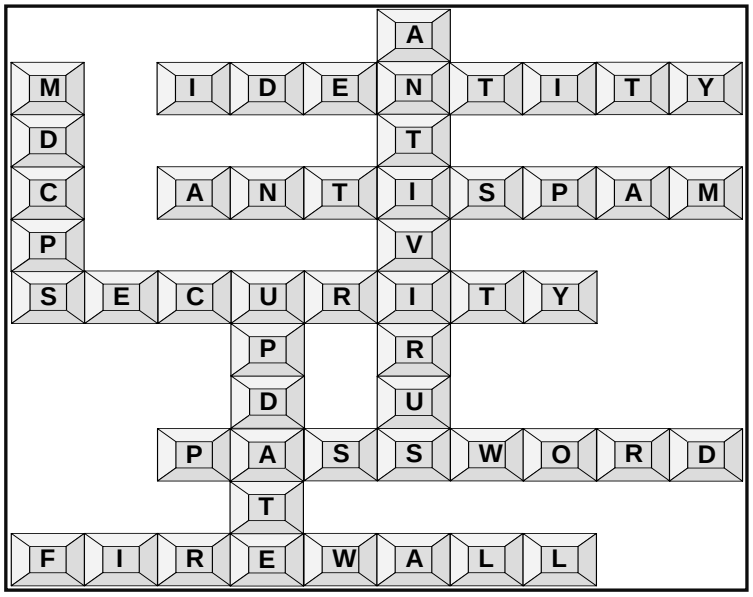
Internal Audit Report

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

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



Increased adherence to the M-DCPS Network Security Standards and oversight of technical staff can improve network security and availability.

March 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:
Mr. Trevor L. Williams, CPA

Supervised by:
Mr. Trevor L. Williams, CPA

Miami-Dade County Public Schools
giving our students the world

March 24, 2011

Members of the School Board of Miami-Dade County, Florida
Members of the School Board Audit 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 audit at various schools aligned within Information Technology Services (ITS) Infrastructure and Systems Support (ISS) Area III to assess network security and to evaluate the mechanisms in place at those schools to protect critical systems and data.

This report covers 21 of the 58 schools that are under the auspices of ITS ISS Area III. An assessment of the remaining 37 schools within ITS ISS Area III 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 at the schools serviced in 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.

Our findings and recommendations were discussed with management. Management's responses along with 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

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.

Our audit objectives focused on assessing each school's compliance with the District's policies as described in the M-DCPS Network Security Standards (NSS) document and with industry best practices.

The increase in potential risk of exposure and the vulnerability of data in today's environment make it incumbent upon the District to be increasingly proactive in protecting its student, business and employee data and the systems supporting these processes. The findings and corresponding recommendations presented in this report are intended to assist the District in protecting these resources.

Our findings indicate that adequate management of network resources is generally taking place. However, certain trends identified during the course of this audit disclosed areas that can greatly benefit from additional standardization across the M-DCPS network, as well as increased oversight of school-based technology support staff. There were other less critical matters discussed with management that are not reported herein.

OVERVIEW OF FINDINGS

- **Administrator's awareness of the M-DCPS NSS and the need to migrate all computers to the DADESCHOOLS domain and to ensure that critical software updates are installed on these machines are evident.**
- **School site Active Directory computer accounts should be reconciled to BixFix. Some are not.**
- **Antivirus software should be installed on all computers. Some computers did not have this tools installed.**
- **Computers should be password-protected after user logon. Some are not.**
- **Non-standard local administrator accounts are found throughout some school networks.**
- **Although some documentation that is typical for a disaster recovery plan was maintained, routine backups of servers was not being done at some schools.**
- **Review for the presence of unauthorized wireless access points needs to be consistently performed and documented.**

Based on our observations, we have made seven (7) recommendations. Our detailed findings begin on page 9. We would like to thank the administration for their cooperation and courtesies extended to our staff during the audits.

