Internal Audit Report

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

NETWORK AND INFORMATION SECURITY INFORMATION TECHNOLOGY SERVICES INFRASTRUCTURE AND SYSTEMS SUPPORT AREA II – SELECTED SCHOOL SITES

In general, measured improvements in the management of network resources and data security was observed. Still, opportunity to improve network security and availability exists.

September 2011

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 Baluja
Ms. Dina Pearlman, CISA, CIA

Audit Reviewed by:
Ms. Teresita M. Rodriguez, CPA
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

September 15, 2011

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 2010-11 Fiscal Year, we have completed an Information Technology (IT) audit at various schools within Information Technology Services (ITS) Infrastructure and Systems Support (ISS) Area II to assess network security and evaluate the mechanisms in place at those schools to protect critical systems and data.

This is the fourth in a series of reports that address information and network security practices at school sites. This report covers 20 of the 48 schools located within Area II. An assessment of the remaining 28 schools within Area II will be reported on at a future date.

Our audit concludes that while general measures for compliance with the Miami-Dade County Public Schools Network Security Standards are in place within this support area, increasing district-wide standardization efforts as well as oversight of school-based technology support staff could improve network availability and the security of student, personnel, and business data. Because the audit fieldwork for multiple ITS regions have been performed concurrently, similar exceptions have been reported across various regions. We realize that certain trends will likely exist during the early stage of schools migrating their IT resources from a semi-autonomous platform to the present enterprise platform. With that said, it is important to note that marked improvement is emerging due to management's commitment towards a secure District network.

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

- EXECUTIVE SUMMARY 1
- INTERNAL CONTROLS 2
- BACKGROUND 3
- PARTIAL ORGANIZATIONAL CHART..... 4
- TERMINOLOGY 5
- OBJECTIVES, SCOPE AND METHODOLOGY..... 6

FINDINGS AND RECOMMENDATIONS

1 Periodic Reconciliation of Computer Accounts in Active Directory and BigFix is Needed 8

2 Antivirus Software Needs to be Installed on All Computers..... 10

3 A Centralized Timeout Policy for Administrative Computers and Server Consoles Would Enhance Protection of Sensitive Data 12

MANAGEMENT'S RESPONSE..... 14

EXECUTIVE SUMMARY

The Miami-Dade County Public Schools (M-DCPS) system comprises over 350 schools, which principal business is to educate students in a safe environment. In carrying out this mission, each school executes and manages various business processes, transactions and data across the District's network infrastructure. Both the large number of school sites and their sprawling placement throughout the county make keeping network resources available at all times a significant undertaking for the District's IT department.

OVERVIEW OF FINDINGS

School site Active Directory (AD) computer accounts should be reconciled to BigFix. Ten of the 20 locations reviewed (50%) had not reconciled AD.

Eighteen of the 20 schools reviewed (90%) had multiple computers that did not have the required up-to-date antivirus software installed.

Timeouts with password protection after authorized logon and user inactivity should be enabled utilizing a centralized policy to protect critical computers.

This is the fourth in a series of audits that are focused on assessing each school's compliance with the District's policies as described in the M-DCPS Network Security Standards (NSS) document and industry best practices. The audits are conducted and reported according to functional regions within the District's Information Technology Services (ITS) department. Because the audit fieldwork for multiple ITS regions have been performed concurrently, similar exceptions have been reported across various regions. We realize that certain trends will likely exist during the early stage of schools migrating their IT resources from a semi-autonomous platform to the present enterprise platform. However, management's awareness of the reported trend of audit exceptions and their responsiveness in addressing the findings should result in greater compliance with the above-stated standards.

The findings and corresponding recommendations presented in this report are intended to assist the District in protecting its student, business and employee data and the systems supporting these resources. The findings reported in this series of reports indicate that IT concerns need to be explored and addressed district-wide.

Notwithstanding our findings, adequate management of network resources and data security was generally observed. However, certain trends identified during the course of this audit disclosed areas that can greatly benefit from additional standardization across the network and increased oversight of school-based technology support staff. Based on our observations, we have made three 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 20 schools located within ISS Support Area II. An assessment of the remaining 28 schools within this area will be reported at a future date.

