	User access request forms prior to 2006 were not retained.	SSA should revise their procedures and ensure that user access request form documentation is on file and retained for all active users.	Yes	9
4.	Control Finding	The computer room is not alarmed.	SSA should consider installing a camera surveillance system for the room housing SSA's computing resources at the 888 Main Street building.	Yes	9-10
5.	Control Finding	Locking device combination to computer room door is not changed periodically.	SSA should replace the computer room door/combination lock with a new door and County card reader as planned.	Yes	10
6.	Control Finding	Network security setting for password complexity is set to "disabled".	SSA should change the network password complexity setting to "enabled."	Yes	10-11

BACKGROUND

The Social Service Agency's vision statement is "Orange County residents will enjoy a safe and supportive environment that promotes stability and self-reliance." Their mission statement is "to deliver quality services that are accessible and responsive to the community, encourage personal responsibility, strengthen individuals, preserve families, and protect vulnerable adults and children."

The Social Services Agency (SSA) employs over 3,800 staff. SSA administers Federal, State, and County social service programs that protect children and adults from abuse or neglect; enable the frail and disabled to remain in their homes rather than being institutionalized; move eligible families from dependency to self-sufficiency; and provide benefits for eligible CalWORKS, Food Stamps, Refugee, General Relief, and Medi-Cal recipients. SSA comprises four divisions: Adult Services and Assistance Programs; Children and Family Services; Family Self-Sufficiency; and Administrative Services.

SSA administers a total budget of $747 million in appropriations and $684 million in revenues, with a Net County Cost of $63.4 million. Approximately 92% of the Agency's budget is funded through Federal and State sources. SSA also has fiduciary responsibility for approximately $2.3 billion in expenditures paid directly by the State to clients and service providers.

Information Technology Organization

SSA's Information Technology is managed by the Deputy Director, Information Technology, who reports to the Administrative Services Director. SSA Information Technology employs both internal as well as external employees. SSA Information Technology is divided into the following five (5) functions:

- Information Systems: Maintains the information system infrastructure and operations including networks and operations, database administration, internally developed systems, web applications development, and intranet/internet administration.
- Technology Systems: Acquires, deploys and maintains the agency computers and software.
- CWS/CMS Management & Reports Team: Manages the Child Welfare Services/Case Management System (CWS/CMS) application updates and develops and maintains customized reports.
- CFS IT Support Team: Provides Children and Family Services with technical support for CWS/CMS and its associated hardware and software.
- Systems Support Team: Manages CalWIN application updates and provide technical support for CalWIN users.

SSA utilizes a number of key systems including State/Consortia systems:

- CalWIN: Provides eligibility determination, benefit calculation, and case management for CalWORKs, Medi-Cal, CalFresh (Food Stamps), Foster Care, Refugee Cash Assistance, etc. Software is supported by Hewlett Packard by agreement with an 18 California county consortia. SSA provides local technical support.
- CWS/CMS (Child Welfare Services/Case Management System): Tracks and manages all child abuse referrals and case management for County provided services. Software is supported by IBM by agreement with the State including hosting of the software. SSA provides local technical support.
- AIM (Assessment, Intervention, and Management System): Provides management, tracking and printing of State mandated adult abuse reports. The system was developed and supported by SSA Information Technology.
- OCIS (Orangewood Children's Information System): Supports the admission, tracking and reporting to monitor events/activities related to children entered into the First Step Assessment Center, Orangewood Children and Family Center, Emergency Shelter Home, or Temporary Shelter Home facilities. The system was developed and supported by SSA Information Technology.

CEO/Information Technology provides the following services to SSA:

- OnBase: Document management system.
- File Server Management: Several SSA servers are housed and maintained by CEO/IT including the CalWIN pop server, report management server, and Golden workstation used for testing.

