Internal Audit Report

**Miami-Dade County Public Schools**
**Office of Management and Compliance Audits**

# DISTRICT CENTRAL OFFICES NETWORK AND INFORMATION SECURITY

## OFFICE OF THE CONTROLLER

Adequate management of network resources and data security was generally observed; however, the audit identified certain areas where IT data security could be enhanced. Also, district-wide analysis and implementation of the recommendations should be considered.

March 2012

**THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA**

Ms. Perla Tabares Hantman, Chair
Dr. Lawrence S. Feldman, Vice Chair
Dr. Dorothy Bendross-Mindingall
Mr. Carlos L. Curbelo
Mr. Renier Diaz de la Portilla
Dr. Wilbert "Tee" Holloway
Dr. Martin Karp
Dr. Marta Pérez
Ms. Raquel A. Regalado

Mr. Alberto M. Carvalho
Superintendent of Schools

Mr. Jose F. Montes de Oca, CPA
Chief Auditor
Office of Management and Compliance Audits

**Contributors to This Report:**

Audit Performed by:
Mr. Luis O. Baluja

Audit Reviewed by:
Mr. Trevor L. Williams, CPA

Supervised by:
Mr. Trevor L. Williams, CPA

**Miami-Dade County Public Schools**
giving our students the world

***Superintendent of Schools***
*Alberto M. Carvalho*

***Chief Auditor***
*Jose F. Montes de Oca, CPA*

***Miami-Dade County School Board***
*Perla Tabares Hantman, Chair*
*Dr. Lawrence S. Feldman, Vice Chair*
*Dr. Dorothy Bendross-Mindingall*
*Carlos L. Curbelo*
*Renier Diaz de la Portilla*
*Dr. Wilbert "Tee" Holloway*
*Dr. Martin Karp*
*Dr. Marta Pérez*
*Raquel A. Regalado*

March 1, 2012

Members of the School Board of Miami-Dade County, Florida
Members of the School Board Audit and Budget Advisory Committee
Mr. Alberto M. Carvalho, Superintendent of Schools

Ladies and Gentlemen:

In accordance with the approved Audit Plan for the 2011-12 Fiscal Year, we have completed an Information Technology (IT) audit within the Office of the Controller and its direct reports (Payroll, Accounts Payable, and General Accounting) to assess network security and evaluate controls and standard mechanisms in place to protect critical systems and data.

This is the third in a series of reports that address information and network security practices at District offices.

Our audit concludes that while general measures for compliance with the Miami-Dade County Public Schools Network Security Standards are in place, increasing central office standardization efforts and proactive reviews could improve network availability and the security of business data.

Our findings and recommendations were discussed with management, whose responses and explanations are included herein. We would like to acknowledge the administration's positive, prompt and efficient response to our recommendations. We would also like to thank management for the cooperation and courtesies extended to our staff during the audit.

Sincerely,

José F. Montes de Oca

Jose Montes de Oca, CPA, Chief Auditor
Office of Management and Compliance Audits

## TABLE OF CONTENTS

Page



## FINDINGS AND RECOMMENDATIONS

## EXECUTIVE SUMMARY

The Office of the Controller (Controller) reports to the Chief Financial Officer (CFO) and is a component of the Financial Services bureau. Financial Services provides for the effective, efficient and timely management of the financial transactions of the district, including planning, estimating, and controlling revenues and expenditures, receiving and investing revenues. It is also involved in making payroll and vendor payments, conducting procurement activities and accounting for these transactions in an appropriate manner, in accordance with the standards of the Florida Department of Education (FDOE), and of the Government Accounting Standards Board (GASB). The business units of Payroll, General Accounting, and Accounts Payable report to the Controller's office. Together, these offices manage and use large amounts of financial data.

This is the third in a series of audits that are focused on assessing central office compliance with district policies, as described in the Miami-Dade County Public Schools (M-DCPS) Network Security Standards (NSS) document and industry best practices. This audit was conducted and reported according to direct reporting structure of the affected offices/departments.

The findings and corresponding recommendations presented in this report are intended to assist the district in protecting its business and employee data and the systems supporting these resources.

