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:

Miami Dade Public Housing Agency
(Currently a part of Public Housing and Community Development Department)

Project Number 11-143370

October 11, 2012

Charles Anderson, CPA
Commission Auditor

Auditors

Michael O. Bayere, CIA, CISA, CISSP	Auditor-In-Charge
Norma Roig, CPA, CGMA	Senior Auditor
Noel Aranha, CPA, CGMA	Acting Audit Manager

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

THIS PAGE INTENTIONALLY BLANK

BOARD OF COUNTY COMMISSIONERS
OFFICE OF THE COMMISSION AUDITOR

M E M O R A N D U M

TO: Honorable Joe A. Martinez, Chairman
And Members, Board of County Commissioners

FROM: Charles Anderson, CPA
Commission Auditor

DATE: October 11, 2012

SUBJECT: Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information (*former Public Housing Agency)*

We have concluded our Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information for the former Public Housing Agency (now part of Public Housing and Community Development Department) and submit this report which contains findings, recommendations, and management responses. Management concurred with all of our findings and recommendations, except for one where they partly concurred. We have provided clarifying comments where they did not fully concur.

We thank the staff of Internal Services, Information Technology Department, and Public Housing and Community Development for their cooperation and input throughout the review. Please let me know if you need further information.

c: Mayor Carlos Gimenez, County Mayor
Russell Benford, Deputy Mayor, Office of the Mayor
Gregg Fortner, Executive Director, PHCD
R. A. Cuevas, Jr., County Attorney
Chris Mazzella, 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
Jose L. Rivero, Director, Technical Services Division, PHCD

THIS PAGE INTENTIONALLY BLANK

TABLE OF CONTENTS

I. Objectives and Scope …...……1

II. Methodology …...……..1

III. Background ……...……...2

IV. Summary Results ……3

V. Findings and Recommendations ……4

Finding 1 ……..4
Recommendations…….....4
Management Response…….....5

Finding 2 ...……...5
Recommendations ……....6
Management Response ……...6

Finding 3 ……...6
Recommendation .……....7
Management Response……..7

Finding 4 ...……...7
Recommendation .……....7
Management Response……..7

Finding 5 ...……...8
Recommendations ……....8
Management Response…….....9
Commission Auditor Comments …….....9

Finding 6 ...……10
Recommendations ……11
Management Response ...……...11

Finding 7 ...……11
Recommendation .……...12
Management Response ...……...12

Finding 8 ...……12
Recommendation …….... 13
Management Response ...……...13

Finding 9 ...……13
Recommendation …….... 13
Management Response ...……...14

Attachment:
Management Response memo……..……15

THIS PAGE INTENTIONALLY BLANK

1. OBJECTIVES AND SCOPE

As part of the work plan approved by the Miami-Dade County Board of County Commissioners (BCC), the Office of the Commission Auditor (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) Department. 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 clients (programs applicants/participants). The scope of the audit was from October 1, 2010 through March 31, 2012.

II. METHODOLOGY

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and IT Audit and Assurance standards (*issued by ISACA*), except for section 3.82 (b) of GAGAS which requires audit organizations to obtain an external peer review at least once every three years. Those standards require that we plan and perform the audit to obtain sufficient, reliable, relevant and appropriate evidence to provide a reasonable basis for our findings and conclusion based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion based on the audit objectives.

To accomplish our objectives, we identified all MDPHA services/programs, and reviewed processes for the collection, processing, transmission, storage, and disposal of programs participants' information that are considered confidential. We identified relevant regulations, statutes, standards and Acts that applied to MDPHA programs with respect to information security. We identified all the major systems (applications and databases) the department uses in its processes, and performed risk analysis of the processes and systems to determine our audit tests.

Our audit tests included a review of physical controls for safeguarding records and electronic media containing confidential information across the department; and tests of security controls incorporated into computer applications and databases for those applications and databases managed and maintained either by the MDPHA or the Miami Dade Information Technology Department (ITD). We reviewed network security controls for protecting MDPHA computer network systems. We also used commercial vulnerability assessment software[1] to perform vulnerability assessment on MDPHA critical servers (centralized, high capacity computers serving other computers) and a sample of user computers (workstations). Due to access restrictions, we did not perform detailed security review of applications and databases used by MDPHA but are owned, maintained and administered either by the State of Florida or the Federal government.

