




**BOARD OF COUNTY COMMISSIONERS  
OFFICE OF THE COMMISSION AUDITOR**

**M E M O R A N D U M**

**TO:** Michael Liu, Director, Department of Public Housing and Community Development (PHCD)

**FROM:** Charles Anderson, CPA  
Commission Auditor 

**DATE:** March 4, 2016

**SUBJECT:** **Closure** of the Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information – *Former Public Housing Agency*

---

The Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information (*Former Public Housing Agency*) final report was issued on October 11, 2012. On May 5, 2015, the Office of the Commission Auditor (OCA) issued a Follow-up report. The Follow-up report summarized the OCA's assessment of the implementation status of recommendations contained in the original audit report as follows: Two findings in the original report had been fully resolved, six findings were partially resolved, and one was not resolved.

In the Follow-up report, OCA requested the management of PHCD to report, within 90 days, subsequent actions taken by management to implement the recommendations on audit findings that were still pending. We have received and reviewed the requested management report (*attached*) of subsequent actions. While it is clear from the management report that some of the pending issues were not conclusively resolved, we are satisfied that the management proposed actions, when implemented, would resolve the pending issues. We would like to reiterate management's responsibility in ensuring that all internal control weaknesses identified in the audit report are adequately resolved. This audit is now closed.

We thank the staff of the PHCD and the Information Technology Department for their cooperation and input throughout the audit lifecycle. Please let me know if you need further information.

c: Honorable Chairman Jean Monestime,  
and Members, Board of County Commissioners  
Mayor Carlos Gimenez, County Mayor  
Russell Benford, Deputy Mayor, Office of the Mayor  
Abigail Prince-Williams, County Attorney  
Mary T. Cagle, Inspector General  
Cathy Jackson, Director, Audit and Management Services  
Angel Petisco, Director, Information Technology Department  
Mari Saydal-Hamilton, Assistant Director, PHCD  
Lars Schmekel, Chief Security Officer, Information Technology Department  
Ray Diaz, Manager, Technical Services Division, PHCD


THIS PAGE INTENTIONALLY BLANK

# Memorandum



**Date:** February 23, 2016

**To:** Charles Anderson, CPA, Commission Auditor  
Board of County Commissioners, Office of the Commission Auditor

**From:** Michael Liu, Director   
Public Housing and Community Development

**Subject:** **Follow-up Report:** Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information – *Former Public Housing Agency*

---

This serves as a response to the reported findings and recommendations to the initial memorandum as well as the follow-up responses provided on May 15, 2015.

**Finding 1:** Department uses Wireless Local Area Network (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.

*ITD Response: ITD has replaced all remote location Access Points with WPA2 compliant AP's. ITD will continue to address and replace remaining Wireless Encryption Protocol (WEP) enabled Access Points within other facilities, county wide, through the edge network modernization project. If access Points on the new edge infrastructure have WEP configured, it will be disabled by FY 14-15 year.*

*The Enterprise Security Office will develop and implement a procedure to identify and follow up with ITD Field Services to ensure quarterly vulnerability reports are addressed in a timely manner within the next 90 days. The Enterprise Security Office has developed a manual process for identification and inventory of WEP based AP's. This process will be implemented through the Field Services Division and technicians will be trained within the next 120 days. The use of automated tools to identify WEP based AP's will be re-investigated to determine if remote inventory can be accomplished programmatically and used in the continued planning for the decommissioning older WEP based AP's*

**ITD Follow-up Response (2-17-16):**

*Staffing constraints have delayed the implementation of the proposed procedures. Procedures have been developed, however training delayed. WEP based Access Points at other County locations will be removed from service over the next 6 months and is anticipated to be completed by the end of FY15-16.*

**Finding 2:** Access to electronic files containing confidential information of programs' applicants/participants was not effectively restricted to only those who should have access.

**Recommendations:**

- a) PHCD should ensure that appropriate access privileges are set on all folders and files containing confidential or sensitive information, and establish a periodic review process to revalidate assigned access privileges.
- b) PHCD should securely delete files and documents that are no longer required for business use.
- c) PHCD should educate end users and data owners on how to effectively protect their electronic documents from unauthorized access.