**OVERVIEW OF FINDINGS**

**High-priority and security updates for operating systems and some mainstream software products are significantly outdated.**

**Some servers performing critical functions are running unsupported operating systems.**

**Antivirus software installation and updating is inconsistent.**

**A centralized timeout policy has not been implemented for central office computers.**

**Reconciliation of computer accounts and management of organizational units within active directory is needed.**

*Some of the findings reported in this series of reports indicate that Information Technology (IT) concerns need to be explored and addressed district-wide. Specifically, the recommendations presented should not only be considered for implementation in the Controller's office, but should be used as a catalyst for all district central offices to assess their IT security status.*

Adequate management of network resources and data security was generally observed; however, the audit identified certain areas where IT data security could be enhanced. Based on our observations, we have made six (6) recommendations with detailed findings beginning on page 8.

## INTERNAL CONTROLS

The charts below summarize our overall assessment of network, data and systems security found at the four offices reviewed.

| INTERNAL CONTROLS RATING | | | |
|---|---|---|---|
| **CRITERIA** | **SATISFACTORY** | **NEEDS IMPROVEMENT** | **INADEQUATE** |
| **Process Controls** | **X** | | |
| **Policy & Procedures Compliance** | | **X** | |
| **Effect** | **X** | | |
| **Information Risk** | **X** | | |
| **External Risk** | | **X** | |

| INTERNAL CONTROLS LEGEND | | | |
|---|---|---|---|
| **CRITERIA** | **SATISFACTORY** | **NEEDS IMPROVEMENT** | **INADEQUATE** |
| **Process Controls** | **Effective** | **Opportunities exist to improve effectiveness.** | **Do not exist or are not reliable.** |
| **Policy & Procedures Compliance** | **In compliance** | **Non-Compliance Issues exist.** | **Non - compliance issues are pervasive, significant, or have severe consequences.** |
| **Effect** | **Not likely to impact operations or program outcomes.** | **Impact on outcomes contained.** | **Negative impact on outcomes.** |
| **Information Risk** | **Information systems are secure.** | **Data systems are mostly secure but can be improved.** | **Systems are vulnerable to unauthorized access, which may expose sensitive information.** |
| **External Risk** | **None or low.** | **Potential for damage.** | **Severe risk of damage.** |

## BACKGROUND

M-DCPS currently utilizes approximately 125,000 computers at over 400 different physical locations across an enterprise-level network. This large network connects students, teachers, administrators and parents with a vast amount of information and educational tools. Business transactions such as the procurement of goods and services as well as employee payroll are also processed on the District's network. These and many other critical district functions rely on the availability of a robust network with properly managed resources and equipment.

