

**SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**



FROM: County Auditor-Controller

SUBMITTAL DATE:
September 29, 2008

SUBJECT: Internal Audit Report 2008-004.1: Department of Public Social Services - Disposal of Computers and Related Equipment

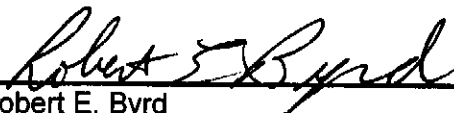
RECOMMENDED MOTION: Receive and file Internal Audit Report 2008-004.1: Department of Public Social Services - Disposal of Computers and Related Equipment.

BACKGROUND: The Auditor-Controller completed an audit of the County of Riverside Department of Public Social Services (DPSS) for disposal of computers and related equipment. Our primary objective was to assess the adequacy of internal controls over the disposal of computers and related equipment, including the removal of confidential county information.

The audit found adequate internal controls were maintained over the disposal process of computers and laptops as well as the removal of confidential county information. Internal controls over mobile devices were generally adequate; however, we identified areas where controls could be improved such as the encryption of mobile devices and compliance with Department Policy 23-004 regarding the identification and tracking of assets.

Management concurred with all audit findings and recommendations and provided a corrective action plan. We will follow-up within one year to verify that DPSS management took the planned corrective action.

Departmental Concurrence



 Robert E. Byrd
 County Auditor-Controller

FINANCIAL DATA	Current F.Y. Total Cost:	\$ 0	In Current Year Budget:	N/A
	Current F.Y. Net County Cost:	\$ 0	Budget Adjustment:	N/A
	Annual Net County Cost:	\$ 0	For Fiscal Year:	N/A

SOURCE OF FUNDS: N/A	Positions To Be Deleted Per A-30	<input type="checkbox"/>
	Requires 4/5 Vote	<input type="checkbox"/>

C.E.O. RECOMMENDATION:

County Executive Office Signature

Dep't Recomm.: Consent Policy
 Per Exec. Ofc.: Consent Policy

Prev Ann Ref:

District:

Agenda Number:



County of Riverside

INTERNAL AUDIT REPORT

Department of Public Social Services Disposal of Computers and Related Equipment

September 29, 2008

Office of
Robert E. Byrd, CGFM
County Auditor-Controller

4080 Lemon Street
P.O. Box 1326
Riverside, CA 92502-1326



**OFFICE OF THE
COUNTY 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



**COUNTY OF RIVERSIDE
AUDITOR-CONTROLLER**
Robert E. Byrd, CGFM
AUDITOR-CONTROLLER

Bruce Kincaid, MBA
ASSISTANT
AUDITOR-CONTROLLER

September 29, 2008

Ms. Susan Loew
Director
Department of Public Social Services
4060 County Circle Drive
Riverside, CA 92503

Subject: Internal Audit Report 2008-004.1: Department of Public Social Services - Disposal of Computers and Related Equipment

Dear Ms. Loew:

We have completed an audit of computers and related equipment disposal procedures for the Department of Public Social Services as one of three departments selected for detailed testing as part of a countywide audit. We conducted the audit during the period August 8, 2007 through March 7, 2008, for operations of July 1, 2005 thru March 7, 2008.

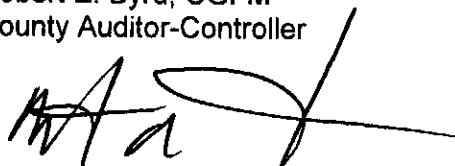
Our primary objective was to provide an independent assessment about the adequacy of internal controls over the disposal of computers and related equipment, including the removal of stored confidential county information.

We conducted our audit in accordance with the auditing standards established by the Institute of Internal Auditors. These standards require that we plan and perform the audit to provide sufficient, competent, and relevant evidence to achieve the audit objectives. We believe the audit provides a reasonable basis for our conclusions.

