BOARD OF COUNTY COMMISSIONERS
OFFICE OF THE COMMISSION AUDITOR

M E M O R A N D U M

TO: Honorable Chairman Jean Monestime
and Members, Board of County Commissioners

FROM: Charles Anderson, CPA
Commission Auditor

DATE: May 08, 2015

SUBJECT: **Follow-up Report**: Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information − *Former Department of Human Services*

We issued the final report of the Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information − Former Department of Human Services *(now part of Community Action and Human Services Department (CAHSD))* on October 11, 2012. We submit this follow-up report, which contains the implementation status of our recommendations in the original report.

The Office of the Commission Auditor (OCA) requests that within 90 days, the Director of CAHSD, in conjunction with the Information Technology Department (ITD), report subsequent actions taken to implement the recommendations on audit findings that are currently pending.

We thank the staff of CAHSD and ITD for their cooperation and input throughout the follow-up audit. Please let me know if you need further information.

c: Mayor Carlos Gimenez, County Mayor
Russell Benford, Deputy Mayor, Office of the Mayor
Lucia Davis-Raiford, Executive Director, CAHSD
R. A. Cuevas, Jr., County Attorney
Mary T. Cagle, Inspector General
Cathy Jackson, Director, Audit and Management Services
Angel Petisco, Director, Information Technology Department
Alberto Parjus, Assistant Director, CAHSD
Lars Schmekel, Chief Security Officer, Information Technology Department
Marie Woodson, Division Director, CAHSD
Neil R. Singh, Audit Manager, OCA

THIS PAGE INTENTIONALLY BLANK

MIAMI-DADE COUNTY BOARD OF COUNTY COMMISSIONERS

OFFICE OF THE COMMISSION AUDITOR

AUDIT OF INTERNAL CONTROLS FOR THE PROTECTION OF ELECTRONICALLY STORED PERSONAL AND HEALTH INFORMATION-

Former Department of Human Services

(Now part of CAHSD)

FOLLOW-UP

Project Number 11-143370

May 08, 2015

Charles Anderson, CPA
Commission Auditor

Auditors

Michael O. Bayere, CIA, CISA, CISSP — Auditor-In-Charge
Neil R. Singh, CPA — Audit Manager

111 NW First Street, Suite 1030
Miami, Florida 33128
305-375-4354

THIS PAGE INTENTIONALLY BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY BLANK

I. OBJECTIVE AND SCOPE

The policies and procedures of the Office of the Commission Auditor (OCA) require that we perform follow-up activities within one year from the time of a final audit to report on the implementation status of audit recommendations. The objective of this follow-up audit was to assess the actions taken by management of the Community Action and Human Services Department (CAHSD), and the Information Technology Department (ITD) (where applicable) to remediate, based on our recommendations, the findings in OCA's final audit report. The scope of the follow-up activities was from July 2013 through August 2014.

II. BACKGROUND

In 2012, as part of the Work Plan approved by the Board of County Commissioners (BCC), the OCA conducted the Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information at the former Department of Human Services (DHS). DHS is now part of CAHSD. The final audit report was released on October 11, 2012. The objectives of the audit were to assess the adequacy and operational effectiveness of physical, administrative and technical controls designed for protecting the confidentiality and integrity of personally identifiable and health information of DHS's clients (program participants/applicants).

The following is the summary of findings in the final audit report:

1. Department was using Wireless Local Area Network (WLAN) implemented with poor security features that could easily compromise confidential and sensitive information.
2. Communication link between external users and the County internal network for one important application (computer program) used in the Child Development Bureau was not protected with appropriate security mechanisms.
3. Policies for managing computer users' passwords on department/County computing resources were weak.
4. Access rights of some former and transferred employees were not removed from the Social Services Information System (SSIS) and the Enhanced Field System (EFS) for months/years after the employees had been separated or transferred.
5. Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems.
6. There was no policy for secure use of removable storage media, and no documentation to provide evidence of secure sanitization or destruction of old electronic storage media.
7. Policy for secure custody of clients' files/records was violated in two of the DHS sites we visited.
8. Department did not have policy or guidelines to ensure that user-developed databases and spreadsheets containing clients confidential information were secured with appropriate security mechanisms.