SCOPE AND METHODOLOGY

Our audit evaluated selected general controls (see definition below) and policies/procedures over the administration and use of SSA's computing resources as of December 31, 2011. Our methodology included inquiry, auditor observation, review of policies and procedures, and limited testing of selected controls over the following:

1. The adequacy of SSA's security-related personnel policies.
2. The adequacy of general user access and physical access controls over computer resources to provide reasonable assurance that computer resources are protected from unauthorized personnel and environmental hazards.
3. The adequacy of SSA's systems development and change control policies and procedures 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. The adequacy of segregation of duties within the IT organization.
5. The adequacy of general controls, primarily SSA's policies and procedures, over disaster recovery/business continuity to help mitigate service interruptions.

Definition of Computer General Controls: General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They create the environment in which application systems and controls operate. If general controls are weak, they severely diminish the reliability of controls associated with individual applications. For this reason, general controls are usually evaluated separately from and prior to evaluating application controls.

Definition of Application Controls: Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans. Application controls help make certain that transactions are valid, properly authorized, and completely and accurately processed by the computer. They are commonly categorized into three phases of a processing cycle:

- **Input:** data is authorized, converted to an automated form, and entered into the application in an accurate, complete, and timely manner;
- **Processing:** data is properly processed by the computer and files are updated correctly; and
- **Output:** files and reports generated by the application actually occur and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

Definition Source: Government Accountability Office (GAO) *Federal Information System Controls Audit Manual* (FISCAM).

SCOPE EXCLUSIONS

Our audit did not include an audit or review of the following:

- Application controls.
- Security program/plan, risk assessment, and security management structure.
- Security settings for operating system, file directory, database, and remote access (telecommunication) other than reviewing policy and procedures for their appropriate configuration.
- Access controls regarding classification of information resources according to their criticality and sensitivity, enforcing segregation of duties, and logical controls over databases, specific applications, and telecommunications access.
- System software such as utility software for back-up and recovery, production scheduling, etc.
- Controls or processes performed by other parties including CEO/IT data center physical controls, network monitoring, etc.
- Compliance with laws and regulations applicable to SSA including HIPAA and California Welfare and Institutions Code.

Management's Responsibilities for Internal Controls

In accordance with the Auditor-Controller's County Accounting Manual Section S-2 *Internal Control Systems*: "All County departments/agencies shall maintain effective internal control systems as an integral part of their management practices. This is because management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls." Control systems shall be continuously evaluated by Management and weaknesses, when detected, must be promptly corrected. The criteria for evaluating an entity's internal control structure is the Committee of Sponsoring Organizations (COSO) control framework. Our Internal Control Audit enhances and complements, but does not substitute for the Social Services Agency's continuing emphasis on control activities and self-assessment of control risks.

Inherent Limitations in Any System of Internal Control

Because of inherent limitations in any system of internal controls, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and poor judgment. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or the degree of compliance with the procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in Social Services Agency's operating procedures, accounting practices, and compliance with County policy.

Acknowledgment

We appreciate the courtesy extended to us by the Social Service Agency personnel during our audit. If we can be of further assistance, please contact me directly at 834-5475 or Mike Goodwin, Senior Audit Manager at 834-6066.

Attachments

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Robert J Franz, Interim County Executive Officer
Mike Ryan, Chief Deputy Director, SSA
Carol Wiseman, Division Director, SSA Administrative Services Division
Grady Howe, Deputy Director, SSA Information Technology Services
Steve Vandewater, Network & Operations Manager, SSA Information Technology Services
Foreperson, Grand Jury
Susan Novak, Clerk of the Board of Supervisors

Objective #1: Evaluate the adequacy of SSA's security-related personnel policies.

Work Performed
To accomplish this objective, we obtained and reviewed SSA's security-related personnel policies. Specifically, we obtained copies of personnel policies relating to hiring and separation and reviewed for appropriateness; obtained a copy of SSA's employee confidentiality statement/security agreement and reviewed for compliance with the Medi-Cal's Data Privacy and Security Agreement (Section IV. Confidentiality Statement); obtained a copy of SSA's privacy and security awareness training materials and reviewed for compliance with Medi-Cal's Data Privacy and Security Agreement (Section II. Employee Training and Discipline).

Our evaluation of the policies noted that:

- SSA's personnel policies relating to hiring and separation were appropriate and addressed: computer usage, security practices/confidentiality of data, return of property, keys, identification cards, etc. and also addressed notification to security management of separation and prompt revocation of system access.