Adequate internal controls were maintained over the disposal process of computers and laptops as well as the removal of confidential county information. Internal controls over mobile devices were generally adequate; however, we identified areas where controls could be improved such as the encryption of mobile devices and compliance with Department Policy 23-004 regarding the identification and tracking of assets. Throughout the audit, we discussed the results contained in this report with the appropriate levels of management.

We thank the Department of Public Social Services management and staff for their cooperation; their assistance contributed significantly to the successful completion of the audit.

Robert E. Byrd, CGFM
County Auditor-Controller

A handwritten signature in black ink, appearing to read 'MGA', with a long horizontal stroke extending to the right.

By: Michael G. Alexander, MBA, CIA
Deputy Auditor - Controller

cc: Board of Supervisors
County Counsel
Executive Office
Grand Jury

Table of Contents

	Page
Executive Summary	1
Objectives and Methodology	3
Results	
Computer Disposal	4
Mobile Devices	6
Management Response	Appendix

Executive Summary

Overview

Proper removal of information from computers and laptops prior to disposal is vital in order to protect the County of Riverside from inadvertently disclosing sensitive information. All desktop and laptop computers have the potential to contain confidential or sensitive information. Many computer users believe if they delete files or empty their recycle bin this removes all traces of information stored on the hard drives. This is an incorrect assessment. Forensic Tools may be utilized to retrieve information previously stored on hard drives if the information is not properly removed. It is therefore imperative for each department to implement a reliable and secure process for erasing information stored on computer devices, including Black Berry and other PDA devices, cell phones, and USB drives prior to their disposal. Additionally, the County of Riverside has an obligation to ensure proper use and safeguarding of information stored on mobile devices such as laptops, Black Berry and other PDA devices, cell phones, and USB drives. This can be accomplished through the use of encrypted devices. This is beneficial in cases when a device that is lost or stolen may contain sensitive or confidential information since an encrypted device may be accessed only with the use of a secret decryption key.

We selected three county departments to participate in this audit based upon the confidential nature of information handled by the departments. Confidential information includes names, Social Security numbers, addresses, telephone numbers, financial information, or other personal information that are identifiable to an individual. DPSS was one of the departments selected since it obtains confidential information in order to provide public assistance including Medi-Cal, food stamps, financial assistance, foster care, and many other services. The type of information handled by this department is sensitive in nature and should only be accessible to authorized employees. We conducted detailed testing of the department's electronic information disposal process to determine whether the process ensures that confidential information is securely removed from computer and electronic devices.

Overall Objective

Our overall audit objective was to determine whether the existing internal controls adequately provide the assurance that confidential information stored on computer devices is securely erased prior to their disposal.

Overall Conclusion

Adequate internal controls were maintained over the disposal process of computers and laptops as well as the removal of confidential county information. Internal controls over mobile devices were generally adequate; however, we identified areas where controls could be improved such as the encryption of mobile devices and compliance with Department Policy 23-004 regarding the identification and tracking of

assets. Throughout the audit, we discussed the results contained in this report with the appropriate levels of management.

Details about our audit methodology, results, findings and recommendations are provided in the body of our report.

Objectives

Our detailed audit objectives were:

- to determine the existence and adequacy of internal controls relating to the disposal of computers and related electronic devices; and
- to evaluate the existence and adequacy of internal controls over the removal of confidential information from computers and mobile devices.

Methodology

To accomplish our objectives, we:

- identified and reviewed applicable policies and procedures, Board ordinances, laws, codes and regulations;
- conducted interviews and performed walk-throughs with key DPSS personnel to gain an understanding of computer disposal procedures and in particular the removal of county information and controls over mobile devices;
- documented the department's disposal process;
- identified and reviewed the department's policy for the disposal of computers and mobile devices;
- identified and reviewed the department's compliance with Board of Supervisors' Policy A-58, Enterprise Information Systems Security Policy Section 3.2 and 3.3;
- identified and reviewed the department's process for training staff on the use of mobile devices;
- performed detailed testing of computers to verify confidential county information has been removed prior to being sent to county surplus;
- performed detailed testing to determine if the department is in compliance with Riverside County's Information Security Office Policy S05.01, dated March 1, 2007;
- performed detailed evaluations of the departments documentation for computers, laptops, and mobile devices that were wiped clean; and,
- performed detailed testing to verify employees returned mobile devices.