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. For example, student grades and attendance are reported via an electronic grade book system. Business transactions such as the procurement of goods and services as well as employee payroll are also processed on the District's network. Webinars, which allow principals to participate in important district meetings without having to leave the school campus where they are most needed, are accessed through the network. Parents and students can review student progress using the District's portals. These and many other extremely critical district functions rely on the availability of a robust network with properly managed resources and equipment.

Technical Support Technicians (TSTs)[1] are the primary source of technical support at each school site. On June 17, 2009, the School Board of Miami-Dade County approved agenda item D-26, which realigned the reporting structure for TSTs from the school-site administrator (i.e., principal) to a more centralized model under ITS. Under this model, technicians typically are assigned one or more schools and provide assistance to other nearby schools if needed.

Infrastructure and Systems Support (ISS) is a subdivision of ITS and is responsible for managing technicians and providing all school site IT support. ISS has created six support areas, each maintained by a technical team that serves an average of about 60 schools. ISS Support Area II (48 schools) is staffed as follows:

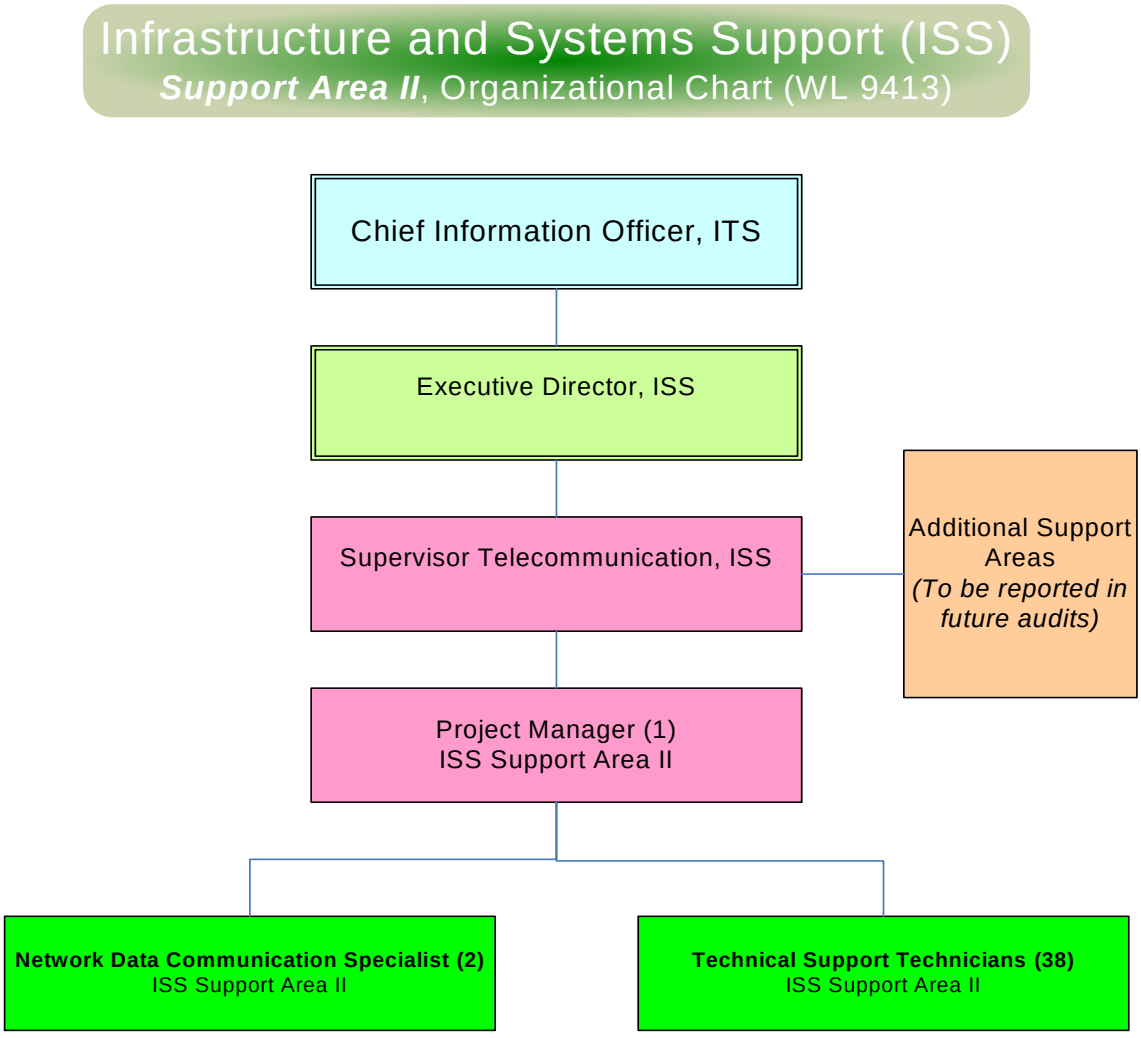
ISS Support Area II (as of May 2011)	
Title	**Quantity**
Technical Support Technician (**TST**): • Microsystems Technician (**MST**) • Computer Specialist (**CS**) • Computer Technician (**CT**)	38
Network Data Communication Specialist (**NDCS**)	2
Network Analyst (**NA**, Administrator)	0
Project Manager (**PM**, Administrator)	1
TOTAL	**41**