OCA's recommendations on the above and the status of implementation by CAHSD and ITD are summarized in the Summary Results below. More details, including management's original actions plan in the final audit report are provided in the Details of Findings Remediation Status (Attachment 1).

III. SUMMARY RESULTS

Our follow-up audit revealed that CAHSD and ITD have made substantial progress in remediating the audit findings. Five of the findings above have been fully resolved, and three have been partially resolved. The five findings that are fully resolved are henceforth closed. Below is the summary of the remediation status of the audit findings:

Finding 1: Department uses WLAN implemented with poor security features that can easily compromise confidential and sensitive information.

Recommendations:

a) ITD should upgrade WLAN to one based on security standards with robust security features (e.g. Wi-Fi Protected Access II (WPA2)).
b) ITD should establish effective risk assessment and control processes to continuously manage the risks of wireless network.

Remediation status: Not fully resolved.

Finding 2: Communication link between external users and the County internal network for one important application (computer program) used in the Child Development Bureau was not protected with appropriate security mechanisms.

Recommendations: CAHSD to work with ITD to enhance the security of the application by employing cryptographic mechanism to protect the communication path between external users and the application server**.**

Remediation Status: Fully resolved.

Finding 3: Policies for managing computer users' passwords on department/County computing resources are weak.

Recommendations:

a) ITD should enforce password maximum lifetime policy for users' domain accounts.
b) CAHSD should request enhancement to the password policy in the EFS that will require users to use strong passwords and also change them periodically.

Remediation Status: Fully resolved.

Finding 4: Access rights of some former and transferred employees were not removed from the SSIS and the EFS for months/years after the employees had been separated or transferred.

Recommendations:

a) CAHSD should delete system accounts of former and transferred employees stated above in EFS; revoke and subsequently delete accounts in EFS whose owners were unidentified.
b) CAHSD should implement written and well-supervised procedures for granting, modifying, monitoring, documenting, and promptly terminating user access on all systems used by the department.

Remediation Status: Fully resolved.

Finding 5: Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems.

Recommendations:

a) ITD should review flaw remediation and system configuration management processes, implement needed enhancements that will assure effective remediation of systems flaws.
b) ITD should develop system configuration standard that ensures all systems security settings conform to best practices that mitigate possible risks.

Remediation Status: Not fully resolved.

Finding 6: There was no policy for secure use of removable storage media, and no documentations to provide evidence of secure sanitization or destruction of old electronic storage media.

Recommendation:

CAHSD and the Internal Service Department (ISD), in conjunction with ITD, should establish a written policy and also guidelines for secure use, sanitization, reuse and destruction of storage media (hard disk and removable media), and documentation requirements to evidence sanitization and destruction actions.

Remediation Status: Not fully resolved.

Finding 7: Policy for secure custody of clients' files/records was violated in two of the DHS sites we visited.

Recommendation:

CAHSD personnel must ensure full compliance with the department's policy on secure custody of client files and records. Records slated for shredding should be given equivalent protection until they are shredded.

Remediation Status: Fully resolved.

Finding 8: Department did not have a policy or guidelines to ensure that user-developed databases and spreadsheets containing clients confidential information are secured with appropriate security mechanisms.

Recommendations:

a) CAHSD, in consultation with ITD, should implement adequate security mechanisms (including encryption) to protect all existing user-developed databases that contain confidential information in the department.

b) CAHSD, in consultation with ITD, should develop a written policy and also guidelines that will ensure all in-house and user-developed applications and databases are secured with appropriate security mechanisms before they are put to use.

Remediation Status: Fully resolved.

IV. CONCLUSION

OCA acknowledges the actions taken by CAHSD and ITD to remediate some of the issues in the audit findings. However, the outstanding issues (as detailed in the attached schedule) need to be resolved as a matter of necessity, without further delay, in order to reasonably protect the confidentiality and integrity of personal and health information of citizens and residents that participate in CAHSD programs.