- SSA's employee confidentiality statement/security agreement complied with Medi-Cal's Data Privacy and Security Agreement – Section IV. Confidentiality Statement.

- SSA's privacy and security awareness training materials and processes complied with Medi-Cal's Data Privacy and Security Agreement – Section II. Employee Training and Discipline.

Conclusion
Based on the work performed, adequate security-related personnel policies have been developed.

As such, we have no findings and recommendations under this audit objective.

Objective #2: Evaluate the adequacy of user access and physical access general controls to provide reasonable assurance that computer resources are protected from unauthorized personnel and environmental hazards.

Work Performed
To accomplish this objective, we audited general computer controls and processes over access to SSA's computing resources located at 888 Main Street. We selected a sample of users with access to SSA's network and determined whether an approved access request was on file. We selected a sample of recently separated employees to verify they no longer had network access. We visited the room housing SSA's computing resources located at 888 Main Street and observed selected controls for compliance with Medi-Cal's Data Privacy and Security Agreement – Section V. Physical Security. We reviewed system security settings for compliance with Medi-Cal's Data Privacy and Security Agreement – Section VI. Computer Security Safeguards and Best Practices. We discussed network system monitoring procedures with SSA. We reviewed procedures for granting/removing remote access. Additionally, we obtained and reviewed SSA's response to issues identified in a third party (Foundstone) Vulnerability Assessment conducted of SSA in October 2007.

Our evaluation of controls and processes noted that:

- Procedures for granting and removing users access to SSA's computing resources were adequate and included:
  - Only department management has the authority to add or modify access rights;
  - Authorization is in written form or communicated via email; and
  - Email authorizations or written authorizations are filed/retained.

- Controls for restricting access to SSA's computing resources located at 888 Main Street were adequate and included:
  - Computers reside in locked or otherwise restricted areas;
  - Combinations, keys, or magnetic card keys are given to authorized personnel;
  - Issuance of combinations, keys, or magnetic cards keys are documented and controlled; and
  - Workstations are logically locked when not in use.

- Physical access controls for the 888 Main Street facility complied with Medi-Cal's Data Privacy and Security Agreement – Section V. Physical Security.

- Procedures for obtaining access to the room housing SSA's computing resources were adequate.

- Network system security settings for accessing SSA's computing resources were appropriate and complied with Medi-Cal's Data Privacy and Security Agreement – Section VI. Computer Security Safeguards as follows:
  - Minimum password length;
  - Number of days before system forces system password changes;
  - Number of times password must be changed before a password may be reused;
  - Number of incorrect logon attempts before the account is locked;
  - Length of lock out period; and
  - Length of time incorrect logon count is retained.

- Based on discussions with SSA, network system monitoring procedures appeared appropriate and included:
  - Potential security violations are recorded by the system;
  - Potential security violations are reviewed on a regular basis by security administration;
  - Potential security violations are investigated and cleared; and
  - Potential security violations are the basis for adjustments to security.

- Procedures for granting/removing remote access were adequate.

- SSA's responses to findings identified in the third party (Foundstone) Vulnerability Assessment conducted of SSA in October 2007 appeared reasonable.

Conclusion

Based on the work performed, adequate user access and physical access general controls were present to provide reasonable assurance that computer resources are protected from unauthorized personnel and environmental hazards.

However, our audit disclosed several issues that impact access to SSA's computing resources. We identified **six (6) Control Findings** to improve and enhance controls and processes in addressing combination door locks, computer room alarms, annual system security reviews, access request forms, user access removal, and password complexity setting. The findings and recommendations are discussed below.

Finding No. 1 – Annual Security Reviews Not Performed (Control Finding)

Summary
The Medi-Cal Data Privacy and Security Agreement (VI. Computer Security Safeguards: Audit Trails Item P) requires all County Department systems processing and/or storing Medi-Cal PII (personally identifiable information) to have at least an annual system security review. Due to budget constraints, SSA did not perform annual system security reviews on a consistent basis.