INTERNAL CONTROLS

The charts below summarize our overall assessment of network, data and systems security found at the 21 schools reported on herein that are under the auspices of ISS Support Area III. An assessment of the remaining 37 schools within ISS Support Area III will be reported on 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 instance, student's grades and attendance are reported via an electronic grade book system. Business transactions such as procurement of goods and services and employee payroll are also processed on the District's network. Webinars, which allow Principals to attend 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's 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.

School-Based Technicians (SBT's) or Technical Support Technicians (TST), (hereinafter referred to as SBTs) 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 SBTs 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 also provide assistance to other nearby schools, as 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 serve about 55-60 schools. ISS Support Area III (58 schools) is staffed as follows:

ISS Support Area III **(February 2011)**	
Title	**Quantity**
School Based Technician (**SBT**): • Microsystems Technician (**MST**) • Computer Specialist (**CS**) • Computer Technician (**CT**)	46
Network Data Communication Specialist (**NDCS**)	2
Network Analyst (**NA**, Administrator)	1
Project Manager (**PM**, Administrator)	1
TOTAL	**50**

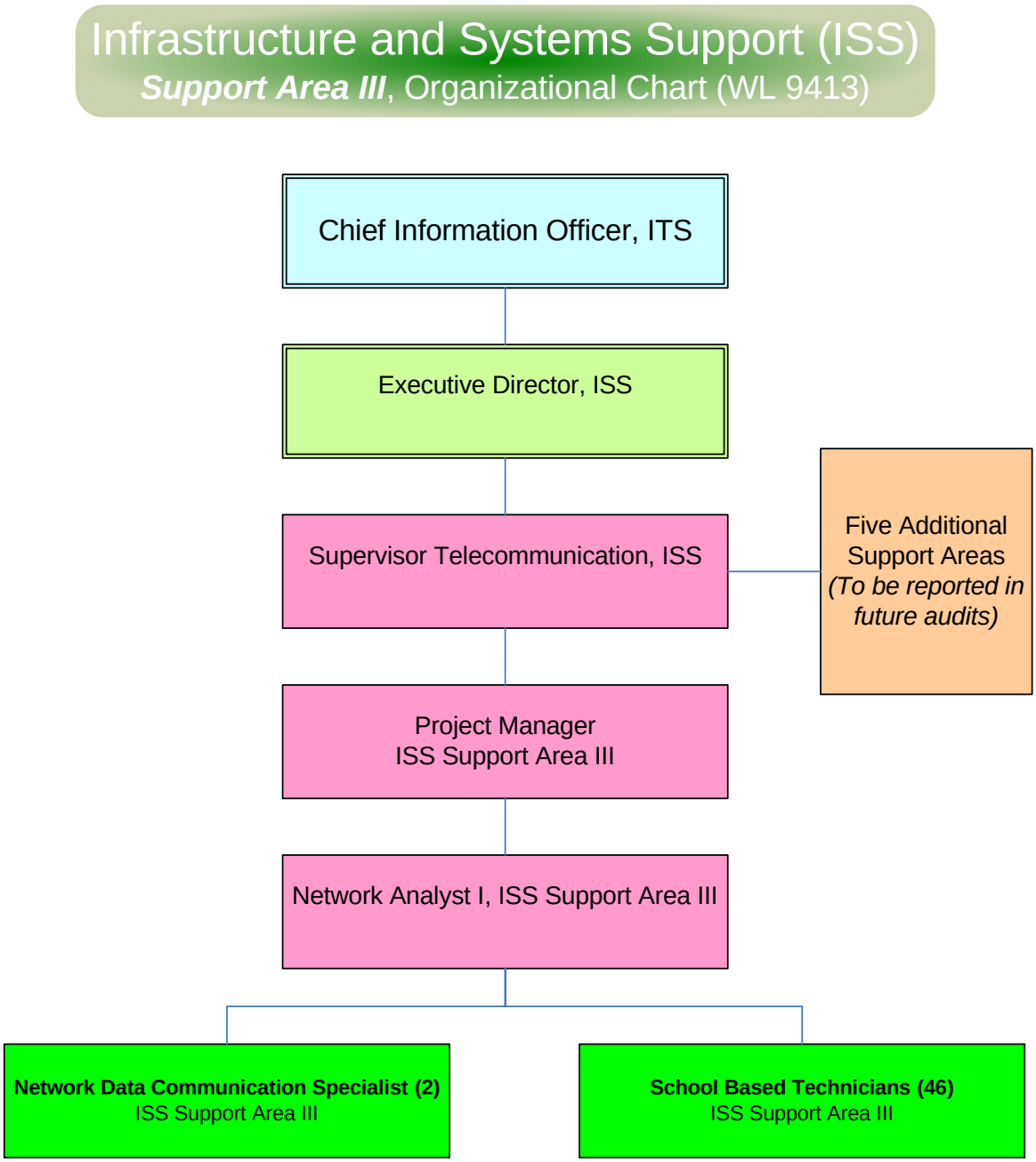
School Based Technicians typically provide routine technology support at schools, including help desk related services, computer and equipment repair, and the managing of network resources such as printers, servers, software and data storage. Other issues, such as infrastructure equipment problems that cannot be handled by the on-site technician are escalated to NDCS staff. SBTs and NDCS report to a Project Manager through a Network Analyst.