ATTACHMENT I

Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information:
Former Department of Human Services (DHS)
Details of Findings Remediation Status

Finding 1	Department uses Wireless Local Area Network (WLAN) implemented with poor security features that can easily compromise confidential and sensitive information.	
	OCA Recommendations	a) Information Technology Department (ITD) should upgrade WLAN to one based on security standards with robust security features (e.g. Wi-Fi Protected Access II (WPA2)). b) Effective risk assessment and control processes should be established by ITD to continuously manage the risks of wireless network.
	Management Remediation Plan	Effective risk assessment and control processes will be established by ITD to continuously manage the risks of the County's wireless network. This will be completed within 90 days after the wireless security implementation plan is approved. The new equipment being proposed for deployment (and associated port charges) is part of the Edge Network Infrastructure project which will update network infrastructure throughout the County. This project was intended to modernize the County's network as well as improve wired and wireless security to meet current standards and best practices. This new infrastructure for both wired and wireless connectivity will be managed centrally by ITD and the risk management process will be integrated as part of the overall management of the network. Although CAHSD was not included in the 2012/13 deployment plan, the department and associated sites will be expedited and should be completed by March 2013.
	Follow up Results	a) WLAN upgrade was partially implemented. Department was still using the legacy (Wired Equivalent Privacy (WEP) based) technology alongside the newly implemented WPA2 technology. b) Process for maintaining wireless Access Points (APs) needs improvement to better mitigate and manage inherent risks of WLAN: • Vulnerabilities in the configurations of wireless APs identified by a vulnerability assessment tool during a quarterly vulnerability assessment scan of APs by ITD were not corrected. Nine critical vulnerabilities identified in multiple APs in a December 15, 2013 scan remained uncorrected as of March 15, 2014. • There was no complete inventory of the insecure WEP based APs that were authorized for use in the County WLAN. Those WEP based APs now need to be decommissioned from the network. • Monitoring process to track and prevent rogue APs from connecting to the County WLAN was not implemented. **<u>Comments</u>** 1) The continued use of WEP based technology for the County WLAN could expose the confidential and sensitive information communicated on the network to possible compromise. 2) Uncorrected vulnerabilities in the configurations of APs could allow hackers to easily compromise

		the WLAN and cause avoidable damage. 3) Lack of complete inventory of all APs installed and operating in the County's network could hinder proper accountability for legitimate APs, and impair possible measures to prevent illegitimate ones. 4) Inadequate monitoring of WLAN activities to track and prevent rogue APs from connecting to the County WLAN could allow malicious individuals to install rogue APs in the network to compromise confidential and sensitive information. **<u>Further Recommendations</u>** 1) ITD should complete the upgrade of the legacy (WEP based) WLAN technology to a more secured WPA2 based technology. 2) ITD should document a complete inventory of all authorized APs installed and operating in the County's WLAN. 3) ITD should ensure that appropriate technical and administrative solutions are implemented to monitor WLAN traffic, and manage all wireless APs and their configurations, in order to mitigate possible risks of rogue APs and the exploitation of vulnerabilities in legitimate APs.
	Conclusion on Remediation Status	Issues not fully resolved: **Finding is open**
Finding 2	Communication link between external users and the County internal network for one important application (computer program) used in the Child Development Bureau was not protected with appropriate security mechanisms.	
	OCA Recommendation	CAHSD to work with ITD to enhance the security of the application by employing cryptographic mechanism to protect the communication path between external users and the application server.
	Management Remediation Plan	The application was modified by ITD in September, 2012 to ensure end to end industry standard encryption between external users and the County system to prevent unauthorized access/eavesdropping by anyone except the authorized user when the application is accessed.
	Follow up Results	The administration of the Child Development Services program for which the software was being used has been transferred to the Early Learning Coalition (ELC). The transfer of the application server to ELC by the County on June 27, 2013 was appropriately documented in the County's Equipment Transfer Form.
	Conclusion on Remediation Status	Issues resolved: **Finding is closed**

ATTACHMENT I

Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information:
Former Department of Human Services (DHS*)*
Details of Findings Remediation Status