Details
Annual system security reviews have not been performed on a consistent basis. Recent budget constraints have limited the ability of SSA to contract with third parties to perform the annual assessments. Annual system security reviews would provide assurance that the County is complying with applicable laws and regulations, as well as comply with the Medi-Cal Data Privacy and Security Agreement (VI. Computer Security Safeguards: Audit Trails Item P). According to the Medi-Cal Data Privacy and Security Agreement, if the County is unable to meet the security and privacy requirements imposed in this Agreement in the manner specified therein due to a lack of funding, DHCS (California Department of Health Care Services) will work with the County to develop a Corrective Action Plan which can be implemented within the resources provided by the State for this purpose. A Corrective Action Plan is intended to substantially meet those security and privacy requirements even if such requirements are met utilizing alternative or different methods than those specified in this Agreement.

Recommendation No. 1
We recommend that SSA ensure system security reviews are performed at least annually.

Social Services Agency Management Response
Concur. SSA will conduct annual system security reviews contingent on availability of funding.

Finding No. 2 – User Access Removal Not Within Policy Timeframes (Control Finding)

Summary
Based on our discussions with SSA Information Technology, user access is typically not removed within 24 hours of employee separation.

Details
SSA Administrative Policies and Procedures Manual – Employee Separation C7 requires that the supervisor shall notify SSA Information Technology to remove an employee's access to computer systems/network within 24 hours upon receipt of employee's separation notice. According to SSA, user access is generally not removed within 24 hours of separation because department supervisors were not forwarding the access removal requests to the appropriate staff in a timely manner. SSA Information Technology has developed a monthly HR separation report to compare with active users to help ensure access is removed for separated users. However, as this procedure is performed monthly, it does not result in compliance with the 24 hour policy requirement. Timely removal helps to prevent unnecessary user accounts from being used inappropriately. SSA should remind supervisors of the 24 hour notification requirement. Additionally, SSA Information Technology should communicate instances or statistics of untimely notifications (as identified in its monthly reviews) to SSA management for their monitoring and any necessary remediation.

Recommendation No. 2
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.

Social Services Agency Management Response

Concur. SSA is drafting a revised policy and procedure that will be vetted through the chain of command to comply with this requirement. Additionally, SSA will consistently review payroll reports as a secondary means to identify separated staff members.

Finding No. 3 – User Access Request Forms Prior to 2006 Were Not Retained (Control Finding)

Summary

User access request forms should be retained as long as the individual requires access to SSA's systems. During our testing of a sample of user access request forms, we found eight (8) out of ten (10) instances where the forms or supporting documentation were not retained and available for our review.

Details

The primary reason for the missing documentation is that user access requests made prior to 2006 were destroyed by SSA. According to SSA Information Technology, the documentation was destroyed due to limited storage space. However, the user access request forms or documentation is needed to support and substantiate user access rights. Without this, SSA and third parties are unable to verify and support that the system access granted to an individual user is appropriate. SSA should revise their procedures to ensure user access request forms are retained. This may be accomplished by forwarding the completed user access requests to SSA Human Resources for filing with the employee's personnel records or scanning the documents and storing in the OnBase document imaging system.

Recommendation No. 3

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

Social Services Agency Management Response

Concur. SSA revised procedures and now retains all user access request forms indefinitely.

Finding No. 4 – Computer Room Not Alarmed (Control Finding)

Summary

The room housing SSA's computing resources at the 888 Main Street building is not protected by an intruder alarm or security cameras. The 888 Main Street building does not have any internal security systems installed within the building.

Details

Our walkthrough of the room housing SSA's computing resources at the 888 Main Street building Found it is not protected by an intruder alarm or security cameras. The 888 Main Street building does not have any internal security systems installed within the building.

Best practices dictate that the room housing computing resources be protected by an alarm system. In addition, the Medi-Cal Data Privacy and Security Agreement (V. Physical Security Item B) requires security guards or a monitored alarm system with or without security cameras 24 hours a day, 7 days a week at County Department facilities and leased facilities where a large volume of Medi-Cal PII (personally identifiable information) is stored. A monitored alarm system would alert SSA management in the event of a break-in to the room housing SSA's computing resources.

Recommendation No. 4
We recommend that SSA consider installing a camera surveillance system for the room housing SSA's computing resources at the 888 Main Street building.