It should be noted that prior to the realignment described above, SBTs were classified as 12-month employees. SBTs now follow a 10-month work schedule similar to most school site personnel. Consequently, IT support resources have diminished significantly and have been compounded by a steady exodus of school site technical staff leaving the M-DCPS workforce.

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 network environments.
BIGFIX	Patch management and remote administration tool, which also provides condition reports of all computers that have connected to the DADESCHOOLS 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.
Tipping Point	Network intrusion prevention device.
WAP	Wireless Access Point

ORGANIZATIONAL CHART



OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with the approved Audit Plan for the 2010-11 Fiscal Year, we have performed an audit of network data and systems security at 21 (or 36%) of the 58 schools located within ISS Support Area III. 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 schools within ISS Support Area III.

We performed the following procedures to satisfy our audit objectives:

- Analyzed site assessments of each school submitted by ISS Project Managers with input from SBTs, NDCS and NA staff, and other data, and selected a sample of schools for review;
- Interviewed District staff identified in the organizational chart;
- Utilized software such as Active Directory, BigFix 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. 2007-005 – ***Selected State Agencies' Progress in Assessing Network and System Vulnerabilities****, Information Technology Audit*, July 2006.

FINDINGS AND RECOMMENDATIONS:

1. RECONCILE SCHOOL SITE ACTIVE DIRECTORY COMPUTER ACCOUNTS

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 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. SBTs 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 enhances accountability and control over software licenses.

Observed Practice

Our audit established that 11 of the 21 locations (or 52%) reviewed have not reconciled AD. The range of the delta for the number of computers in the AD library versus the BigFix library was from a low of 12 computers (16%) to a high of 708 computers (59%).

RECOMMENDATION:

1.1 Require all SBTs to reconcile their location(s) AD on a regular basis using BigFix as a baseline.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Procedure to correct the issue:
We instructed our Technical Support Technicians (TST) to reconcile the Organizational Units (OU) with BigFix by comparing the number of accounts between Bigfix and Active Directory and verifying they are equal. If the tech is unable to locate the machines identified in the Active directory Reports, they are instructed to delete and remove these old computer account entries from Active Directory. The deletion of these accounts will take approximately 30 days before Active Directory reconciles with the Dadeschools domain. In addition it takes 30 days for the above changes to appear in Bigfix Reports.

Policy Implemented for Future Prevention of this issue:
We have already implemented a monthly procedure instructing all TST to compare and verify the BigFix Report to Active Directory for equal number of accounts. All TST's are now required to delete and remove all unused computer accounts as identified in the BigFix report. In addition, ITS field support staff will randomly select sites throughout the Region and verify BigFix numbers with Active Directory.