Results

Computers

Department of Public Social Services uses Remedy 4.0 (Asset Tracking System) to record and track assets that are purchased, transferred, and disposed. The department utilizes Darik's Boot and Nuke (DBAN) software to erase information on computers and laptops. This software renders data on magnetic devices such as hard drives unrecoverable. Upon installation, DBAN will automatically and completely delete the contents of any hard drive that it can detect, making it an appropriate utility for bulk or emergency data destruction. This software is recommended as part of the County's Technology Standards approved by the Board of Supervisors. DBAN software was selected by the department to ensure confidential information is not inadvertently disclosed to the end recipient of discarded computer equipment.

We randomly selected three computers sent by the Department of Public Social Services to county surplus for disposal to verify hard drives were erased and all confidential information was removed. As part of our review, we utilized recovery software to retrieve information originally contained on the hard drives. None of the computers reviewed had an operating system and we did not recover any information. Additionally, we coordinated a forensic evaluation with Riverside County Information Security Office for two other randomly selected computers that were sent by the Department of Public Social Services to county surplus for disposal. The forensic evaluation detected no useable information on the hard drives.

Finding 1

Remedy 4.0 (Asset Tracking System) does not retain the name of the individual who erases the hard drive of computers, or mobile devices. When these items are transferred to the warehouse the name of the individual who erased the computers or mobile devices is replaced with the name of the storekeeper. This occurred because the department did not configure the system to provide a complete history on these transactions. As a result, management cannot determine accountability should confidential county information be compromised.

Recommendation 1

Implement a control in the new version of Remedy (version 7.0) to ensure the name of the individual who erased the hard drive on computers, laptops, or mobile devices does not change when the asset is transferred to warehousing.

Management's Reply

Concur. DPSS Information Technology will implement the following actions:

- Establish additional data fields during the configuration of the Remedy v7.0 product to capture and retain the person's name that erases data from storage devices on computers, laptops, and mobile devices and the date it was erased before they are returned to warehousing.
- Update our process documents to include instructions regarding when and how data is to be erased and who has the responsibility for doing it.

Estimated Date of Corrective Action: 12/1/2008

Results

Mobile Devices

The Department of Public Social Services assigns mobile devices such as, laptops, PDAs, USB drives and cell phones based upon the IT Equipment Approval Matrix, which determines the type and approval needed to assign mobile devices to employees. Utilizing this matrix ensures the Department of Public Social Services is in compliance with the Information Security Office Policy S05.01, Sensitive Data Protection Policy, in particular Mobile Devices or Portable Media.

The department acquired 200 Kingston Technology 512 MB USB 2.0 Data Traveler drives within the last two fiscal years, which were utilized for business purposes. The department is now planning on purchasing USB drives that are encrypted to protect and ensure the department's confidential information is not inadvertently disclosed. Our audit primarily reviewed the procedures for tracking these mobile devices and was accomplished through interviews, physical observation, and the testing of controls. Based upon the results of our inquiries and observations, we determined the department generally had adequate controls over mobile devices; however, we identified areas for improvement as indicated.

Finding 2

The department did not track USB drives using Remedy 4.0 nor are they labeled with asset tags. The department did not maintain an adequate and updated list of USB drives assigned to employees. As a result, the department had no assurance that these items, which could contain confidential information were returned by employees upon termination.

Department of Public Social Services Policy No. 23-004, Section 1, Asset Tracking requires the tracking of fixed and critical assets from the point of purchase through the point of disposal. The USB drives acquired by the department were not tagged nor tracked using Remedy 4.0. The list of USB drives assigned to employees was maintained by Child Protective Services, a division within the Department of Public Social Services, not the department's IT staff.