In addition, we interviewed key personnel and assessed information security physical and administrative controls in seven (7) MDPHA sites across the County, and in other centralized divisions in the administrative office. We reviewed relevant County administrative orders,

[1] Software specifically developed to identify and report on security weaknesses in computer systems

MDPHA and ITD information security policies, administrative procedures and other related records.

We benchmarked our security controls tests with security requirements of the U.S. Department of Housing and Urban Development (HUD) information security policies, applicable regulations, statutes, standards, and acts (including HIPAA[2], the Privacy Act of 1974, Title 24 CFR[3] part 5, and PCI DSS[4]); and with recommended information systems security controls[5] by the National Institute of Standards and Technology (NIST).

III. BACKGROUND

MDPHA administers Federal funds for public housing programs throughout Miami Dade County. MDPHA programs comprise the subsidized public housing and private rental housing programs. The public housing programs are provided for residents in the extremely low-income groups. Programs in this category include Section 8 Housing Voucher Program, Moderate Rehabilitation Program, Assisted Living Program for the elderly, Reasonable Accommodation Program for qualifying people with disabilities, and HOPE IV Public Housing Development Program.

The private rental housing programs are provided to assist persons with low and moderate income who typically would pay up to 30 percent of their adjusted income towards their rent. Programs under this group include Housing Choice Voucher Program, Moderate Rehabilitation Rental Program, and Single Room Occupancy Program. MDPHA oversees more than 9,200 public housing units and provide Section 8 subsidized rental payment for over 17,000 clients.

The MDPHA was organized into five major divisions, namely Administration, Finance and Accounting, Contract Administration, Facilities and Development, and Asset Management. MDPHA is now a part of Public Housing and Community Development Department.

Administration Division oversees administrative functions, including human resources, technical services, quality management, reasonable housing requests, and handles investigations regarding fair housing complaints.

Finance and Accounting Division provides financial supports to the department, including budgeting, accounting, financial reporting, account payable, and revenue management.

Facilities and Development Division manages the capital improvement and development of housing projects, including the HOPE IV program, the America Recovery and Reinvestment Act (ARRA) projects, and the Building Better Community General Obligation Bond projects.

[2] Health Insurance Portability and Accountability Act of 1996
[3] Code of Federal Regulations on Housing and Urban Development
[4] Payment Card Industry Data Security Standards
[5] Recommended Security Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev 3)

Contract Administration Division administers special section 8 programs, including moderate rehabilitation, single room occupancy; and monitors private contractors for the housing choice voucher program.

Asset Management Division provides property management and maintenance services for public housing developments. Services include leasing, occupancy, relocation, rent, eviction, policy review and development.

MDPHA collects information considered to be personally identifiable from both applicants and beneficiaries of its housing programs. For some programs, health related information is obtained and processed. MDPHA also collects credit card related information via the online rental payment service. Personally Identifiable Information (PII) is any information that can be used (either alone or in combination with other information) to uniquely identify, trace or locate an individual. Examples include social security number, driver license number, passport number, credit card number, full name and mother's maiden name, date and place of birth, biometrics (e.g. fingerprints).

To safeguard the confidentiality and integrity of this information, and to ensure compliance with applicable regulations, statutes, standards, and acts (such as HIPAA, the Privacy Act of 1974, Title 24 CFR part 5, and PCI DSS), robust and effective information security is a necessity for the PHCD. The responsibilities for protecting sensitive and confidential information in PHCD rest not only on the department (PHCD), but also on the Information Technology Department (ITD) because ITD provides certain centralized computing and security services to the department.