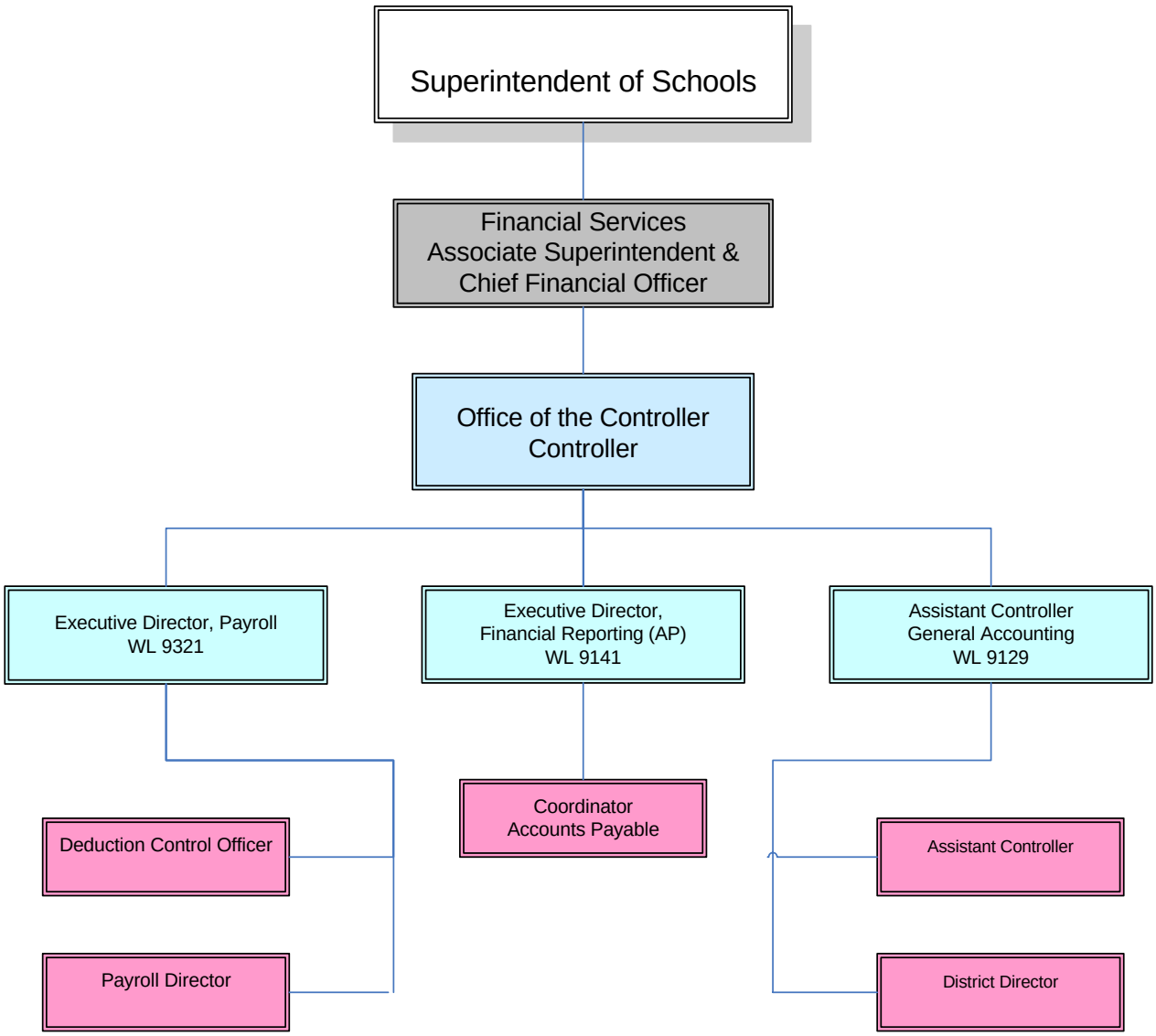
The IT function for the School Board Administration Building (SBAB) complex is maintained by the District's Information Technology Services department (ITS). Infrastructure and Systems Support (ISS) is a subdivision of ITS and is responsible for providing IT support. As such, the Controller's office does not have an exclusively dedicated technical staff. Instead, it is serviced by a team of highly experienced technicians who support the entire SBAB complex, staffed as follows:

| **SBAB Executive Support Team (EST)** | |
|---|---|
| **Title** | **Quantity** |
| Network Data Communication Specialist (**NDCS**) (1 Part-Time, 2 Full-Time) | 3 |
| Communications Support Technician (Telephone) | 1 |
| Network Analyst (**NA**, Administrator) | 1 |
| Project Manager (**PM**, Administrator) | 1 |
| **TOTAL** | **6** |

Technical staff provide routine technology support to the central offices at the SBAB complex, including help desk-related services, computer and equipment repair, and managing network resources such as printers, servers, software and data storage.