TSTs typically provide routine technology support at schools, including help desk related services, computer and equipment repair, and the managing of network

[1] Formerly known as School-Based Technicians or SBT.

resources such as printers, servers, software and data storage. Other issues, such as infrastructure and equipment problems that cannot be handled by the on-site technician are escalated to NDCS staff. TSTs and NDCS report to a Project Manager.

PARTIAL ORGANIZATIONAL CHART



During the course of this audit, at its meeting of April 13, 2011, the School Board approved Agenda Item D-25, which among other actions, implemented a Reduction-In-Force/Layoff of all TSTs (approximately 280). The item also provides for rehiring approximately 200 employees from the same pool of technicians as Temporary Network Infrastructure Support Technician (NIST). These NISTs will follow an 11.5-month work schedule. This reorganization should result in increased IT support services for schools beginning with the 2011-2012 fiscal year.

TERMINOLOGY

Due to the sometimes unfamiliar nature of the issues being discussed 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 the network environments.
BIGFIX	Patch management and remote administration tool, which also provides condition reports of all computers that have connected to the network within the prior 30 days.
DOMAIN	A collective group of computers, which are all members of the same "family".
Group Policy	Centralized method of applying restrictions or conditions to a group of users or computers (Microsoft ® terminology).
IP Address	Internet Protocol or IP address is a unique number assigned to a computer that enables it to access network resources.
Local Administrator	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.
Server	Central repository, which stores and shares data on a network.
SOPHOS	The enterprise-level antivirus (AV) software product in use by the M-DCPS.
IPS (Tipping Point)	Network intrusion prevention device.
WAP	Wireless Access Point – used for wireless network communications.

OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with the approved Audit Plan for FY 2010-2011, we have performed an audit of network data and systems security at 20 of the 48 schools located within ISS Support Area II. 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 followed by the selected schools within ISS Support Area II.

We performed the following procedures to satisfy our audit objectives:

- Analyzed site assessments of each school submitted by ISS Project Managers with input from TSTs, NDCS staff, and other data, and selected a sample of schools for examination;
- Reviewed the District's NSS and other third party reports on IT best practices;
- Interviewed district staff identified in the organizational chart;
- Utilized software such as Active Directory, BigFix, Group Policy and other tools to mine for specific data;
- Reviewed required documentation related to district policies, personnel and network layouts;
- Examined and tested a random sample of servers and desktop computers at each location for compliance with the standards stated in our audit objectives;
- Verified the installation and operation of required and optional equipment;
- Inspected physical storage facilities where servers are housed; 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 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 school issues.

Our determination of each school's compliance or non-compliance with established standards, as well as the resulting findings and recommendations were assessed utilizing the following criteria applied to 19 areas of audit concerns:

- Is the M-DCPS Network Security Standards being followed?
- Are industry best 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 19 areas of audit concerns, we applied our audit tests to either administrative and faculty computers only or to all (i.e., student, faculty and administrative) computers based on the applicability of each audit concern tested.

Throughout this report, references to 'best practices' primarily refer 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. PERIODIC RECONCILIATION OF COMPUTER ACCOUNTS IN ACTIVE DIRECTORY AND BIGFIX 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.