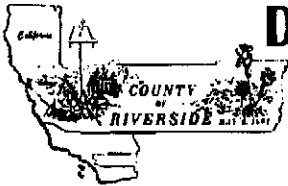
Recommendation 2

Ensure adequate procedures are in place to purchase encrypted USB drives, affix asset tags to all USB drives, and track them using the Asset Tracking System.

Management's Reply Concur. DPSS Information Technology will implement the following actions:

- Update approved hardware list to include only USB drives which are encrypted.
- Issue a Departmental Memorandum requiring all USB drives to be returned to IT for replacement with encrypted USB drives.
- Deploy software to every desktop and laptop computer to restrict use of any USB drive which is not issued by DPSS. Only encrypted USB drives will be allowed.
- Affix DPSS Asset Tags to all USB drives purchased and track them in the Asset Tracking System.

Estimated Date of Corrective Action: 9/30/2008



Department of Public Social Services

Administrative Office: 4060 County Circle Drive, Riverside, CA, 92503
(951) 358-3000 FAX: (951) 358-3036

Susan Loew, Director

June 3, 2008

Mr. Robert E. Byrd, CGFM
Riverside County Auditor-Controller
P.O. Box 1325
Riverside, CA 92502-1326

08 JUN - 9 PM 4: 00
RIVERSIDE COUNTY
AUDITOR-CONTROLLER

Subject: Response to Draft Internal Auditor's Report # 2008-004 –Countywide Disposal of Computers and Related Equipment Audit, Department of Public Social Services

Dear Mr. Byrd,

In response to the above referenced audit, DPSS has addressed the recommendations, and as always, is committed to maintaining the highest standards of transparency and accountability in all aspects of our work.

Please find detailed responses to your specific recommendations in the pages that follow.

If you require further details or have questions, please contact myself or Patricia Reynolds, Assistant Director.

Sincerely,

Susan Loew
Director

Attachment

★ ★ ★ ★ ★

INNOVATIONS IN AMERICAN GOVERNMENT AWARD WINNER - 1996

DATE: May 27, 2008
TO: Auditor-Controller
Audits and Specialized Accounting Division
FROM: Susan Loew, Director
Riverside County Department of Public Social Services
SUBJECT: Reply to Draft Audit Report

Recommendation Number 1:

Implement a control in the new version of Remedy 7.0 (Asset Tracking System) to ensure the name of the individual who erased the hard drive on computers, laptops, or mobile devices does not change when the asset is transferred to warehousing.

Management position concerning the recommendation:

 X Concur Disagree

Comments: None

Corrective Action: DPSS Information Technology will implement the following actions:

- Establish additional data fields during the configuration of the Remedy v7.0 product to capture and retain the person's name that erases data from storage devices on computers, laptops, and mobile devices and the date it was erased before they are returned to warehousing.
- Update our process documents to include instructions regarding when and how data is to be erased and who has the responsibility for doing it.

Actual/estimated Date of Corrective Action: 12/1/2008

These two corrective actions will be tied to the implementation date for Remedy v7.0 as estimated above.

Estimated cost to implement recommendation (if material)

\$ N/A

DATE: May 27, 2008
TO: Auditor-Controller
Audits and Specialized Accounting Division
FROM: Susan Loew, Director
Riverside County Department of Public Social Services
SUBJECT: Reply to Draft Audit Report

Recommendation Number 2.1:

Ensure adequate procedures are in place to purchase encrypted USB drives, affix asset tags to all USB drives, and track them using the Asset Tracking System.

Management position concerning the recommendation:

Concur Disagree

Comments: None

Corrective Action: DPSS Information Technology will implement the following actions:

- Update approved hardware list to include only USB drives which are encrypted.
- Issue a Departmental Memorandum requiring all USB drives to be returned to IT for replacement with encrypted USB drives.
- Deploy software to every desktop and laptop computer to restrict use of any USB drive which is not issued by DPSS. Only encrypted USB drives will be allowed.
- Affix DPSS Asset Tags to all USB drives purchased and track them in the Asset Tracking System.

Actual/estimated Date of Corrective Action: 9/30/2008

Estimated cost to implement recommendation (if material)

\$ N/A