# Office of the Controller

Organizational Chart (WL 9151)



## TERMINOLOGY

Due to the unique terms contained and used in the IT vernacular, as well as the prolific use of acronyms when referring to technology, the following definitions are provided for the reader's reference*:*

| | |
|---|---|
| **AD** | Active Directory® (Microsoft® terminology) – A database of computer and user accounts. A central component of the Windows® platform, Active Directory provides the means to manage the identities and relationships that make up network environments. |
| **Tivoli** | Patch management and remote administration tool, which also provides condition reports of all computers that have connected to the network within the prior 30-day period. |
| **Group Policy** | A centralized method of applying restrictions or conditions to a group of users or computers (Microsoft® terminology). |
| **Local Administrator (LA)** | A special account, which allows a user to have control over the computer, including modifying the computer's profile. |
| **NSS** | M-DCPS Network Security Standards document that delineates security guidelines for M-DCPS. |
| **PC** | Personal computer or workstation. |
| **AV** | Enterprise-level antivirus (AV) software product in use on the M-DCPS network. |

## OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with the approved Audit Plan for FY 2011-2012, we have performed an audit of network data and systems security within the Office of the Controller and its direct reporting business units. The objectives of the audit were to determine whether adequate controls are in place to:

- Protect critical information;
- Protect supporting IT systems;
- Ensure adherence to the District's Network Security Standards (NSS); and
- Identify and apply industry best practices to the District's IT function.

The scope of this audit encompasses current practices and procedures used to maintain the IT function. We performed the following procedures to satisfy our audit objectives:

- Reviewed the District's NSS and other third party reports on IT best practices;
- Interviewed district staff identified in the organizational chart;
- Tested individual user desktop workstations for compliance with the standards stated in our audit objectives;
- Utilized software such as Active Directory®, Group Policy and other tools to mine for specific data;
- Reviewed required documentation related to District policies;
- Verified the installation and operation of required software; and
- Performed other audit procedures as deemed necessary.

We conducted this performance audit in accordance with generally accepted *Government Auditing Standards* issued by the Comptroller General of the United States of America. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

This audit included an assessment of applicable IT internal controls and compliance with the requirements of established policies, procedures and rules. Additionally, the findings and recommendations reflect general trends observed within the sample group reviewed rather than isolating individual issues.

Our determination of each location's compliance or non-compliance with established standards, as well as the resulting findings and recommendations were assessed utilizing the following criteria of audit concerns:

- Is the M-DCPS Network Security Standards being followed?
- Are generally recognized and accepted industry practices being employed?
- What tools are available for detecting undesirable conditions?
- How difficult or time consuming is it to look for or monitor deficiencies?
- How difficult or time consuming is it to implement corrective actions?
- What is the risk to the District associated with non-compliance?
- Is technical staff aware of policies and procedures?

In assessing compliance with the aforementioned areas of audit concerns, we applied our tests to installed, functional computers at the time of the audit.

Throughout this report, to the term "best practices" primarily refers to established practices that were recommended in the State of Florida Auditor General Report No. **2010-062 – *Summary Report of Information Technology Audit Findings***, December 2009. However, we also refer to other generally recognized "best or leading practices".

## FINDINGS AND RECOMMENDATIONS:

### 1. HIGH-PRIORITY/SECURITY UPDATES FOR OPERATING SYSTEMS (OS) AND SOME MAINSTREAM SOFTWARE PRODUCTS ARE SIGNIFICANTLY OUTDATED

Established Standards — Manufacturers generate updates to software in order to provide enhancements, repair deficiencies, and address vulnerabilities identified after the software's initial release. Failing to update software regularly with available updates may place the user's computer and network at risk. In addition, users may experience unnecessary problems that have been identified for which the manufacturer has provided a “fix” during the update process. These problems may also negatively impact efficiency. Most importantly, however, updates typically address critical security flaws that have been identified over time.

Observed Practice — Of the 65 computers tested, none had received any of the available operating system or mainstream software updates for several months. Software and OS updates are a function best handled without requiring user intervention.

**RECOMMENDATION:**

**1.1 ITS should configure the District’s patch management tool to automatically handle critical updates and conduct periodic reviews to confirm timely deployment.**

**RESPONSIBLE DEPARTMENT: Information Technology Services and Office of the Controller**

**MANAGEMENT’S RESPONSE:** ITS uses IBM's BigFix/Tivoli to push Operating System updates to District computers. When ITS contacted IBM about this audit exception, they replied that their product only updates our computers with those patches deemed necessary to provide security fixes. Not all patches released by Microsoft are considered security issues by IBM. When asked if it was possible for the District to designate which patches we wanted pushed, IBM replied in the negative. After discussion with OMCA staff, it was clear that the patches Microsoft call "security" and what IBM calls "security" are different. ITS will bring both IBM and Microsoft into a discussion to determine what is causing the disconnect.