IV. SUMMARY RESULTS

Overall, we found that in order to better safeguard the confidentiality and integrity of information in PHCD, improvements are necessary in the following areas:

- Department uses wireless local area network (WLAN)[6] implemented with poor security features that can easily compromise confidential and sensitive information.
- Access to electronic files containing confidential information of programs' applicants/participants was not effectively restricted to only those who should have access.
- Unencrypted emails were being used to transmit and share confidential documents.
- Cryptographic mechanism (encryption)[7] necessary to better protect confidential information in databases[8] was not implemented for certain critical database used by the department.
- Policies and processes for managing computer users' passwords and accounts on department and County computing resources were weak.
- Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems.

[6] Network of computers linked together via wireless technology
[7] Process of using mathematical algorithm to transform plain text information into a format unreadable to persons except those possessing the algorithm key
[8] Repositories of electronic records

- Department did not have written policy or guideline for secure use, sanitization and destruction of electronic storage media.
- Closed clients' document files due for destruction were not destroyed.
- Department did not have adequate computer and information security training and awareness program for members of its workforce.

For security reasons, certain specific information about the above findings is excluded from this report. The specific information was provided to the management of the department and ITD in a separate appendix (*Appendix I*), which is considered sensitive and exempt from public records, in accordance with Chapter 119.071(1)(f) of Florida Statutes.

V. FINDINGS AND RECOMMENDATIONS

Finding 1
Department uses wireless local area network (WLAN) implemented with poor security features that can easily compromise confidential and sensitive information (*Appendix I #T.1*).

The department's WLAN is part of the legacy wireless local area network deployed by the Information Technology Department (ITD) across County departments. The legacy WLAN employed Wired Equivalent Privacy (WEP) security to protect transmitted information. However, WEP is well-known to have inherent security flaws that can easily be exploited by attackers to intercept and compromise information being transmitted on the network. Information that can be compromised includes user login credentials, sensitive systems information, and other confidential information. The National Institute of Standards and Technology (NIST) says the following concerning one of the inherent weaknesses of WEP: "*WEP suffers from a number of cryptographic weaknesses that enable attackers with readily available software tools to decipher captured data, sometimes with as little as a few minutes of recorded traffic*[9]".

Good security practice and relevant information security standards (including HIPAA of 1996, PCI DSS, and NIST SP800-53) require the implementation of appropriate security controls to protect confidentiality and integrity of information during transmission.

Recommendations
a. ITD should upgrade wireless local area network (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.

[9] NIST Special SP 800-97 – Establishing Wireless Robust Security Networks (p. 3-9)

Management Response

PHCD concurs with this finding and responds to the recommendations as follows:

a. *PHCD requested that ITD's Field Services Division provide an estimate for implementation of wireless security. ITD, working closely with PHCD completed the estimate as requested. An implementation plan will be created based on the assessment and estimate. Historically, network equipment located at departmental sites was purchased by departments, either as part of the initial deployment or purchased as needed to replace aging, unsupported equipment. Support and maintenance of the original equipment was provided by ITD. The purchase of replacement equipment as part of modernization or upgrade of the network was funded by departments and implemented by ITD. Recently, ITD adopted a new support model whereby aging network equipment is replaced with newer equipment providing additional functionality and security. The purchase, maintenance and recapitalization of the equipment is now included in a monthly "port charge" of $10.00/active port. A port is defined as the point where a network device (computer/server/printer) is connected to the County's network. The annual service charges include deployment, configuration, management and recapitalization/replacement of the network equipment. This updated business model ensures that each participating department's network will remain current, state of the art, supported and secure.*

b. ITD will develop an effective risk assessment and control processes to continuously manage the risks of 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.

Finding 2

Access to electronic files containing confidential information of programs' applicants/participants was not effectively restricted to only those who should have access *(Appendix I # T.2).*

We found multiple electronic files and documents containing MDPHA clients' and applicants' confidential information (more than 270,000 records) stored in central locations (computer servers) accessible to personnel in County departments other than MDPHA. Those personnel who do not have any business needs for such information should not have access to these confidential records.

Good security practices and relevant information security standards (including HIPAA of 1996, NIST SP800-53, PCI DSS and the Privacy Act of 1974) require that appropriate technical

controls, administrative policies and procedures be implemented to prevent unauthorized users from gaining access to confidential information.