**Remediation Status:** Fully resolved

**Finding 3:** Unencrypted emails were being used to transmit and share confidential documents.

**Recommendation:**

Personnel should stop sending confidential information via unencrypted emails. Department should consider the possibility of creating a shared repository (with appropriate access control) to be used for sharing information in the affected operational process.

**Remediation Status:** Not fully resolved.

***PHCD Response:***

*As mentioned in the findings, PHCD has taken steps to train staff on the use of the Secure Ad Hoc Transfer Module, including making it part of the new employee orientation. PHCD will fulfill this finding by establishing a formal use policy within 30 days that will require personnel to use the Secure Ad Hoc Transfer Module to share or transfer confidential documents.*

***PHCD Response (2-17-16):***

For internal and secure communications, all users are utilizing a minimum of Microsoft Exchange and Outlook 2010. For external communications, PHCD utilizes the County's secure electronic file transfer solution which encrypts confidential information that needs to be shared with external parties. The County includes this as part of the employee onboarding training.

**Finding 4:** Cryptographic mechanism (encryption) necessary to better protect confidential information in databases was not implemented for certain critical database used by the department.

**Recommendation:**

PHCD in conjunction with ITD should implement appropriate encryption, truncation or similar mechanism to conceal or disguise sensitive or confidential contents of records in critical databases.

**Remediation Status:** Not resolved at all.

***ITD & PHCD Response:*** *In the initial audit response, it was indicated that the vendor would be contacted to determine when encryption would be available through their software. A follow up by PHCD and ITD with the vendor will be completed within the next 60 days to determine the availability of a vendor supplied encryption solution and associated fiscal impact. ITD has discussed the performance impact of natively enabling full database encryption (SQL) with PHCD. ITD and PHCD will engage with third party encryption vendors to determine if alternatives exist which would meet performance requirements by encrypting only sensitive fields and confidential data as necessary and do not invalidate vendor support from the application or database vendors.*

Follow-up Report: Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information – Former Public Housing Agency

***ITD & PHCD Response (2-17-16):***

PHCD's vendor does not have an encryption solution and does not have any immediate plans to implement one as it is not a HUD requirement or being heavily requested by its clients. ITD's security and database teams have put forth a significant amount of effort in providing multiple layers of security. All County databases, including PHCD databases, are in the process of being moved to a Secure Access Zone (SAZ). This network security zone is being implemented to provide a stronger, consistent level of security and access to the databases. Access to any databases in this zone must follow stringent guidelines and every connection request is submitted to the Office of the CSO (Chief Security Officer) for review and approval. While this does not specifically address the recommendation of an encryption solution, we do believe that ITD has established "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records..." per federal guidelines. When implementing additional security, cost, administrative burden, efficiency, resources, and risk should all be taken into account to determine whether a safeguard is feasible to implement.

**Finding 5:** Policies and processes for managing computer user passwords and accounts on department and County computing resources were weak. We also noted a number of practices with respect to computer user accounts that impaired security of computer systems and accountability for user actions. These include:

- a) Unnecessary default (built-in) accounts were not disabled in some user computers.
- b) Generic/shared accounts were being used to administer critical databases and applications.
- c) Excessive high privileges were assigned to users in critical databases and application beyond what the users needed to perform their job functions.
- d) Users' successful logins (access) to critical databases were not being logged.
- e) Computer accounts of 26 former employees of PHCD and 20 former employees of a business partner were not disabled promptly after the employees were separated.

**Recommendations:**

- a) ITD should enforce password maximum lifetime policy for users' domain accounts.
- b) PHCD should disable all unnecessary default accounts on computers, databases and applications.
- c) Assign unique ID to each person with computer access to ensure accountability for each user's actions, and remove excessive privileges assigned to any user.
- d) Enable logging of access to critical systems to provide sufficient audit trail for users' access.
- e) Establish written and well-supervised procedures for granting, modifying, monitoring, and promptly revoking user access on all systems used by the department.

**Remediation Status:** Not fully resolved

***ITD & PHCD Response:*** ITD will work with PHCD to ensure unnecessary default accounts are fully disabled within 90 days. During this period, another review of generic accounts and privilege levels will be conducted to ensure appropriate access levels and unique user ID's ITD will align PHCD user policy with enterprise password policy and implemented by FY 14-15 year end. Logging capabilities of applications will be reviewed to determine if the application is capable of capturing sufficient user access/action data

*audit trails and will determine if audit logs can be exported to a logging server for a minimum of 1 year retention.*

***ITD & PHCD Response (2-17-16):***

In September 2015, ITD implemented an automated process that will automatically disable a user account that has not authenticated itself within a 60 day period. To supplement this process, ITD also sends a weekly report to IT administrators and support staff detailing which user accounts are encroaching on the 60 day period as a preventative measure to ensure that critical accounts are not marked inactive and thus impact business operations.