In addition, we do not patch servers that we do not control automatically because of the

high probability that a patch will inadvertently break an application, especially at schools. If a large number of servers are affected by a patch at the same time, the District will suffer a major outage. Patching servers must be done manually by the server's administrator.

## 2. SOME SERVERS PERFORMING CRITICAL FUNCTIONS ARE RUNNING UNSUPPORTED OPERATING SYSTEM

Established Standards — An operating system (OS) is the foundation upon which all software functions and processing are performed. A computer is nearly useless without the OS, which controls and manages hardware, peripherals, and software resources. It is the "middle-man" between applications and hardware and serves as the interface for users. Over time, manufacturers typically replace an OS version in order to introduce new features and address security concerns that cannot be achieved through an update process for existing platforms.

Observed Practice — One of the offices audited has servers running critical processes on an unsupported OS platform. Support from the manufacturer for this OS version ended July 2010. Several other deficiencies, which are not detailed in this report for security reasons, were also noted.

**RECOMMENDATION:**

**2.1 The Office of the Controller should coordinate with ITS to either upgrade or virtualize the indicated servers to a version that is fully supported by the manufacturer as soon as possible.**

**RESPONSIBLE DEPARTMENT: Office of the Controller and Information Technology Services**

**MANAGEMENT'S RESPONSE:** Windows 2000 is no longer supported by Microsoft but the version of the imaging product present on these servers is unable to run on a newer OS. ITS has been working with the vendor that originally provided the imaging product used on these servers to get a new version of the software so that the servers can be upgraded to a newer OS release and be virtualized.

## 3. ANTIVIRUS (AV) SOFTWARE INSTALLATION AND UPDATING IS INCONSISTENT

Established Standards

Through memoranda from the Superintendent of Schools, school and non-school site administrators are notified of revisions to the M-DCPS Network Security Standards (NSS) and of the need to fully comply with district security initiatives in order to keep its network secure. According to the NSS sections 4.1.1.9, 5.0.19, 5.1.1.18 and industry recommended best practices, current antivirus software should be installed on all computers. AV software is a vital component needed to safeguard data and to protect M-DCPS business processes and confidential student/employee information from viruses and other malicious threats.

Observed Practice

Several conditions were noted on some of the computers reviewed:

- no AV installation
- two AV products installed simultaneously
- outdated AV definitions

The District is currently transitioning to a new AV product. Through our ongoing discussions with ITS, we were made aware that unanticipated problems with the automated removal of the previous AV and installation of the new AV product had been encountered. These technical or product-related issues are believed to be the cause for the conditions noted above concerning the computers we reviewed. Management is currently working to resolve the AV installation problems noted above with a final resolution pending.

Automated deployment significantly reduces labor and overhead that would otherwise be incurred with individual installation. Heavy reliance is placed exclusively on this method for AV installation. As such, it is imperative that these problems are resolved quickly.

**RECOMMENDATIONS:**

**3.1 The Office of the Controller should coordinate with ITS to provide technical support to remove of the previous AV versions, install the new AV software, and periodically update the AV definitions.**

**RESPONSIBLE DEPARTMENT: Office of the Controller and Information Technology Services**

**MANAGEMENT'S RESPONSE:** ITS concurs with this recommendation. Because of the issues the new AV application has had, ITS is currently pushing new AV definitions regularly to the District equipment through a different, more manual procedure. Once the difficulties documented in the narrative have been resolved, ITS will work with the Office of the Controller to ensure that all their machines have up-to-date AV engines and definitions, that they are maintained at that high level, and that old AV applications have been removed.

