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 V – SELECTED SCHOOL SITES

Adequate management of network resources and data security was generally observed; but opportunity to improve network security and availability exists.

June 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

June 23, 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 (IT) audit at various schools within Information Technology Services (ITS) Infrastructure and Systems Support (ISS) Area V to assess network security and evaluate the mechanisms in place at those schools to protect critical systems and data.

This is the third in a series of reports that address information and network security practices at school sites. This report covers 20 of the 74 schools that are under the auspices of ITS ISS Area V. An assessment of the remaining 54 schools within ITS ISS Area V 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.

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

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.

This is the third 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

OVERVIEW OF FINDINGS

- **School site Active Directory (AD) computer accounts should be reconciled to BigFix. Nineteen of the 20 locations reviewed (or 95%) have not reconciled AD.**
- **Four of the 20 schools reviewed (or 20%) had multiple computers that did not have the required up-to-date antivirus software installed.**
- **Eight of the 20 schools reviewed (or 40%) had one or more computers that had not been made a member of the domain.**
- **Timeouts with password protection after authorized logon and user inactivity should be enabled on computers through a centralized policy to protect critical computers.**
- **While computers generally contained the required minimum accounts, various non-standard Local Administrator accounts are found throughout 11 of the 20 (or 55%) school networks tested.**
- **Wireless access point sweeps, administrative hard drive disposal, and disaster recovery plans need to be consistently performed and documented.**
- **Intrusion prevention devices should be timely repaired and installed.**

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. There were other less critical matters discussed with management that are not reported herein.

Based on our observations, we have made 12 recommendations with detailed findings beginning on page 10.

INTERNAL CONTROLS

The charts below summarize our overall assessment of network, data and systems security found at the 20 schools reported on herein that are under the auspices of ISS Support Area V. An assessment of the remaining 50 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's 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 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 a 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.

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 also 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. Previously, we have reported the results of the audits we have conducted at two of the six support areas. ISS Support Area V (70 schools) is staffed as follows:

ISS Support Area V (as of May 2011)	
Title	**Quantity**
Technical Support Technician (**TST**): • Microsystems Technician (**MST**) • Computer Specialist (**CS**) • Computer Technician (**CT**)	50
Network Data Communication Specialist (**NDCS**)	2
Network Analyst (**NA**, Administrator)	0
Project Manager (**PM**, Administrator)	1
TOTAL	**53**

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

TSTs 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 and equipment problems that cannot be handled by the on-site technician are escalated to NDCS staff. TSTs and NDCS in this support area report to a Project Manager.

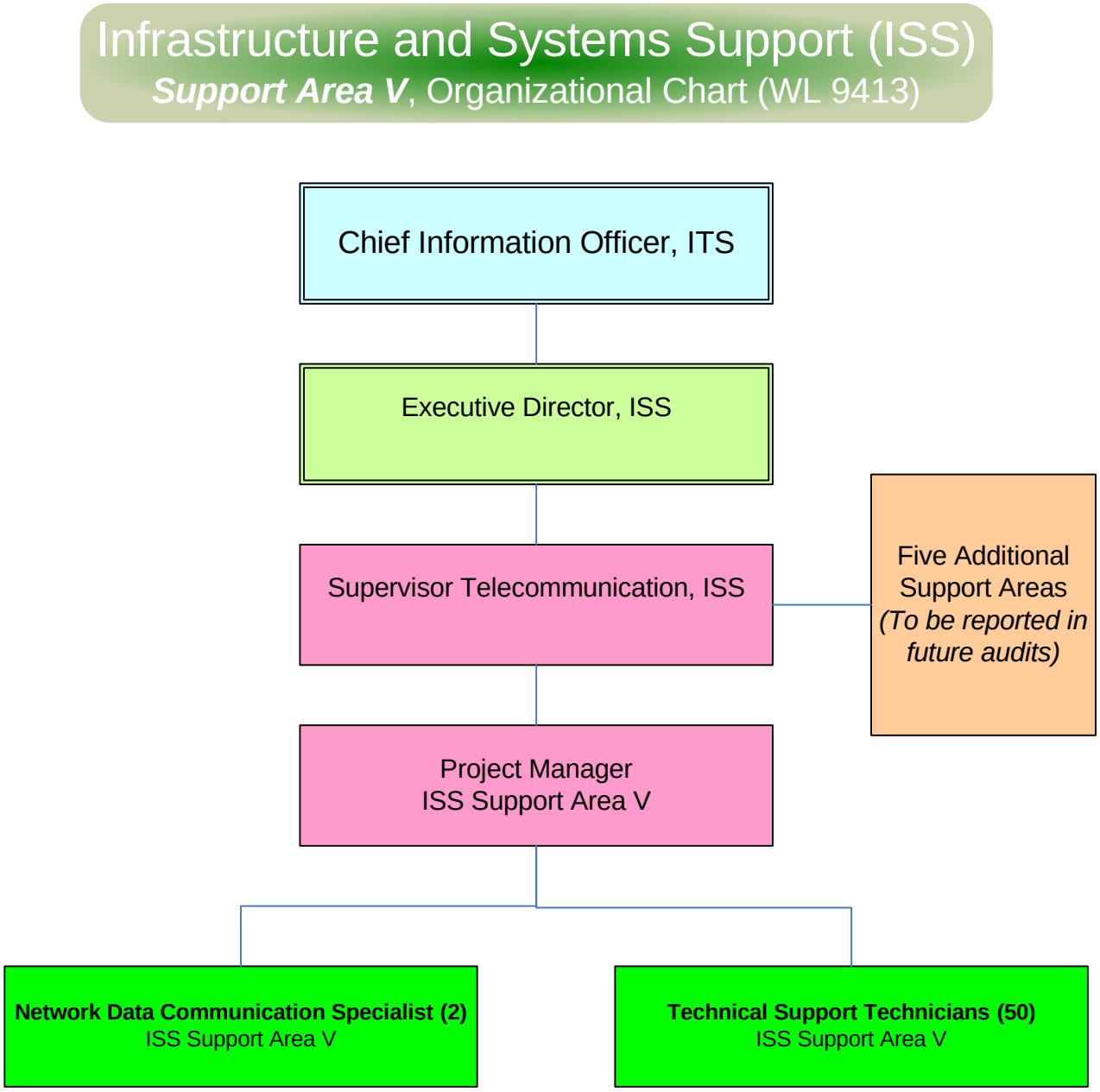
It should be noted that prior to the realignment described above, TSTs were classified as 12-month employees. At the start of our audit fieldwork, TSTs followed a 10-month work schedule similar to most school site personnel. Consequently, IT support resources have diminished significantly and have been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