Please refer to attachments A, B, and C which outline user account management procedures along with the auditing policy enabled on all Miami Dade County workstations and servers.

- User Account Management SOP
- Terminated Employee Procedures SOP

**Finding 6:** Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems.

**Recommendations:**

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

**Remediation Status:** Not fully resolved

***ITD Response:***

*ITD will further improve the process through the development of follow up procedures including an incident ticketing capability with Field Services to ensure corrective action targeting high risk vulnerabilities initially not corrected by automated patching are addressed and automated processes are re-enabled.*

*In addition to the OS patching currently being performed by the SCCM environment, the Information Technology Leadership Council (ITLC) formed the Browser Modernization Working Group. This group has developed procedures and recommendations on browser modernization which will address additional application vulnerabilities in commonly used third party software including Java, Adobe Acrobat Reader and Adobe Flash. This is currently being piloted by WASD and will be implemented at CAHSD and PHCD by FY 14-15 year end.*

***ITD & PHCD Response (2-17-16):***

ITD is currently working on a “secure host image” that contains a standard system configuration that ensures all system security settings conform to best practices that mitigate possible risks. ITD is working with PHCD IT support staff to test and rollout the image to all users. Barring any major unforeseen issues, it is expected that this rollout will take 2-3 months.

**Finding 7:** Department did not have a written policy or guidelines for secure use, sanitization and destruction of electronic storage media.<sup>4</sup>

**Recommendations:**

PHCD should establish a written policy and procedures for secure use, sanitization and destruction of storage media. Policy should include documentation requirements to evidence media sanitization and disposal actions.

**Remediation Status:** Not fully resolved.

***PHCD Response:***

*PHCD created a formal, signed IT Asset Management Standard Operating Procedure document in January 2015 which includes procedures for sanitization and destruction of storage media and documentation requirements. In addition, PHCD believes that this policy and guidelines is applicable countywide and therefore a countywide policy (administrative order) should be created to address this for all departments.*

***ITD & PHCD Response (2-17-16):***

This finding should be closed.

**Finding 8:** Closed clients' document files due for destruction were not destroyed.

**Recommendations:** PHCD should comply with record retention policy and securely destroy clients' records that have outlived their retention periods.

**Remediation Status:** Fully resolved.

**Finding 9:** PHCD did not have adequate computer and information security training and awareness program for members of its workforce.

**Recommendations:** PHCD should establish a computer and information security training and awareness program that provides initial and ongoing training/awareness for members of its workforce. The program should address minimum training for all members, as well as additional training specific to staff job functions.

***PHCD Response:***

*As mentioned in the findings, PHCD has undergone efforts to train staff via the Secure IT Training and also has sent communications to all PHCD staff reminding them of the need to protect sensitive information to include the "Do's and Don't's of a Human Firewall" and HUD Notice PIH-2014-10, which provides Privacy Protection Guidance for Public Housing Agencies and other third parties.*

*As recommended, PHCD will also take additional steps and draft a formal policy requiring mandatory training. We will coordinate the training through ITD's Information Security Awareness Coordinator.*

**Remediation Status:** Not fully resolved.

***ITD & PHCD Response (2-17-16):***

PHCD will continue with efforts mentioned in previous response and will coordinate recurring training of staff through ITD.

Thank you for this opportunity to address the findings and recommendations of your audit. If you have any questions, please contact us at 786-469-4100

- c: Russell Benford, Deputy Mayor, Office of the Mayor
- R. A. Cuevas, Jr., County Attorney
- Mary T. Cagle, Inspector General
- Cathy Jackson, Director, Audit and Management Services
- Angel Petisco, Director, Information Technology Department
- Mari Saydal-Hamilton, Assistant Director, PHCD
- Lars Schmekel, Chief Security Officer, Information Technology Department
- Ray Diaz, Manager, Technical Services Division, PHCD
- Neil R. Singh, Audit Manager, OCA