BigFix is a software tool that has been deployed to all district computers. It periodically reports to a central database and closely matches the actual number of "live" computers. TSTs have access to BigFix reports, which can be used to reconcile AD.

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

Observed Practice

At 10 of the 20 schools reviewed (or 50%), significant differences exist between the number of computers recognized in AD and those recognized in BigFix. For the 20 schools combined, the AD computer count totaled 11,425 versus 9,663 in BigFix.

According to the Auditee, differences in the computer library counts were due to a number of factors, including computers being added or removed from the network, hardware conflict, corrupt software and time lag between the completion of certain actions and the scheduled BigFix update. Periodically running the appropriate AD and BigFix routines will identify these conditions and aid in reconciling computer accounts.

RECOMMENDATION:

1.1 Require TSTs to run the appropriate AD and BigFix routines and reports on a regular basis, and to reconcile their location(s) AD using BigFix as a baseline.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this finding. In researching this issue, the following are some of the reasons we found to account for more AD counts than BigFix counts:

- Computers with corrupted BigFix and/or Sophos clients do not appear on BigFix counts.
- Computers pending repair and/or service still appear in AD counts.
- There are always new computers' deployment and imaging in progress which may be included in one count and not the other.
- Wireless labs and off-site loaner devices are not being actively used when BigFix reports run and thus not included.

ITS Standards Implemented to resolve the findings:

- Require NISTs to run monthly BigFix and AD reports in order to analyze and reconcile reports and fix any corrupted clients, with the goal of less than a 10% difference.
- Require NISTs to document the reasons for the differences and make this document available to ITS and auditors on request.
- Require NITSTs to run any unused wireless labs every few months, in order to ensure that wireless devices receive their update in a timely fashion and are included in the BigFix counts.
- Require that all M-DCPS off-site devices be brought in once a month to connect to the network for updates.
- ITS will perform random audits to verify that standards and procedures are being followed.
- ITS will continue to hold monthly Operations Review Meetings with all NISTs to provide current information and remind NISTs to follow all District policies.

2. ANTIVIRUS SOFTWARE NEEDS TO BE INSTALLED ON ALL COMPUTERS

Established Standards

Through memoranda from the Superintendent of Schools, all 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 all district security initiatives in order to keep its network secure. According to the NSS sections 4.1.1.9, 4.3.3, 5.0.8 and 5.17 and industry recommended best practices, antivirus (AV) software should be installed on all computers.

Observed Practice

Eighteen of the 20 schools reviewed (90%) had multiple computers that did not have the required up-to-date AV software installed. We realize that 100% compliance at all schools is difficult to achieve; however, the number of instances of non-compliance appears to indicate a condition that affects a number of schools within ITS ISS Area II. Moreover, tools are readily available to detect and rectify this condition.

The District utilizes an AV solution called SOPHOS. 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. AV software is automatically deployed on the network via BigFix. This method of deployment significantly reduces labor and overhead that would otherwise be incurred with individual installation. Many TSTs rely exclusively on this method for AV installation.

TSTs have access to reports, which quickly identify PCs that are missing or indicating a problem with their AV software. This report allows technicians to pinpoint and address AV software issues efficiently and keep vulnerability to a minimum by ensuring all computers are protected. However, staff at ITS has identified several instances where SOPHOS has reported an unexpected number of computers as not being a Sophos client. Based on data ITS staff has collected,

they have estimated that amount to be between 5% and 10% of the District's computer population. ITS staff has identified possible reasons for the noted condition, and has been working with the SOPHOS vendor to resolve the issues. However, the vendor has not been able to provide solutions to all of the issues encountered.

RECOMMENDATION:

2.1 TSTs should be required to routinely review BigFix AV reports for all assigned locations to proactively address AV deficiencies.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this finding. In researching the issue, we did not find any school computer that did not have the required AV software installed. Only a few computers at some schools had corrupted BigFix and/or Sophos clients which prevented them from receiving the latest AV updates. These corrupted machines are re-imaged or manually corrected as detected in an on-going corrective process.

ITS Standards Implemented to resolve findings:

- Require NISTs will run monthly AV Reports utilizing BigFix.
- ITS will recommend implementing Window Server Update Services (WSUS) as a backup to BigFix.
- ITS will perform random audits to verify that standards and procedures are being followed.