Inadequate protection of confidential and sensitive information from those who do not have legitimate needs to access such information can result in data breaches. According to *Ponemon Institute LLC* report on the *United States 2011 Cost of Data Breach Study*[10], the average cost (direct and indirect expenses to organization) of data breach per compromised record is $194.

Recommendations

a. PHCD should ensure that appropriate access privileges are set on all folders & 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.

Actions taken by the department

Subsequent to our audit field work, the department corrected the inappropriate access privileges granted on the affected files and documents.

Management Response

PHCD concurs with this finding and responds to the recommendations as follows:

a. A file share permission was identified which allowed read permission (Users ( ))[11] 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 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.

Finding 3

Unencrypted emails were being used to transmit and share confidential documents (*Appendix I #T.3*).

We found a particular operational process in which scanned clients confidential information were being shared among personnel for review and approval purposes via unencrypted emails. Sharing confidential information via unencrypted emails can lead to breach of information. Good security practice and relevant information security standards (including HIPAA of 1996, PCI DSS, and

[10] http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US

[11] Specified directory redacted for security reasons

NIST SP800-53) require the implementation of appropriate security controls (including encryption) to protect the confidentiality and integrity of information during transmission.

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 Response
PHCD concurs with this finding and responds to the recommendation as follows:

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.

ITD Response - ITD will investigate the implementation of secure, encrypted email and provide recommendations on implementation and costs by January 30, 2013.

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

We found that no encryption or truncation mechanism was implemented to protect sensitive information, such as social security number (SSN), in one critical database that holds MDPHA clients records. Good security practice demands that encryption, truncation or similar mechanisms be used to conceal or disguise sensitive contents in data repository (database). This security feature provides an additional layer of protection for the data in case a person gains unauthorized access to the database.

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 Response
PHCD concurs with this finding and responds to the recommendation as follows:

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.

Finding 5
Policies and processes for managing computer users' passwords and accounts on department and County computing resources were weak *(Appendix I #T.5).*

We found that computer users are not required to periodically change the passwords to their domain accounts on the County/department computer network. The domain account for each employee grants access to the County/department computing and network resources. We found users that had been using the same passwords for more than four (4) years. Failure to change accounts passwords periodically gives malicious users or attackers almost endless time to figure out user's password, or to continue to use passwords that have been compromised. Good security practice requires that computer users are forced to change their passwords at reasonable intervals (e.g. every 90 or 180 days). ITD is responsible for enforcing password policy across County networks.

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 need to perform their job functions.
d. Users' successful logins (access) to critical databases were not being logged.
e. Computer accounts of twenty six (26) former employees of MDPHA and twenty (20) former employees of a business partner were not disabled promptly after the employees were separated.

These practices pose a number of risks. Leaving unnecessary default (built-in) accounts active on computer systems can provide easy channel for attackers or malicious users to gain unauthorized access to such systems. Using generic/shared accounts to administer systems hinders the ability to account for the actions of individual personnel using the shared accounts. Giving excessive system privileges to computer users can lead to both the abuse of such privileges and unauthorized actions. Not logging successful access to critical systems impedes audit trail of access to systems and information. Unrevoked accounts of former employees and former external users can become veritable tool for malicious individuals to gain unauthorized access to stored information.

<u>Recommendations</u>
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 Response

Adequate procedures for user passwords and accounts are currently in place throughout the department. Additional details are included in the following response to the recommendations:

a. *Domain Password policies have been developed which are aligned with information security best 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 signatures included. Our department's Personnel staff use workflows in our HRIS application to ensure that Technical Services Division is promptly notified to restrict access for departed or soon to depart employees*.

Commission Auditor Comments

Response (c): Specific accounts that were being shared by staff to perform sensitive and privileged tasks on databases were identified, communicated to and discussed with the department.

Response (e): Procedures for managing computer user access existed in the department but were not adequate, partly because of inadequate supervision/follow up. We identified and communicated to the department specific user accounts of former employees and contractors that should have been removed or disabled on multiple systems.

