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 05, 2015

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

We issued the final report of the Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information − Former Public Housing Agency (*now a part of Public Housing and Community Development (PHCD) Department)* 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 PHCD, 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 PHCD 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
Michael Liu, Director, PHCD
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

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 Public Housing Agency

(Now a part of PHCD Department)

FOLLOW-UP

Project Number 11-143370

May 05, 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 prior audit recommendations. The objective of this follow-up audit was to assess the actions taken by management of Public Housing and Community Development (PHCD) 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 Miami-Dade Public Housing Agency (MDPHA). MDPHA is now part of Public Housing and Community Development (PHCD). 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 MDPHA'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. Access to electronic files containing confidential information of programs' applicants/participants was not effectively restricted to only those who should have access.
3. Unencrypted emails were being used to transmit and share confidential documents.
4. Cryptographic mechanism (encryption) necessary to better protect confidential information in databases was not implemented for certain critical database used by the department.
5. Policies and processes for managing computer users' passwords and accounts on department and County computing resources were weak.
6. Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems.
7. Department did not have written policy or guidelines for secure use, sanitization and destruction of electronic storage media.
8. Closed clients' document files due for destruction were not destroyed.
9. Department did not have adequate computer and information security training and awareness program for members of its workforce.

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

II. SUMMARY RESULTS

Our follow-up audit revealed that PHCD and ITD have made substantial progress in remediating the audit findings. Two of the findings above have been fully resolved, six have been partially resolved, and one has not been resolved. The two findings that are fully resolved are henceforth closed. Below is the summary of the remediation status of the audit findings:

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.

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.

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.

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

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:

a) ITD should review flaw remediation and system configuration management processes, and implement needed enhancements that will assure effective remediation of systems flaws.
b) 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

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

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.

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.

Remediation Status: Not fully resolved.

IV. CONCLUSION

OCA acknowledges the actions taken by PHCD 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 PHCD programs.

ATTACHMENT I

Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information:
Former Public Housing Agency (PHA)
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**) ITD should establish an effective risk assessment and control processes to continuously manage the risks of wireless network.
	Management Remediation Plan	ITD will develop an effective risk assessment and control processes 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 PHCD 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.

ATTACHMENT I

Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information:
Former Public Housing Agency (PHA)
Details of Findings Remediation Status

		Comments **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 breaches. **2**) Uncorrected vulnerabilities in the configuration 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 can allow malicious individuals to install rogue APs in the network to compromise confidential and sensitive information. **Further Recommendations** **1**) ITD should complete the upgrade of the legacy (WEP based) WLAN technology to a more secured WPA2 based technology. **2**) ITD should document 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	Access to electronic files containing confidential information of programs' applicants/participants was not effectively restricted to only those who should have access.	
	OCA 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.
	Management Remediation Plan	**a**) A file share permission was identified which allowed read permission to the specified group across all PHCD folders. This has now been rectified with ITD's assistance as noted above in the auditor's own findings labeled as "Actions taken by department." **b**) PHCD is reviewing the retention requirements for electronic files.

		c) This item is being addressed by ITD's Secure IT Training, which is available online as a mandatory required training for all county employees. As of September 26, 2012, 332 of 454 (73 %) PHCD employees either completed or were in some stage of completion of the IT Secure Training. It is expected that this mandate will be finalized within the next three months.
	Follow up Results	**a**) Access to shared electronic resources has been properly restricted to authorized users. **b**) Old files that were no longer required for business use were identified and deleted. **c**) Employees received relevant training relating to security of electronic information.
	Conclusion on Remediation Status	Issues resolved: **Finding is closed**
Finding 3	Unencrypted emails were being used to transmit and share confidential documents.	
	OCA 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.
	Management Remediation Plan	**a**) PHCD has already employed secured SharePoint sites for collaboration amongst various teams. The technology will be leveraged for site staff to securely share files to meet the operational needs. We expect to have this option deployed by November 15, 2012 across the department. **b**) ITD will investigate the implementation of secure, encrypted emails and provide recommendations on implementation and costs by January 30, 2013.
	Follow up Results	**a)** Microsoft Exchange 2010 was implemented, but the encryption functionality was not yet enabled for sending encrypted emails. **b)** There was no policy to mandate personnel to use the Secure Ad Hoc Transfer Module implemented as an alternative solution for sending confidential documents. **Comments** PHCD should either enable the email encryption functionality in Exchange 2010 or develop a formal use policy that will require personnel to use the Secure Ad Hoc Transfer Module to share or transfer confidential documents.
	Conclusion on Remediation Status	Issues not fully resolved: **Finding is open**

ATTACHMENT I

Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information:
Former Public Housing Agency (PHA)
Details of Findings Remediation Status

Finding 4	Cryptographic mechanism (encryption) necessary to better protect confidential information in databases was not implemented for certain critical database used by the department.	
	OCA 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.
	Management Remediation Plan	PHCD in conjunction with the application vendor and ITD are working on the design of a solution to implement protection of sensitive or confidential contents of records in critical databases. The design and cost for implementation are expected to be available by January 30, 2013 and an implementation plan will follow two weeks from the approval date.
	Follow up Results	No encryption mechanism has been implemented to protect the confidential data residing in critical databases. As per PHCD follow up response, the vendor is aware of the need for integrating a cryptographic solution into their system and plans on doing so in future releases.
	Conclusion on Remediation Status	Issues not resolved: **Finding is open**
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 MDPHA and 20 former employees of a business partner were not disabled promptly after the employees were separated.	
	OCA 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
	Management	**a)** Domain Password policies have been developed which are aligned with information security best