**3.2 ITS should continue to work with the AV vendors to resolve the conditions noted above. Until resolved, manual installation of AV should be performed on all new workstations deployed district-wide.**

**RESPONSIBLE DEPARTMENT: Information Technology Services**

**MANAGEMENT'S RESPONSE:** ITS concurs with this recommendation and is working with the AV vendor to resolve the difficulties. At this writing great strides have been made toward this end but we still must make sure that the product is able to scale to the approximately 130,000 computers the District must maintain.

## 4. A CENTRALIZED TIME-OUT POLICY FOR CENTRAL OFFICE COMPUTERS WOULD IMPROVE PROTECTION OF SENSITIVE DATA

Established Standards

Section 4.1.1.10 of the NSS reads, in pertinent part:

*"All administrative computers and server consoles that are used to access or control sensitive data must have a screen saver timeout and password after a specific period of inactivity or some other lockout mechanism to prevent unauthorized persons from accessing the data via the logged-in user's account. The Windows timeout with password is available even if the specific application does not have one."*

Sections 4.1.1.9 and 5.1.3 also describe the importance of locking portable devices.

Observed Practice

We examined 65 workstations in the areas audited in the Controller's Office and found that no centralized timeout policy was in place on any of the workstations. Although users can enable this policy on their own, our experience indicates that when left up to the user, implementation is generally ignored.

After authorized users logon to the M-DCPS network, many district functions, network resources, and confidential data are made accessible. Unsupervised and unlocked computers pose a threat to the integrity of district and student information. Furthermore, tampering would be difficult to detect and may go unnoticed since changes are accomplished while logged in as an authorized user.

**RECOMMENDATION:**

**4.1 Obtain assistance from ITS to implement a group policy that forces computers in the Controller's Office to automatically lock after a preset period of user inactivity, not to exceed 30 minutes.**

**RESPONSIBLE DEPARTMENT: Office of the Controller**

**MANAGEMENT'S RESPONSE:** ITS concurs with this finding but is trying to find a way to implement different timeout standards based on the sensitivity of the data accessed

by the user. A "one-size-fits-all" timeout policy is very difficult to implement in the district. ITS worked with the Council of Great City Schools (CGCS) to establish a baseline among large, urban districts but in the end was asked to make a recommendation to CGCS since the resulting survey showed that school districts around the country used wildly varying policies. It is clear a time-out may have to be implemented based on user need and on job responsibilities and position.

It is important to note that the Network Security Standards (NSS) also requires users to lock their computers when they walk away, and indeed this is the best and preferred method to protect user accounts and data, as a timeout does not take immediate effect. A way needs to be established to hold individual users accountable for their actions. A Weekly Briefing (#10003) was sent out to remind users of their responsibilities in this area.

## 5. RECONCILIATION OF COMPUTER ACCOUNTS WITHIN ACTIVE DIRECTORY IS NEEDED

Established Standards

The District utilizes a technology developed by the Microsoft Corporation called Active Directory® (AD). Simply put, AD is a database housing an account for every computer on the network. Over time, with the addition, removal and servicing of computers, AD becomes populated with "orphaned" accounts that are not associated with a "live" computer. This results in thousands of unused or "orphaned" accounts remaining in the database.

It is a leading practice that AD be reconciled, thereby improving performance and providing a true representation of the actual computer population. Knowing the true population of computers also enhances accountability and control over software licensing.

Observed Practice

Compared to the actual computer population and taking into account recent installations, the number of AD accounts exceeded the actual count by about 62%. AD should be reconciled with the existing computer population. Tools are available that can determine the length of time since last logon, providing a starting point for identifying inactive computer accounts for purging. Since technical staff at SBAB is directly involved with managing computers, they should be given the ability to manage AD accounts. Proper management of AD provides better organization and the ability to apply policies when needed.

**RECOMMENDATION:**

**5.1 Obtain assistance from ITS to reconcile the computer accounts in AD to the actual computer population and to establish a schedule for periodic reconciliation of same.**

**RESPONSIBLE DEPARTMENT: Information Technology Services**

**MANAGEMENT'S RESPONSE:** ITS agrees that maintaining and getting rid of old accounts does reduce the clutter when administrating AD, but should not be an auditable finding. It is not feasible to programmatically reconcile computer account objects in Active Directory. Computers may be taken offsite, or may be out of communication with Active Directory for a prolonged period of time. Earlier attempts at

deleting objects that were considered dormant caused many support tickets from the school sites. ITS uses Big Fix to account for computers and to manage endpoint equipment. Comparing Big Fix to the AD is an unnecessary extra step. Dormant computer accounts do not raise a security concern by simply existing, and do not affect the performance of the Active Directory.