Finding 3	Policies for managing computer users' passwords on department/County computing resources are weak.	
	OCA Recommendations	a) ITD should enforce password maximum lifetime policy for users' domain accounts. b) CAHSD should request enhancement to the password policy in the Enhanced Field System (EFS) that will require users to use strong passwords and also change them periodically.
	Management Remediation Plan	a) Domain password policies have been developed which are aligned with information security best practices. These requirements were enabled for all CAHSD accounts in a phased implementation to minimize user impact and business interruption. This implementation was completed on September 27, 2012. b) EFS database is being replaced by Early Learning Information System (ELIS) throughout the State of Florida. The roll out in Dade County is scheduled for July 2013. The EFS administrator is being trained in the new database which is a more robust and secure application that provides password policy configuration and more secure features
	Follow up Results	a) Password policies have been enhanced to provide reasonable protection for user accounts. b) Department no longer uses EFS, since the Child Development Services program for which it was being used had been transferred to the Early Learning Coalition.
	Conclusion on Remediation Status	Issues resolved: **Finding is closed**
Finding 4	Access rights of some former and transferred employees were not removed from the Social Services Information System (SSIS) and the EFS for months/years after the employees had been separated or transferred.	
	OCA Recommendations	a) CAHSD should delete system accounts of former and transferred employees stated above in EFS; revoke and subsequently delete accounts in EFS whose owners were unidentified. b) CAHSD should implement written and well-supervised procedures for granting, modifying, monitoring, documenting, and promptly terminating user access on all systems used by the department.
	Management Remediation Plan	a) For auditing and historical purposes user accounts cannot be deleted from the EFS system. However, to disable use, accounts are placed inactive and passwords are changed. b) CAHSD will expand the implementation of the developed CAHSD Policy and Procedure (P&P), "New Accounts, Transfers and Terminations" which establishes that each user is granted a unique identifier for access through a supervisor approved Central Registration System (CRS) form where only the needed operational account privilege is requested and granted. In addition, CAHSD's Human Resources division is in constant contact with CAHSD's Information Technology Unit to disable any accounts and/or passwords for employees who retired, transferred or terminated from the County.

	Follow up Results	a) EFS is no longer being used by the department, since the Child Development Services program for which it was being used had been transferred to the Early Learning Coalition. b) The policies and procedures for computer user access management are documented, are reasonably adequate and were complied with during the period reviewed.
	Conclusion on Remediation Status	Issues resolved: **Finding is closed**
Finding 5	Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems.	
	OCA Recommendations	a) ITD should review flaw remediation and system configuration management processes, implement needed enhancements that will assure effective remediation of systems flaws. b) ITD should develop system configuration standard that ensures all systems security settings conform to best practices that mitigate possible risks.
	Management Remediation Plan	a) ITD employs an automated flaw remediation system to correct known system vulnerabilities. The system was recently upgraded improving automated processes for fixing flaws. The system has also been enhanced to detect and correct additional flaws that were not being addressed by the previous version. It is anticipated that the number of software defects will be significantly reduced. Integrated with the automated fix process, ITD will provide CAHSD regular reports on systems that are non-compliant for follow-up and manual correction of flaws that the automated system cannot fix. b) CAHSD and ITD will work together to develop a system configuration standard that ensures all systems security settings conform to best practices that mitigate possible risks within the next 90 days.
	Follow up Results	a) Two unpatched vulnerabilities were discovered from the 22 computers on which we performed a vulnerability scan. One of the flaws was ranked as High Risk and the other as Medium Risk (in terms of the possibility of being exploited and the consequences to the organization if they were exploited). One of the flaws has remained unpatched for more than three months, and the other one for more than twelve months after the patches were released by the software vendor. b). Eight different configurations vulnerabilities were discovered from the scanned computers. Three (37.5%) of those flaws were ranked as Medium Risk; and five (62.5%) were ranked as Low Risk. ITD is yet to implement the planned configuration standards for user computers and servers. **Comments** a) Although there were significant improvements in the compliance level for software patches, there is still a need for improvement to ensure that flaws capable of being exploited are remediated promptly.