Finding 6

Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems *(Appendix I #P.1).*

Computer flaws are either configuration errors or program errors/bugs that expose computer systems to possible attacks and unauthorized access. Software vendors release patches[12] periodically to correct known errors or bugs in their software. Timely and effective application of those patches, as soon as they are released, is critical to safeguarding vulnerable computers from the activities of computer hackers who frequently search for such vulnerabilities to exploit.

We scanned twenty-three (23) computers (including servers) in MDPHA and found eighty-four (84) different types of program flaws that remained unpatched months after the vendors had released patches. Because there are different levels of risk associated with software vulnerabilities, industry best practice is to prioritize the speed with which released patches are applied, such that security patches that are rated 'High' risk are applied first before those with lower risk ratings. The goal should be to apply all relevant security patches promptly before attackers exploit the vulnerabilities. ITD patch management policy and procedures require that all security patches be applied to all applicable systems within the County network within one (1) month following the release of patches.

For the eighty-four (84) unpatched flaws we identified in our assessment, the number of months that had elapsed since the release of the relevant patches up to the time of our assessment, and the risk levels associated with the unpatched system flaws are depicted in *Tables 1* and *2* below.

Table 1: *Age Analysis of Unpatched System Flaws*

Months	Number of Patches	%
3 – 6	19	23%
7 – 12	10	12%
13 – 36	21	25%
Over 36	34	40%

Table 2*: Risk Levels of Unpatched System Flaws*

Risk Level	Number of Flaws	%
High	59	70%
Medium	21	25%
Low	4	5%

Risk level is determined based on industry Common Vulnerability Scoring System (CVSS), which considers, among other factors, the likelihood and the impacts of a vulnerability being exploited.

From the assessment of the twenty-three (23) sampled computers, we also found sixty-seven (67) system configurations (security settings) that did not conform to recommended best practices necessary to mitigate possible inherent risks.

Computers generally have security settings that can be set to different levels, which in turns determine the degree of protection offered to the computer(s) against exploitation. Misconfigurations of computer systems can open up cracks for malicious users to gain unauthorized access to systems resources and confidential information. Those security settings

[12] Programs written by software vendors to correct known bugs or errors in their earlier released software

identified in our assessment as not conforming to recommended best practices, together with their associated risks are summarized in T*able 3* below.

Table 3: *Risk Levels of System Configuration Flaws*

Risk Level	Number of Settings	%
High	4	6%
Medium	10	15%
Low	53	79%

ITD, in conjunction with department staff, is responsible for patch and configuration management on department computer systems. Although ITD had automated the process for applying patches to vulnerable computers, there needs to be regular and timely review and follow up on systems patched level in order to: (1) identify previous remediation that were unsuccessful, in order to reapply them either manually or via automated system; and (2) discover new vulnerabilities that require remediation.

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 Response

PHCD concurs with this finding and responds to the recommendations as follows:

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.

Finding 7

Department did not have written policy or guideline for secure use, sanitization and destruction of electronic storage media *(Appendix I #P.2).*

MDPHA personnel remove computer hard drives before sending empty computer boxes to Internal Services department (formerly GSA) for donation or disposal. We found hard drives that were locked in a cabinet by the department (MDPHA) without any plan, policy or guidance on how to securely sanitize or destroy them. According to MDPHA staff, the department inherited this practice from HUD's management team that took over the operations of the department from

10/18/07 through 08/25/08. HUD management team possibly could have chosen to store the hard drives without a plan to destroy them during the team's tenure in order to preserve the drives for possible investigations. MDPHA (now PHCD) is now responsible for the management of the department and should ensure that good policies and procedures are in place for secure operations and service delivery.

Good security practice demands that organization have functional policy and procedure for the use, sanitization, reuse and disposal of storage media. In addition, there should be sufficient documentation to track media sanitation/disposal actions (i.e. what was disposed, when, how, and by whom). Without appropriate policy and guidance to ensure secure use, sanitization and disposal, removable storage media may be used insecurely, and old media containing confidential information may eventually be disposed insecurely.

Recommendation

PHCD should establish 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 Response

PHCD concurs with this finding and responds to the recommendation as follows:

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 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.