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 and standards, in order to keep its network secure. According to the M-DCPS NSS 4.1.1.9, 5.0.8 and 5.0.17 and industry recommended best practices, antivirus (AV) software should be installed on all computers.

Observed Practice

Our review showed that all 21 schools audited maintained evidence of their employee's awareness of the M-DCPS NSS. Furthermore, all 21 schools audited ensured that critical software updates or patches were installed on their computers. In addition, in order to access network resources and to receive district-deployed patches and software, PCs on the M-DCPS network must be members of a ***domain*** or "family" of computers. The computers tested at all 21 schools visited were members of the DADESCHOOLS domain. However, seven (7) of the 21 schools audited (or 33%) had computers that did not have the required 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 III. 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, protect M-DCPS business processes and confidential student/employee information from viruses and other malicious threats. AV software is automatically deployed on the District's network via BigFix, the patch management tool the District uses. This method of deployment significantly reduces labor and overhead that would otherwise be incurred with individual installation. Many SBTs rely exclusively on this method for AV installation.

SBTs 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.

RECOMMENDATION:

2.1 Require SBTs to regularly review BigFix AV reports for all assigned locations to address AV deficiencies.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Procedure to correct the issue:
We ran BigFix reports in order to discover any machines missing the required antivirus software. During the school visit by an ITS district tech we supported the SBT by physically verifying the machines identified in the BigFix report. If the machine identified in BigFix was missing the anti-virus (AV) software the TST was required to manually install Sophos. If we find the desktop did have AV installed an email was sent to Network Services (Antivirus Administrator) to verify these machines again and to update BigFix.

Policy Implemented for Future Prevention of this issue:
ITS immediately implemented a regular procedure which requires all SBTs to check BigFix for any machines missing Sophos. The above procedure needs to be repeated to physically verify and correct any machines that appear in the report.

3. COMPUTERS NEED TO BE PASSWORD-PROTECTED AFTER USER LOGON

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."

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 information.

We examined a sample of administrative computers and found that at 10 of the 21 schools visited (or 48%), timeouts with password protection after authorized logon had not been enabled on an unacceptably large number of computers, leaving those computers vulnerable to tampering. Additionally, this function is frequently being left to the discretion of individual users. Our experience finds that when left up to the individual user, implementation of this setting is generally ignored. Furthermore, tampering would be difficult to detect since changes are accomplished while logged in as an authorized user and may go undetected.

RECOMMENDATION:

3.1 Require SBTs to implement a group policy that forces sensitive computers on the school's network (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, but should not exceed 15 minutes.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Procedure to correct the issue:
We immediately implemented an ITS Group Policy at those sites to lockup a login session within a period of 5-15 minutes.

Policy Implemented for Future Prevention of this issue:
Since taking over the supervision of the TST's last August we have instructed them on the use of Group Policy. We now have group policies that will time out/lock all administration and teacher desktops after 15 minutes of idle mode, which they are currently implementing. Also, they had only been putting it on Teachers' Groups, but we are expecting them to place the policy into the main Organizational Unit (OU) to affect all personnel at a site.

4. NON-STANDARD LOCAL ADMINISTRATOR ACCOUNTS ARE FOUND THROUGHOUT SOME SCHOOL NETWORKS

Established Standards

The standard method for accessing District computers involves supplying a network user ID and password. This process grants or limits access to the computer and network resources based on permissions that have been applied to a users account by network administrators.

A ***Local Administrator*** (LA) login is a powerful account allowing complete and unrestricted access to the computer and all information contained therein. LA accounts are typically known only to network managers and are used to install/uninstall software and hardware, and for troubleshooting purposes.

A second component related to LA access concerns LA Groups, (i.e., user accounts which are members of a **group** that has been given LA authority). Using **group accounts** to provide access instead of individual user accounts is an industry best practice and is required by NSS 4.1.1.13.