		b) As recommended in the audit report, ITD should implement secure configurations standards that meet, at a minimum, configuration best practices (as specified in the configuration benchmarks guides published by the Center for Internet Security (CIS)) for all operating systems on user computers and servers.
	Conclusion on Remediation Status	Issues not fully resolved: **Finding is open**
Finding 6	There was no policy for secure use of removable storage media, and no documentations to provide evidence of secure sanitization or destruction of old electronic storage media.	
	OCA Recommendation	CAHSD and the Internal Service Department (ISD), in conjunction with ITD, should establish a written policy and also guidelines for secure use, sanitization, reuse and destruction of storage media (hard disk and removable media), and documentation requirements to evidence sanitization and destruction actions.
	Management Remediation Plan	ITD's Field Services Division has in place a Media-Vise compact desktop/laptop hard drive destruction unit. The Media-Vise Compact unit allows safe and quick destruction of data stored on County IT hard drive assets. ITD and CAHSD will be coordinating to leverage our existing Service Level Agreement (SLA) with the Field Services Division to establish a disk/data destruction procedure which has led to the destruction of 50 hard drives as of October 1, 2012.
	Follow up Results	There was a list of computer hard drives scheduled for disposal from April through July, 2013; however, there was no documentation to provide evidence of proper actual destruction. CAHSD does not yet have a documented policy and procedures that would ensure continuous and consistent practices for secure media sanitization and disposal. **Comments** CAHSD management should implement a formal Electronic Media Disposal policy to ensure consistent and documented practices for securely disposing computers and storage media.
	Conclusion on Remediation Status	Issues not fully resolved: **Finding is open**
Finding 7	Policy for secure custody of clients' files/records was violated in two of the DHS sites we visited.	
	OCA Recommendation	CAHSD Personnel must ensure full compliance with the department's policy on secure custody of client files and records. Records slated for shredding should be given equivalent protection until they

		are shredded.
	Management Remediation Plan	a) Require that all Upper Level Management protect MDC office areas that contain information assets, and information processing facilities. b) Require that all CAHSD's employees take part in all County-Wide Security Awareness Training and Refresher. As of September 24, 2012, 89% of employees have completed the Mandatory Security Awareness Refresher Training. We are planning to have this mandate completed by October 31, 2012. c) Also, HIPPA online training will be provided agency wide to the staff whose works requires the manipulation of sensitive and confidential clients' data. d) Requested link to CAHSD Policies and Procedures (P&P)be pushed out to all CAHSD workstations upon final approval of P&P.
	Follow up Results	From March 2013 through April 2014, CAHSD personnel took a number of computer and information security related trainings, as detailed below: Number of staff — Training Title 506 — HIPPA/HITECH Security Awareness course; 591 — HIPPA/HITECH Privacy course; 159 — Initial Security Awareness course; 83 — PCI Data Security course; 83 — Recognizing Identity Theft course; 227 — Security Awareness Refresher course. **Comments** Personnel were receiving necessary security awareness training that should help them to comply with security requirements. Security awareness training policy and procedures have been developed and approved into operation by CAHSD management.
	Conclusion on Remediation Status	Issues resolved: **Finding is closed**
Finding 8	Department did not have a policy or guidelines to ensure that user-developed databases and spreadsheets containing clients confidential information are secured with appropriate security mechanisms.	
	OCA Recommendations	a) CAHSD, in consultation with ITD, should implement adequate security mechanisms (including encryption) to protect all existing user-developed databases that contain confidential information in the department.

		b) CAHSD, in consultation with ITD, should develop a written policy and also guidelines that will ensure all in-house and user-developed applications and databases are secured with appropriate security mechanisms before they are put to use.
	Management Remediation Plan	a) The Department will assess and inventory databases currently in use within the department; • Request inventory of databases and spreadsheets for security assessment. • Identify databases and spreadsheets owners and custodians. • Appropriate security measures will be implemented for those databases, including the access to the Secure File Transfer Protocol (SFTP) server. b) An In-house Programming P&P was developed and is awaiting approval and dissemination throughout the entire CAHSD.
	Follow up Results	An In-house software development policy has been implemented. The policy provides baseline requirements intended to ensure that better security and documentation requirements are met in all in-house developed systems.
	Conclusion on Remediation Status	Issues resolved: **Finding is closed**

THIS PAGE INTENTIONALLY BLANK