Finding 8

Closed clients' document files due for destruction were not destroyed *(Appendix I #P.3).*

We noticed in two of the sites we visited that clients' files that had been closed and maintained beyond their retention periods were yet to be destroyed. Some files had been closed as far back as between 1992 through 2000 but were still retained. Because files that have exceeded their retention periods were not destroyed, it creates space constraints for securing files in those locations. In one location, clients' files were stored in open boxes on top of file cabinets placed in a common office area used for multiple purposes, including attending to visitors and eating lunch. In another location, closed old files were stored in unlocked cabinets placed in a room used by the maintenance and janitorial personnel.

According to the State of Florida *General Records Schedule GS1-SL for State and Local Government Agencies*, MDPHA is required to retain clients' files as follows:

a. *Record copy*: 5 years after funds expended and accounted for and/or satisfaction of loans, whichever is later, provided applicable audits have been released.
b. *Duplicates*: until obsolete, superseded, or administrative value is lost.

We believe that client files that have been closed for over 12 to 20 years have lost their administrative values.

Recommendation
PHCD should comply with record retention policy, and securely destroy clients' records that have outlived their retention periods.

Management Response
PHCD concurs with this finding and responds to the recommendation as follows:

The report references two sites where clients' files were closed and maintained beyond their retention periods without being destroyed. Currently, PHCD has a decentralized organizational footprint, which complicates the ongoing effort to manage the retention schedules of thousands of files created at the site level. 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.

Finding 9
MDPHA did not have adequate computer and information security training and awareness program for members of its workforce *(Appendix I #P.4).*

MDPHA did not provide relevant awareness and training on computer and information security for majority of its workforce. The only employees in MDPHA that were provided certain level of such training were those employees (*less than 30% of department workforce)* that use the Enterprise Income Verification (EIV) system. EIV is owned and administered by the U.S. Department of Housing and Urban Development (HUD). HUD policy for the use of the system mandates users to have specific computer security training before they are granted access to the system. The remaining majority of MDPHA workforce did not receive computer security awareness and training.

Good security practice and relevant information security standards (including HIPAA of 1996, NIST SP800-53) require that security awareness and training program be established for members of the workforce. Without the necessary security training and awareness, members of staff will fall short in the knowledge and security consciousness required to protect sensitive and confidential information.

Recommendation
PHCD should establish 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 Response

PHCD concurs with this finding and responds to the recommendation as follows:

This finding was first discussed during a pre-exit meeting held on May 9, 2012 with Michael Bayere, Auditor-In-Charge. During the meeting, PHCD's Senior Human Resources Manager assured Mr. Bayere that we would identify the appropriate training resources and provide such training to all PHCD employees. The assignment was given to PHCD's Training coordinator, Juanita Brunson-Alonso, who was instructed to contact ITD for assistance in providing IT Security Training. Ms. Brunson-Alonso was advised by ITD that the Secure IT Training was available online and that taking the training was a mandatory requirement for all county employees. Ms. Brunson-Alonso then sent the training link by email to all PHCD employees advising that it was mandatory for all employees to take the training. Even though we have 165 employees in the department who are not assigned computers, we scheduled morning and afternoon training sessions of 3-hours each in our computer lab for a period of 3 weeks to ensure that all PHCD employees had access to the training. As of September 26, 2012, 332 of 454 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.

Attachment 1

Memorandum

MIAMI-DADE COUNTY

Date: September 26, 2012

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

From: Gregg Fortner, Executive Director
Public Housing and Community Development

Subject: Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information (Former Public Housing Agency)

We are in receipt of the Final Draft memorandum dated September 4, 2012, on the above referenced subject as issued by the Board of County Commissioners' Office of the Commission Auditor (OCA). This serves to provide Public Housing and Community Development's (PHCD) and Information Technology Department's (ITD) response to the reported findings and recommendations from that memorandum.

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. ITD should upgrade wireless local area network (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.