Social Services Agency Management Response
Concur. 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 including: Sheriff presence during business hours; a reception desk that monitors entry at the lobby area; and key card access to the elevators, to the outer door that leads into the area where the server room is located, and to the server room itself. The key card reader for the server room door has been installed.

Finding No. 5 – Combination Door Lock Not Changed Periodically (Control Finding)

Summary
Best practice recommends that combination locks be changed periodically to ensure only authorized personnel know the combination. The combination lock to the room housing SSA's computing resources at the 888 Main Street building is not changed on a periodic basis.

Details
The combination lock to the room housing SSA's computing resources at the 888 Main Street building is not changed on a periodic basis. The lock combination is controlled by OC Public Works, and SSA Information Technology indicated it is not practical to change it on a regular basis. Also, to access the floor where the computer resources are housed, an individual requires an access badge. However, by not changing the combination, there is the potential for unauthorized individuals to access the room housing SSA's computing resources at the 888 Main Street building.

Subsequent to our fieldwork, SSA investigated options and decided to replace the existing computer room door/combination lock with a new door and a County card reader to control access to their computer room. This will allow SSA to specifically control who has access to the computer room (through card reader authorization requests), provides logging capabilities regarding who entered the room and when, and leverages existing policies of collecting access cards (and terminating building access rights) upon separation of an employee. In addition, if required for any reason, permission to access the room can be controlled via the card reader authorization system. A work order to have OC Public Works install this new door and card reader has been initiated by SSA with an expected completion date by the end of December 2012. Based on our discussions with SSA, this approach appears reasonable.

Recommendation No. 5
We recommend that SSA replace the computer room door/combination lock with a new door and County card reader as planned.

Social Services Agency Management Response
Concur. The replacement door and card reader have been installed.

Finding No. 6 – Password Complexity Setting is Disabled (Control Finding)

Summary
Best practice recommends that complex passwords be selected by users. SSA's network security setting for password complexity is set to "disabled."

Details
The network security setting for "Password must meet complexity requirements" is set to "disabled". This setting does not require users to select complex passwords. Complex passwords are recommended as they are more secure.

Recommendation No. 6
We recommend that SSA change the network password complexity setting to "enabled."

Social Services Agency Management Response
Concur. SSA anticipates full implementation of this requirement by the end of May 2013.

Objective #3: Evaluate the adequacy of SSA's systems development and change control policies and procedures 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.

Work Performed
To accomplish this objective, we reviewed policies and procedures over system development and change control including review of project documentation for one sample change request/implementation. We reviewed written procedures for implementing new systems and modifications to systems from request to installation. We inquired whether production data is used during the testing process and whether that data is adequately secured. We reviewed emergency change management procedures. We inquired whether adequate vendor support was provided. We inquired whether packaged software documentation was adequate. We determined whether a maintenance contract was in effect for selected applications.

Our evaluation of policies and procedures noted that:

- Written procedures for implementing new systems/modifications to systems from request to installation were reasonable and addressed the following:
  - User management notifies IT of requests in writing;
  - Users are involved in the development of specifications or approve specifications;
  - Project management systems include key project information such as programmer, requesting user, scheduled completion date, and actual completion date;
  - Project priorities are established by a combination of user management and executive management (a steering committee);
  - The current status of all projects is regularly monitored by management;
  - Program testing is conducted in a "test environment" which is isolated from the production environment;
  - Users review and approve the result of programming projects initiated by them;
  - New programs or program modifications are reviewed and approved by an independent party and IT management authorizes migration to production; and
  - An appropriate independent IT party migrates programs to production from the staging area only after appropriate authorization.

- Based on discussions with SSA Information Technology, production data is generally not used during the testing process and is adequately secured when warranted.

- Based on discussions with SSA Information Technology, emergency change management procedures are appropriate.

- Based on discussions with SSA Information Technology, vendor support appears adequate and provides the following:
  - Vendor support has been defined;
  - Vendor provides product fixes and enhancements in a timely manner;
  - A full range of training is available for the software package; and
  - Procedures for requesting software enhancements are straight forward.