3. A CENTRALIZED TIMEOUT POLICY FOR ADMINISTRATIVE COMPUTERS AND SERVER CONSOLES WOULD ENHANCE 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 locking devices.

Observed Practice

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 significant threat to the integrity of district and student information.

We examined a sample of critical workstations (teacher, server, administrative) and found that at 7 of the 20 schools visited (35%), timeouts with password protection after authorized logon had not been enabled, leaving those unprotected computers vulnerable to tampering. This function is being left to the discretion of individual users. Our experience indicates that when left up to the user, implementation of this setting is generally ignored. Furthermore, tampering would be difficult to detect and may go unnoticed since changes are accomplished while logged in as an authorized user.

RECOMMENDATION:

3.1 Require TSTs to implement a group policy that forces sensitive computers (teacher, server and administrative workstations) to automatically lock after

a preset period of user inactivity. The preset period may vary by user/group depending on the sensitivity of the data on each system; however, it should not exceed 15 minutes.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this finding. Although the time-out policy has been included in the Group Policy Orchestrator (GPO) it has not been fully accepted by all users. As a result, ITS has attended several seminars and Webinars regarding security, but ITS is not aware of any industry standards in the field of education. ITS is working with the Council of Great City Schools (CGCS) to establish a baseline among large, urban districts to see M-DCPS' standing. This issue requires the input and buy-in of several departments, and as a result the fifteen minute time-out may have to be implemented based on user need. ITS is scheduling a meeting with several departments in an effort to develop a time-out analysis, based on job responsibilities and position. It is important to note that the Network Security Standards requires that users lock their computers when they walk away, and indeed this is the best way to protect the data, as a time-out does not take immediate effect. The District needs to establish a process to hold individual users accountable for their actions; the recent Weekly Briefing (#10003) reminded users of their responsibilities in this area.

ITS Standards Implemented to resolved findings:

- The NISTs must reboot all servers on a schedule in order for all policies to take effect.
- Implement Group Policy Orchestrator to lock and/or log off the user after a set time on non-active session.
- ITS will schedule meeting with affected departments and will provide a recommendation.

MANAGEMENT'S RESPONSE

MEMORANDUM

September 14, 2011
DK #002/2011-2012

TO: José Montes-de-Oca, Chief Auditor
Office of Management and Compliance Audits

FROM: Debbie Karcher, Chief Information Officer
Information Technology Services DCK

SUBJECT: **RESPONSE TO OMCA DRAFT OF INFRASTRUCTURE AND SYSTEMS SUPPORT (ISS) AREA II, SELECTED SCHOOL SITES FIELD AUDIT**

Below are the Information Technology Services (ITS) responses to the three items on the Infrastructure and Systems Support (ISS) AREA II, Selected School Sites Field Audit. It should be noted that it is very difficult to maintain a one hundred percent, secured technology environment in classrooms, especially considering that student users are very technologically savvy and often actively try to evade security efforts. In addition, there are over 125,000 District-owned computers connected to the network, with many more personally-owned devices coming constantly online and challenging M-DCPS' security processes. The local computers' protective applications are merely the first line of defense in a many-layered approach to security. Through the District's Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), computers that are breeched are quickly identified, isolated, shut down, and scheduled for cleaning; thus, protecting the rest of the network.

Additionally, please note that this audit was the fourth set of audits, in a series of four school area audits. The previous three sets of school audits, which included Area I, Area III, and Area V, each listed a minimum of seven exceptions. Area II Schools' Audit listed three exceptions which can be explained by the reorganization of Network Infrastructure Support Technicians (NISTs) and ITS' continuous effort to standardize technology at all schools.

ITS and the NISTs strive to maintain technological environments that are one hundred percent secure. As the number of computers and technology continue to grow in our schools, ITS is developing more programmatic and automated strategies to address differences between apparent and real discrepancies. ITS realizes that physical inspections in order to maintain compliance are not always possible. To facilitate compliance, ITS has also requested to see and sign off on the Field Audit Worksheets, as agreed by both departments, since some discrepancies have been identified.