PHCD Response - PHCD concurs with this finding and responds to the recommendations as follows:

a. PHCD requested that ITD's Field Services Division provide an estimate for implementation of wireless security. ITD, working closely with PHCD completed the estimate as requested. An implementation plan will be created based on the assessment and estimate. Historically, network equipment located at departmental sites was purchased by departments, either as part of the initial deployment or purchased as needed to replace aging, unsupported equipment. Support and maintenance of the original equipment was provided by ITD. The purchase of replacement equipment as part of modernization or upgrade of the network was funded by departments and implemented by ITD. Recently, ITD adopted a new support model whereby aging network equipment is replaced with newer equipment providing additional functionality and security. The purchase, maintenance and recapitalization of the equipment is now included in a monthly "port charge" of $10.00/active port. A port is defined as the point where a network device (computer/server/printer) is connected to the County's network. The annual service charges include deployment, configuration, management and recapitalization/replacement of the network equipment. This updated business model ensures that each participating department's network will remain current, state of the art, supported and secure.
b. ITD will develop an effective risk assessment and control processes to continuously manage the risks of 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.

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 & tiles 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.

Actions taken by the department:

Subsequent to the audit fieldwork, the department corrected the inappropriate access privileges granted on the affected files and documents.

PHCD Response - PHCD concurs with this finding and responds to the recommendations as follows:

a. A file share permission was identified which allowed read permission (Users) 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 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.

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

OCA Recommendations:

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.

PHCD Response - PHCD concurs with this finding and responds to the recommendation as follows:

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.

ITD Response - ITD will investigate the implementation of secure, encrypted email and provide recommendations on implementation and costs by January 30, 2013.

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.

PHCD Response - PHCD concurs with this finding and responds to the recommendation as follows:

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.

Finding 5 - Policies and processes for managing computer users' passwords and accounts on department and County computing resources were weak.

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.

PHCD Response - Adequate procedures for user passwords and accounts are currently in place throughout the department. Additional details are included in the following response to the recommendations:

a. Domain Password policies have been developed which are aligned with information security best 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 signatures included. Our department's Personnel staff use workflows in our HRIS application to ensure that Technical Services Division is promptly notified to restrict access for departed or soon to depart employees.

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, 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.

PHCD Response - PHCD concurs with this finding and responds to the recommendations as follows:

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.

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

OCA Recommendation:

PHCD should establish 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.

PHCD Response - PHCD concurs with this finding and responds to the recommendation as follows:

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 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.

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

OCA Recommendation:

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

PHCD Response - PHCD concurs with this finding and responds to the recommendation as follows:

The report references two sites where clients' files were closed and maintained beyond their retention periods without being destroyed. Currently, PHCD has a decentralized organizational footprint, which complicates the ongoing effort to manage the retention schedules of thousands of files created at the site level. 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.

Finding 9 - MDPHA did not have adequate computer and information security training and awareness program for members of its workforce.

OCA Recommendation:

PHCD should establish computer and information security training and awareness program that provide 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 - PHCD concurs with this finding and responds to the recommendation as follows:

This finding was first discussed during a pre-exit meeting held on May 9, 2012 with Michael Bayere, Auditor-In-Charge. During the meeting, PHCD's Senior Human Resources Manager assured Mr. Bayere that we would identify the appropriate training resources and provide such training to all PHCD employees. The assignment was given to PHCD's Training coordinator, Juanita Brunson-Alonso, who was instructed to contact ITD for assistance in providing IT Security Training. Ms. Brunson-Alonso was advised by ITD that the Secure IT Training was available online and that taking the training was a mandatory requirement for all county employees. Ms. Brunson-Alonso then sent the training link by email to all PHCD employees advising that it was mandatory for all employees to take the training. Even though we have 165 employees in the department who are not assigned computers, we scheduled morning and afternoon training sessions of 3-hours each in our computer lab for a period of 3 weeks to ensure that all PHCD employees had access to the training. As of September 26, 2012, 332 of 454 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.

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.

cc: Russell Benford, Deputy Mayor, Office of the Mayor
Mari Saydal-Hamilton, Assistant Director, PHCD
Jose L. Rivero, Director, Technical Services Division, PHCD
Angel Petisco, Director, ITD
Lars Schmekel, Chief Security Officer, ITD