Observed Practice

Our audit found that although the computers tested at all 21 schools visited had the required minimum accounts or groups, 15 of the 21 schools audited (or 71%) showed the presence of an unacceptably large number of various non-standard LA accounts (*accounts with the same type of LA authority in addition to the required built-in account*) throughout the network. This practice significantly increases the risk of unauthorized access to systems, bypassing the controls of a standard network login. Furthermore, it also introduces the potential for non-technical users to perform unauthorized, unintended or harmful configuration.

In addition, at 6 of the 21 schools audited (or 29%), LA access was being handled using standalone accounts. By adding or removing users from groups, permissions are efficiently managed when a user's role changes.

RECOMMENDATIONS:

4.1 Require SBTs to verify and delete all non-standard LA accounts. Existing image files (deployable copies of hard drive installations) should be

reviewed to ensure that non-standard LA accounts are not part of the image to prevent unintentional redistribution.

RESPONSIBLE DEPARTMENT: **Information Technology Services**

MANAGEMENT'S RESPONSE:

Procedure to correct the issue:
ITS directed the site technicians in the use of special scripts through Group policy, which were implemented and pushed immediately to detect and remove all non-standard local administrator accounts from the system.

Policy Implemented for Future Prevention of this issue:
SBTs are now required to check BigFix on a monthly basis to verify if there's any non-standard local Admin accounts present in their locations. They must run a special script at least once a month to detect these accounts. On a regular basis they should be running a script to remove these accounts from the system, which can be attached to the login script.

4.2 Require that all other LA-type access be managed through group memberships, not individual accounts.

RESPONSIBLE DEPARTMENT: **Information Technology Services**

MANAGEMENT'S RESPONSE:

All individual local administrator accounts are being systematically removed by the Group Policy tool within Microsoft Active Directory or manually by TST as they are detected. This is being accomplished by the deployment of ghost scripts software, login scripts, physical removal and Group Policy. This process ensures that all LA-type accounts are managed via active directory group membership.

5. SERVERS NEED TO BE ROUTINELY BACKED UP

Established Standards — Servers are essentially upgraded computers equipped with redundancy components to protect against failure and act as a centralized network repository where users can store and access critical data. Routine backups are a necessary step towards restoring data in the event of failure. The District's NSS 4.1.1.7 and best practices recommend that servers be backed up periodically as part of an entity's disaster recovery routine.

Observed Practice — Our audit showed that all 21 schools visited maintained documentation of the layout of their network and their hard drive disposal process, and 18 of those schools maintained a written disaster recovery plan. However, four (4) of the 21 schools audited (or 19%) were not performing routine data backups of their servers as is required by the M-DCPS NSS and typical disaster recovery plans.

RECOMMENDATION:

5.1 Require that SBTs comply with NSS 4.1.1.7 and best practices by performing routine backups of critical data. In addition, backup procedures should be fully documented, with copies made available to the school Principal and the appropriate ITS Administrator.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

For all remaining data servers, ITS is recommending the use of the districts Collaboration Portal that is available to all students and staff to store their critical data, thereby eliminating the need for physical servers to be located at school sites. This will eliminate the need to back up these servers until all data resides on the collaboration site.

All TST's are required to perform weekly backups using available equipment to the school following the standard backup procedure document that they have filled in with the detailed steps, file names and server names and backup device names, types and locations, on how to recover from a possible loss of data. The copy of the document is always available to the principal and ITS administrators. The instructions provided in the backup document are detailed and simple enough that any technical person can follow. Lastly, during our monthly organization review meetings we continue to emphasize regularly the need for the weekly backups.

6. PERFORM REVIEWS FOR THE PRESENCE OF UNAUTHORIZED WIRELESS ACCESS POINTS AND DOCUMENT THE RESULTS

Established Standards

When installed correctly, Wireless Access Points (WAPs) provide a simple and cost effective method of making network resources available. Information Technology Services has developed an operating practice where SBTs are required to perform routine sweeps throughout their assigned campus to detect the installation of unapproved WAPs. Results are to be documented and reported to the Principal and an ITS Administrator for appropriate action, if necessary.