- Based on discussions with SSA Information Technology, packaged software documentation appears adequate and includes the following:
  - Installation documentation is provided by the vendor;
  - Software manuals explain product features and functions;
  - User procedural documentation is supplied;
  - System operations documentation is provided;
  - Documentation provided by the vendor is easy to read and easy to use; and
  - Documentation for fixes is provided by the vendor.

- Maintenance contracts were in effect for selected system software and hardware.

Conclusion
Based on the work performed, adequate system development and change control policies and procedures had been developed to help ensure only authorized programs and authorized modifications are implemented and that errors are not introduced into programs when they are developed or as a result of subsequent modifications.

As such, we have no findings and recommendations under this audit objective.

Objective #4: Evaluate whether an adequate segregation of duties exist within the IT organization.

Work Performed
To accomplish this objective, we reviewed the IT organization chart and job descriptions to determine whether there is an adequate segregation of duties.

Conclusion
Based on the work performed, an adequate segregation of duties exists within the IT organization.

As such, we have no findings and recommendations under this audit objective.

Objective #5: Evaluate the adequacy of SSA's policies and procedures for disaster recovery/business continuity to help mitigate service interruptions.

Work Performed
To accomplish this objective, we reviewed applicable policies and procedures for backup and recovery. We also determined whether SSA was participating in the CEO/IT contingency planning project and the status of their involvement. We observed controls to protect computing resources from environmental hazards at the room housing SSA's computing resources at the 888 Main Street building. We determined whether a maintenance contract was in effect for the computer hardware.

Our evaluation of controls and processes noted that:

- SSA was participating in the CEO/IT contingency planning project and is 73% complete with Phase One as of April 5, 2012.

- Written backup and recovery procedures were appropriate and addressed the following:
  - Backups (system, data, full, incremental) are taken regularly;
  - The recovery process and back-up tapes were recently write tested as part of the Solano County recovery solution to ensure that they can be utilized if required;
  - The backup scheme allows the system to be restored to within 24 hours of the incident;
  - On-site backup tapes are stored in secured, locked and fireproof facilities;
  - Off-site backup tapes are stored in secured, locked and fireproof facilities;
  - Backup tapes are rotated between on-site and off-site storage facilities; and
  - Recovery procedures are documented.

- Controls to protect computing resources from environmental hazards at the room housing SSA's computing resources at the 888 Main Street building were adequate and included:
  - Smoke, heat, and water detection devices are installed to provide early warning;
  - Automated fire extinguishing systems are installed;
  - Hand held fire extinguishers are located in strategic locations near the computer;
  - Raised flooring;
  - Computers are secured either in rack mounts or bolted to the floor;
  - Uninterrupted power supply (UPS) units are installed for all significant system components;
  - Emergency lighting has been installed; and
  - Protection systems (fire extinguishers, etc.) are maintained regularly.

- Maintenance contracts were in effect for the computer hardware.

Conclusion
Based on the work performed, adequate policies and procedures for disaster recovery/business continuity have been substantially developed to help mitigate service interruptions.

As such, we have no findings and recommendations under this audit objective.

ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit observations and recommendations, we will classify audit report items into three distinct categories:

- **Critical Control Weaknesses:**
  Audit findings or a combination of Significant Control Weaknesses that represent serious exceptions to the audit objective(s), policy and/or business goals. Management is expected to address Critical Control Weaknesses brought to their attention immediately.

- **Significant Control Weaknesses:**
  Audit findings or a combination of Control Findings that represent a significant deficiency in the design or operation of internal controls. Significant Control Weaknesses require prompt corrective actions.

- **Control Findings:**
  Audit findings concerning internal controls, compliance issues, or efficiency/effectiveness issues that require management's corrective action to implement or enhance processes and internal controls. Control Findings are expected to be addressed within our follow-up process of six months, but no later than twelve months.