	Remediation Plan	practices. These requirements will be enabled for all PHCD accounts in a phased implementation to minimize user impact and business interruption. This implementation is expected to be completed by December 18, 2012. **b)** PHCD is reviewing the disabling of group access to default accounts, databases and applications. In addition, ITD has communicated to PHCD Departmental administrators the implementation of disabling and renaming guest accounts on windows systems which will be completed on October 2, 2012. **c)** This process is already in current practice throughout the department at PHCD. 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, PHCD's Human Resources division is in constant contact with PHCD's Technical Services Division to disable any accounts and/or passwords for employees who retired, transferred or terminated from the County. **d)** It should be noted that PHCD's Emphasys Computer Solutions database (ECS) currently logs user access to client accounts and has been used on occasion for internal employee investigations. ITD will implement an automated method to record unsuccessful logins. Logs will be retained for review for a period of one year. This is expected to be in place by October 30, 2012. **e)** This is already the current practice throughout the department at PHCD. As previously stated, each user is granted unique access through a supervisor approved CRS form where only the needed operational account privilege is requested and granted. The CRS form is required by ITD and is part of the County's written policies and procedures in order to create a unique user in Active Directory. In order for access rights to be modified, a new CRS form must be completed with the appropriate supervisor
	Follow up Results	Password and account policies are still very weak for the critical database referenced in the audit report. From the sample of 27 user accounts in a database on which we conducted a password audit, two accounts had a blank password; in another two accounts, the passwords were the same as the user IDs; and one other account had a common, easy to guess password. Further, the database password expiration policy was not enforced. **<u>Comments</u>** PHCD should work with ITD to enforce strong access and password policies that would eliminate and prevent the use of weak passwords on critical systems and databases. Enforced policies should also require password changes at periodic intervals.

ATTACHMENT I

Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information:
Former Public Housing Agency (PHA)
Details of Findings Remediation Status

	Conclusion on Remediation Status	Issues not fully resolved: **Finding is open**
Finding 6	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, and implement needed enhancements that will assure effective remediation of systems flaws. **b**) ITD should develop a 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 PHCD regular reports on systems that are non-compliant for follow-up and manual correction of flaws that the automated system cannot fix. **b)** PHCD 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**) 1. Twenty five different unpatched vulnerabilities were discovered from the 22 computers on which we performed vulnerability scan. Eighteen (72%) of those flaws were ranked as High Risk in terms of possibility of being exploited and the consequences to the organization if they were exploited. The remaining seven (28%) vulnerabilities were classified as Medium Risk. Twenty one (84%) of the unpatched flaws had been outstanding for more than 24 months after the software vendor released fixes. 2. Nine of the 22 computers scanned in PHCD were still running on the Window XP operating system which is no longer supported by Microsoft (i.e. security patches and updates are no longer being provided by Microsoft to address vulnerabilities that may be discovered in the future). **b)** Seventy eight different configurations vulnerabilities were discovered from the scanned computers. Thirteen (17%) of those flaws were ranked as Medium Risk; 65 (83%) were ranked as Low Risk. ITD is yet to implement the planned configuration standards for user computers and servers. **Comments** **a)** ITD and PHCD should improve on follow up activity in the vulnerability management process as recommended in the audit report. PHCD should consider the replacement of unsupported operating

		system(s), or quarantine the computers on which they run if they must be used for proprietary applications. **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 7	Department did not have a written policy or guidelines for secure use, sanitization and destruction of electronic storage media.	
	OCA Recommendation	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.
	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 PHCD have leveraged 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 110 hard drives as of September 24, 2012.
	Follow up Results	Sufficient documentation was maintained for storage media that were destroyed between September 2012 and September 2013. However, there was no media disposal policy that has been formally documented and approved into operation by the PHCD management that would ensure continuous and consistent practice for secure media sanitization and disposal. **<u>Comments</u>** PHCD management should approve into operation a formal 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 8	Closed clients' document files due for destruction were not destroyed.	
	OCA Recommendation	PHCD should comply with the record retention policy and securely destroy clients' records that have outlived their retention periods.

Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information:
Former Public Housing Agency (PHA)
Details of Findings Remediation Status

	Management Remediation Plan	We are appreciative of the audit findings and will continue to address this problem by reviewing stored documents, sending relevant documents to storage with the Clerk of Courts, or destroying them in accordance with the appropriate state retention schedules. The Asset Management Director responsible for overseeing the Public Housing program will be notified of the finding that files were improperly stored and we will implement controls to take care of the problem.
	Follow up Results	There was documentary evidence showing that from November 2013 through January 2014: • Fifty four boxes of records were transferred to the Clerk of Courts for archival storage. • A thousand and ninety five boxes of records were submitted to the Clerk of Courts for destruction.
	Conclusion on Remediation Status	Issues resolved: **Finding is closed**
Finding 9	PHCD did not have adequate computer and information security training and awareness program for members of its workforce.	
	OCA Recommendation	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.
	Management Remediation Plan	As of September 26, 2012, 332 of 454 (73%) PHCD employees either completed or were in some stage of completion of the IT Secure Training. We hope to have this mandate finalized within the next three months.
	Follow up Results	PHCD employee training records showed that 878 employees completed the Secure IT Training from June 1, 2012 through March 12, 2014. However, there was no written policy on computer security awareness training that requires or would remind employees to retake training periodically. **Comments:** PHCD management should approve into operation a formal policy on computer security awareness training to ensure that employees continue to adhere to training requirements.
	Conclusion on Remediation Status	Issues not fully resolved: **Finding is open**