In addition, NSS 4.2, states in part that, *"ITS must be informed of all District wireless installations. This includes school sites… Site supervisors and technicians should check that other staff does not install rogue devices without approval and/or correct security settings. These devices become open doors to hackers seeking to get into the network."*

Observed Practice

Due to the relatively low cost and wide availability of these devices, WAPs are sometimes purchased and installed without the knowledge of school administrators or technicians. This creates a vulnerable entry point to the M-DCPS network that can be accessed by devices such as laptops, tablets and smart-phones. At three (3) of the 21 schools audited (or 14%), verification for unauthorized WAPs was not being performed.

RECOMMENDATION:

6.1 Required SBTs to comply NSS 4.2 by routinely performing sweeps for the presence of unauthorized WAPs and reporting the documented results to the Principal and the appropriate ITS Administrator.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

On the first of each month all TST's are required to scan the school (by using a laptop or some other available equipment) for unauthorized access points throughout the school. In addition the TST is required to create a Heat ticket for each scan performed. The Heat ticket number together with the date is later recorded in a log that is kept in the MDF room. This monthly scan is also verified by the principal who is also required to sign the log.

MANAGEMENT'S RESPONSE

MEMORANDUM

March 22, 2011
DK# 105/2010-2011

TO: Dr. Richard H. Hinds, Associate Superintendent and Chief Financial Officer
Financial Services

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

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

SUBJECT: **RESPONSE TO OMCA DRAFT OF INFRASTRUCTURE & SYSTEMS SUPPORT (ISS) AREA III-SELECTED SCHOOL SITES**

Below is the Information Technology Services (ITS) response to the 6 items on the ISS Area III selected school sites field audit.

RECOMMENDATIONS:

1.1 Require all SBTs to reconcile their location(s) AD on a regular basis using BigFix as a baseline.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Procedure to correct the issue:
We instructed our Technical Support Technicians (TST) to reconcile the Organizational Units (OU) with BigFix by comparing the number of accounts between Bigfix and Active Directory and verifying they are equal. If the tech is unable to locate the machines identified in the Active directory Reports, they are instructed to delete and remove these old computer account entries from Active Directory. The deletion of these accounts will take approximately 30 days before Active Directory reconciles with the Dadeschools domain. In addition it takes 30 days for the above changes to appear in Bigfix Reports.

Policy Implemented for Future Prevention of this issue:
We have already implemented a monthly procedure instructing all TST to compare and verify the BigFix Report to Active Directory for equal number of accounts. All TST's are now required to delete and remove all unused computer accounts as identified in the BigFix report. In addition, ITS field support staff will randomly select sites throughout the Region and verify BigFix numbers with Active Directory.

2.1 Require SBTs to regularly review BigFix AV reports for all assigned locations to address AV deficiencies.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Procedure to correct the issue:

We ran BigFix reports in order to discover any machines missing the required antivirus software. During the school visit by an ITS district technician we supported the SBT by physically verifying the machines identified in the BigFix report. If the machine identified in BigFix was missing the anti-virus (AV) software the TST was required to manually install Sophos. If we find the desktop did have AV installed an email was sent to Network Services (Antivirus Administrator) to verify these machines again and to update BigFix.

Policy Implemented for Future Prevention of this issue:

ITS immediately implemented a regular procedure which requires all SBTs to check BigFix for any machines missing Sophos. The above procedure needs to be repeated to physically verify and correct any machines that appear in the report.

3.1 **Require SBTs to implement a group policy that forces sensitive computers on the school's network (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, but should not exceed 15 minutes.**

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Procedure to correct the issue:

We immediately implemented an ITS Group Policy at those sites to lockup a login session within a period of 5-15 minutes.