ATTACHMENT B: Social Services Agency Management Responses

County of Orange
SOCIAL SERVICES AGENCY
888 N. MAIN STREET
SANTA ANA, CA 92701-3518
(714) 541-7700

MICHAEL L. RILEY, Ph.D.
DIRECTOR

MIKE RYAN
CHIEF DEPUTY DIRECTOR

CAROL WISEMAN
DIVISION DIRECTOR
ADMINISTRATIVE SERVICES

WENDY AQUIN
DIVISION DIRECTOR
ADULT SERVICES &
ASSISTANCE PROGRAMS

GARY TAYLOR
DIVISION DIRECTOR
CHILDREN & FAMILY SERVICES

NATHAN NISHIMOTO
DIVISION DIRECTOR
FAMILY SELF-SUFFICIENCY

RECEIVED
2013 JAN 31 PM 2:00
INTERNAL AUDIT DEPARTMENT

January 29, 2013

Dr. Peter Hughes, CPA, Director
Internal Audit Department
12 Civic Center Plaza, Room 232
Santa Ana, CA 92701

Subject: Response to Information Technology Audit No. 1142 of Social Services Agency Computer General Controls

On December 4, 2012, the Director of Social Services Agency (SSA) received the draft Information Technology Audit No. 1142 of Social Services Agency Computer General Controls as of December 31, 2011. We appreciate the acknowledgement that the audit found that: adequate security-related personnel policies have been developed; adequate user access and physical access general controls were present to provide reasonable assurance that computer resources are protected from unauthorized personnel and environmental hazards; adequate systems development and change control policies and procedures have been developed; adequate segregation of duties exists within the IT organization; and adequate policies and procedures for disaster recovery/business continuity have been substantially developed to help mitigate service interruptions.

The following provides our management responses to the audit report recommendations;

Finding No. 1 – Annual System Security Reviews Not Performed (Control Finding)

Recommendation No. 1
We recommend that SSA ensure system security reviews are performed at least annually.

Social Services Agency Management Response:
SSA will conduct annual system security reviews contingent on availability of funding.

Finding No. 2 – User Access Removal Not Within Policy Timeframes (Control Finding)

Recommendation No. 2
We recommend that SSA implement procedures and/or additional communications to ensure supervisors are notifying SSA Information Technology of separated users within 24

ATTACHMENT B: Social Services Agency Management Responses (continued)

hours of their separation.

Social Services Agency Management Response:
SSA is drafting a revised policy and procedure that will be vetted through the chain of command to comply with this requirement. Additionally, SSA will consistently review payroll reports as a secondary means to identify separated staff members.

Finding No. 3 – User Access Request Forms Prior to 2006 Were Not Retained (Control Finding)

Recommendation No. 3
We recommend that SSA revise their procedures and ensure that user access request forms documentation is on file and retained for all active users.

Social Services Agency Management Response:
SSA revised procedures and now retains all user access request forms indefinitely.

Finding No. 4 – Computer Room Not Alarmed (Control Finding)

Recommendation No. 4
We recommend that SSA consider installing a camera surveillance system for the room housing SSA's computing resources at the 888 Main Street Building.

Social Services Agency Management Response:
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 including: Sheriff presence during business hours; a reception desk that monitors entry at the lobby area; and key card access to the elevators, to the outer door that leads into the area where the server room is located, and to the server room itself. The key card reader for the server room door has been installed.

Finding No. 5 – Combination Door Lock Not Changed Periodically (Control Finding)

Recommendation No. 5
We recommend SSA replace the computer room door/combination lock with a new door and County card reader as planned.

Social Services Agency Management Response:
The replacement door and card reader have been installed.

Finding No. 6 – Password Setting Complexity Setting is Disabled (Control Finding)

Recommendation No. 6
We recommend that SSA change the network password complexity setting to "enabled".

Social Services Agency Management Response:
SSA anticipates full implementation of this requirement by the end of May 2013.

ATTACHMENT B: Social Services Agency Management Responses (continued)

If you have any questions concerning this response, please call me at (714)541-7773 or Carol Wiseman, Administrative Services Division Director at (714)541-7776.

Sincerely,

Michael L. Riley, Ph.D.
Director
Social Services Agency

cc: Bob Franz, Interim CEO
Mike Ryan, Chief Deputy Director, SSA
Carol Wiseman, Director, Administrative Services Division
Grady Howe, Deputy Director, SSA Information Technology Services