**MANAGEMENT'S RESPONSE:**

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

**RHH:059**
**February 29, 2012**
**305-995-1225**

**TO:** Mr. Jose F. Montes de Oca, Chief Auditor
Office of Management and Compliance Audits

**FROM:** Richard H. Hinds, Associate Superintendent and Chief Financial Officer
Financial Services

**BY:** Connie Pou, Controller
Office of the Controller

**SUBJECT: RESPONSE TO THE INTERNAL AUDIT – NETWORK AND INFORMATION SECURITY; DISTRICT OFFICES – OFFICE OF THE CONTROLLER**

Following are the responses to the above mentioned audit report.

**1.1 Given that the Office of the Controller and ITS report to the CFO, the CFO should direct ITS to configure the District's patch management tool to automatically handle critical updates. Staff should conduct periodic reviews to confirm timely deployment.**

**Management Response:**

ITS uses IBM's BigFix/Tivoli to push Operating System updates to District computers. When ITS contacted IBM about this audit exception, they replied that their product only updates our computers with those patches deemed necessary to provide security fixes. Not all patches released by Microsoft are considered security issues by IBM. When asked if it was possible for the District to designate which patches we wanted pushed, IBM replied in the negative. After discussion with OMCA staff, it was clear that the patches Microsoft call "security" and what IBM calls "security" are different. ITS will bring both IBM and Microsoft into a discussion to determine what is causing the disconnect.

In addition, we do not patch servers that we do not control automatically because of the high probability that a patch will inadvertently break an application, especially at schools. If a large number of servers are affected by a patch at the same time, the District will suffer a major outage. Patching servers must be done manually by the server's administrator.

**2.1 The Office of the Controller should coordinate with ITS to either upgrade or virtualize the indicated servers to a version that is fully supported by the manufacturer as soon as possible.**

**Management Response:**

Windows 2000 is no longer supported by Microsoft but the version of the imaging product present on these servers is unable to run on a newer OS. ITS has been working with the vendor that originally provided the imaging product used on these servers to get a new version of the software so that the servers can be upgraded to a newer OS release and be virtualized.

**3.1 The Office of the Controller should coordinate with ITS to provide technical support to remove of the previous AV versions, install the new AV software, and periodically update the AV definitions.**

**Management Response:**

ITS concurs with this recommendation. Because of the issues the new AV application has had, ITS is currently pushing new AV definitions regularly to the District equipment through a different, more manual procedure. Once the difficulties documented in the narrative have been resolved, ITS will work with the Office of the Controller to ensure that all their machines have up-to-date AV engines and definitions, that they are maintained at that high level, and that old AV applications have been removed.

**3.2 ITS should continue to work with the AV vendors to resolve the conditions noted above. Until resolved, manual installation of AV should be performed on all new workstations deployed district-wide.**

**Management Response:**

ITS concurs with this recommendation and is working with the AV vendor to resolve the difficulties. At this writing great strides have been made toward this end but we still must make sure that the product is able to scale to the approximately 130,000 computers the District must maintain.

**4.1 Obtain the assistance from ITS to implement a group policy that forces computers in the Controller's Office to automatically lock after a preset period of user inactivity, not to exceed 30 minutes.**

**Management Response:**

ITS concurs with this finding but is trying to find a way to implement different timeout standards based on the sensitivity of the data accessed by the user. A "one-size-fits-all" timeout policy is very difficult to implement in the district. ITS worked with the Council of Great City Schools (CGCS) to establish a baseline among large, urban districts but in the end was asked to make a recommendation to CGCS since the resulting survey showed that school districts around the country used wildly varying policies. It is clear a time-out may have to be implemented based on user need and on job responsibilities and position.