Since the beginning of the school-based "Field Audits," ITS has incorporated monthly meetings with all NISTs, where procedures and standards are reviewed. As you know, since several members of Management and Compliance Audit were invited to a meeting and attended, these ***Operations Review Meetings*** keep all NISTs updated on technology standards and changes, including audit and security procedures.

RECOMMENDATIONS:

1.1 Require TSTs to run the appropriate AD and BigFix routines and reports on a regular basis, and to reconcile their location(s) AD using BigFix as a baseline.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Reconcile school site active directory computer accounts.

ITS Audit Response:

- ITS concurs with this finding. In researching this issue, the following are some of the reasons we found to account for more AD counts than BigFix counts:
  - Computers with corrupted BigFix and/or Sophos clients do not appear on BigFix counts.
  - Computers pending repair and/or service still appear in AD counts.
  - There are always new computers' deployment and imaging in progress which may be included in one count and not the other.
  - Wireless labs and off-site loaner devices are not being actively used when BigFix reports run and thus not included.

ITS Standards Implemented to resolve the findings:

- Require NISTs to run monthly BigFix and AD reports in order to analyze and reconcile reports and fix any corrupted clients, with the goal of less than a 10% difference.
- Require NISTs to document the reasons for the differences and make this document available to ITS and auditors on request.
- Require NITSTs to run any unused wireless labs every few months, in order to ensure that wireless devices receive their update in a timely fashion and are included in the BigFix counts.

- Require that all M-DCPS off-site devices be brought in once a month to connect to the network for updates.
- ITS will perform random audits to verify that standards and procedures are being followed.
- ITS will continue to hold monthly Operations Review Meetings with all NISTs to provide current information and remind NISTs to follow all District policies.

2.1 TSTs should be required to routinely review BigFix AV reports for all assigned locations to proactively address AV deficiencies.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Antivirus software needs to be installed on all computers.

Audit Response:

- ITS concurs with this finding. In researching the issue, we did not find any school computer that did not have the required AV software installed. Only a few computers at some schools had corrupted BigFix and/or Sophos clients which prevented them from receiving the latest AV updates. These corrupted machines are re-imaged or manually corrected as detected in an on-going corrective process.

ITS Standards Implemented to resolve findings:

- Require NISTs will run monthly AV Reports utilizing BigFix.
- ITS will recommend implementing Window Server Update Services (WSUS) as a backup to BigFix.
- ITS will perform random audits to verify that standards and procedures are being followed.

3.1 Require TSTs to implement a group policy that forces sensitive computers (teachers, server and administrative workstations) to automatically lock after a preset period of user inactivity. The preset period may vary by user/group depending on the sensitivity of the data on each system, not to exceed 15 minutes.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Computers needs to be password-protected after user login

Audit Response:

- ITS concurs with this finding. Although the time-out policy has been included in the Group Policy Orchestrator (GPO) it has not been fully accepted by all users. As a result, ITS has attended several seminars and Webinars regarding security, but ITS is not aware of any industry standards in the field of education. ITS is working with the Council of Great City Schools (CGCS) to establish a baseline among large, urban districts to see M-DCPS' standing. This issue requires the input and buy-in of several departments, and as a result the fifteen minute time-out may have to be implemented based on user need. ITS is scheduling a meeting with several departments in an effort to develop a time-out analysis, based on job responsibilities and position. It is important to note that the Network Security Standards requires that users lock their computers when they walk away, and indeed this is the best way to protect the data, as a time-out does not take immediate effect. The District needs to establish a process to hold individual users accountable for their actions; the recent Weekly Briefing (#10003) reminded users of their responsibilities in this area.

ITS Standards Implemented to resolved findings:

- The NISTs must reboot all servers on a schedule in order for all policies to take effect.
- Implement Group Policy Orchestrator to lock and/or log off the user after a set time on non-active session.
- ITS will schedule meeting with affected departments and will provide a recommendation.

DK:jp

cc: Dr. Richard Hinds
Mr. Trevor Williams
Mr. Javier Pérez
Mr. James O'Donnell

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

Network and Information Security
Information Technology Services
Infrastructure and Systems Support Area II:
Selected School Sites

MIAMI-DADE COUNTY PUBLIC SCHOOLS
Office of Management and Compliance Audits
1450 N.E. 2nd Avenue, Room 415
Miami, Florida 33132