Policy Implemented for Future Prevention of this issue:

Since taking over the supervision of the TST's last August we have instructed them on the use of Group Policy. We now have group policies that will time out/lock all administration and teacher desktops after 15 minutes of idle mode, which they are currently implementing. Also, they had only been putting it on Teachers' Groups, but we are expecting them to place the policy into the main Organizational Unit (OU) to affect all personnel at a site.

4.1 Require SBTs to verify and delete all non-standard LA accounts. Existing image files (deployable copies of hard drive installations) should be reviewed to ensure that non-standard LA accounts are not part of the image to prevent unintentional redistribution.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Procedure to correct the issue:

ITS directed the TSTs in the use of special scripts through Group policy, which were implemented and pushed immediately to detect and remove all non-standard local administrator accounts from the system.

Policy Implemented for Future Prevention of this issue:

SBTs are now required to check BigFix on a monthly basis to verify if there's any non-standard local Admin accounts present in their locations. They must run a special script at least once a month to detect these accounts. On a regular basis they should be running a script to remove these accounts from the system, which can be attached to the login script.

4.2 Require that all other LA-type access be managed through group memberships, not individual accounts.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

All individual local administrator accounts are being systematically removed by the Group Policy tool within Microsoft Active Directory or manually by TST as they are detected. This is being accomplished by the deployment of ghost scripts software, login scripts, physical removal and Group Policy. This process ensures that all LA-type accounts are managed via active directory group membership.

5.1 Require that SBTs comply with NSS 4.1.1.7 and best practices by performing routine backups of critical data. In addition, backup procedures should be fully documented, with copies made available to the school Principal and the appropriate ITS Administrator.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

For all remaining data servers, ITS is recommending the use of the districts Collaboration Portal that is available to all students and staff to store their critical data, thereby eliminating the need for physical servers to be located at school sites. This will eliminate the need to back up these servers until all data resides on the collaboration site.

All TST's are required to perform weekly backups using available equipment to the school following the standard backup procedure document that they have filled in with the detailed steps, file names and server names and backup device names, types and locations, on how to recover from a possible loss of data. The copy of the document is always available to the principal and ITS administrators. The instructions provided in the backup document are detailed and simple enough that any technical person can follow. Lastly, during our monthly organization review meetings we continue to emphasize regularly the need for the weekly backups.

6.1 Required SBTs to comply NSS 4.2 by routinely performing sweeps for the presence of unauthorized WAPs and reporting the documented results to the Principal and the appropriate ITS Administrator.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

On the first of each month all TST's are required to scan the school (by using a laptop or some other available equipment) for unauthorized access points throughout the school. In addition the TST is required to create a Heat ticket for each scan performed. The Heat ticket number together with the date is later recorded in a log that is kept in the MDF room. This monthly scan is also verified by the principal who is also required to sign the log.

cc: Mr. Trevor Williams
Mr. Jim O'Donnell
Mr. Javier Perez
Ms. Dina Pearlman
Mr. Rolando Avila
Mr. Luis Baluja

The School Board of Miami-Dade County, Florida, adheres to a policy of nondiscrimination in employment and educational programs/activities and programs/activities receiving Federal financial assistance from the Department of Education, 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 sex 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.

School Board Rules 6Gx13- 4A-1.01, 6Gx13- 4A-1.32, and 6Gx13- 5D-1.10 - prohibit harassment and/or discrimination against a student or employee on the basis of gender, race, color, religion, ethnic or national origin, political beliefs, marital status, age, sexual orientation, social and family background, linguistic preference, pregnancy, or disability.

Veterans are provided re-employment rights in accordance with P.L. 93-508 (Federal Law) and Section 295.07 (Florida Statutes), which stipulate categorical preferences for employment.

Revised 5/9/03

INTERNAL AUDIT REPORT

Network and Information Security
Information Technology Services
Infrastructure and Systems Support Area III –
Selected School Sites

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