It is important to note that the Network Security Standards (NSS) also requires users to lock their computers when they walk away, and indeed this is the best and preferred method to protect user accounts and data, as a timeout does not take immediate effect. A way needs to be established to hold individual users accountable for their actions. A Weekly Briefing (#10003) was sent out to remind users of their responsibilities in this area.

**5.1 Obtain the assistance from ITS to reconcile the computer accounts in AD to the actual computer population and to establish a schedule for periodic reconciliation of the same.**

**Management Response:**

ITS agrees that maintaining and getting rid of old accounts does reduce the clutter when administrating AD, but should not be an auditable finding. It is not feasible to programmatically reconcile computer account objects in Active Directory. Computers may be taken offsite, or may be out of communication with Active Directory for a prolonged period of time. Earlier attempts at deleting objects that were considered dormant caused many support tickets from the school sites. ITS uses Big Fix to account for computers and to manage endpoint equipment. Comparing Big Fix to the AD is an unnecessary extra step. Dormant computer accounts do not raise a security concern by simply existing, and do not affect the performance of the Active Directory.

## MIAMI-DADE COUNTY PUBLIC SCHOOLS ANTI-DISCRIMINATION POLICY

***Federal and State Laws***

The School Board of Miami-Dade County, Florida adheres to a policy of nondiscrimination in employment and educational programs/activities and strives affirmatively to provide equal opportunity for all as required by:

**Title VI of the Civil Rights Act of 1964** - prohibits discrimination on the basis of race, color, religion, or national origin.

**Title VII of the Civil Rights Act of 1964 as amended** - prohibits discrimination in employment on the basis of race, color, religion, gender, or national origin.

**Title IX of the Education Amendments of 1972** - prohibits discrimination on the basis of gender.

**Age Discrimination in Employment Act of 1967 (ADEA) as amended** - prohibits discrimination on the basis of age with respect to individuals who are at least 40.

**The Equal Pay Act of 1963 as amended** - prohibits gender discrimination in payment of wages to women and men performing substantially equal work in the same establishment.

**Section 504 of the Rehabilitation Act of 1973** - prohibits discrimination against the disabled.

**Americans with Disabilities Act of 1990 (ADA)** - prohibits discrimination against individuals with disabilities in employment, public service, public accommodations and telecommunications.

**The Family and Medical Leave Act of 1993 (FMLA)** - requires covered employers to provide up to 12 weeks of unpaid, job-protected leave to "eligible" employees for certain family and medical reasons.

**The Pregnancy Discrimination Act of 1978** - prohibits discrimination in employment on the basis of pregnancy, childbirth, or related medical conditions.

**Florida Educational Equity Act (FEEA)** - prohibits discrimination on the basis of race, gender, national origin, marital status, or handicap against a student or employee.

**Florida Civil Rights Act of 1992** - secures for all individuals within the state freedom from discrimination because of race, color, religion, sex, national origin, age, handicap, or marital status.

**Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA)** - Prohibits discrimination against employees or applicants because of genetic information.

*Veterans are provided re-employment rights in accordance with P.L. 93-508 (Federal Law) and Section 205.07 (Florida Statutes), which stipulate categorical preferences for employment.*

**In Addition:**

**School Board Policies 1362, 3362, 4362, and 5517** - Prohibit harassment and/or discrimination against students, employees, or applicants on the basis of sex, race, color, ethnic or national origin, religion, marital status, disability, genetic information, age, political beliefs, sexual orientation, gender, gender identification, social and family background, linguistic preference, pregnancy, and any other legally prohibited basis. Retaliation for engaging in a protected activity is also prohibited.

***Revised: (07-11)***

# INTERNAL AUDIT REPORT

## District Central Offices Network and Information Security

## Office of the Controller

**MIAMI-DADE COUNTY PUBLIC SCHOOLS**
**Office of Management and Compliance Audits**
**1450 N.E. 2nd Avenue, Room 415**
**Miami, Florida 33132**
Telephone: (305)995-1318 ♦ Fax: (305)995-1331
http://mca.dadeschools.net