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 and may help to slow or prevent the previously described exodus.

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.

ORGANIZATIONAL CHART



OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with the approved Audit Plan for the 2010-2011 Fiscal Year, we have performed an audit of network data and systems security at 20 of the 70 schools located within ISS Support Area V. 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 V.

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 review;
- 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

Our audit found that at 19 of the 20 schools reviewed (or 95%), 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 10,460 versus 7,147 in BigFix. The range of the delta, among individual schools, for the number of computers in the AD library versus the BigFix library was within a low of 30 computers (11%) to a high of 587 computers (46%).

Differences in the computer library counts could be 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 Audit Response:

- ITS concurs with this finding. In researching this issue, the following are some of the reasons we found for the AD counts to be greater than the Big Fix counts:
    - Computers with corrupted Big Fix and/or Sophos clients not showing on Big Fix counts.
    - Computers pending repair and/or service still showing in AD.
    - New computers deployment and imaging in progress.
    - Wireless labs and off-site loaner devices not being actively used when Big Fix reports run.

ITS Standards Implemented to resolve the findings:

- Require TST to run Monthly Big Fix and AD reports in order to correlate reports and fix any corrupted clients, with the goal to have less than a 10% delta.
- Require TST to document reasons for delta, which can be provided to ITS and auditors on request.
- Require TST to run any unused wireless labs every few months in order to ensure, wireless devices receive their updates, in a timely fashion and be counted by Big Fix. Also 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 audit to verify Standards and procedures are being followed.
- ITS continues to hold monthly Operations Review, with all TSTs, in an effort to provide up to date information and remind TSTs to adhere to and 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 5.1.17 and industry recommended best practices, antivirus (AV) software should be installed on all computers.

Observed Practice

Our audit found that all, except for one (1) of the 20 schools audited maintained evidence of their employee's awareness of the M-DCPS NSS. Furthermore, all 20 schools audited ensured that critical software updates or patches were installed on their computers. However, four (4) of the 20 schools reviewed (or 20%) 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 V. 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 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 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 note any schools which did not have the required AV software installed. Only a few computers at some schools had corrupted Big Fix and/or Sophos clients which prevented them from receiving the latest AV updates. These corrupted machines are re-imaged or manually corrected in an on-going process as they appear.

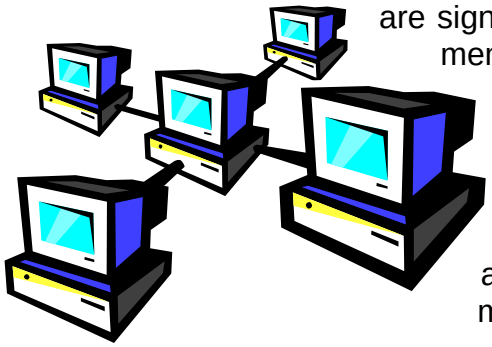
ITS Standards Implemented to resolve findings:

- Require TST to run Monthly AV Reports utilizing Big Fix.
- Recommend implementing Window Update Services Server (WSUS) as backup to Big Fix.
- ITS will perform random audits to verify Standards and procedures are being followed.

3. ALL COMPUTERS SHOULD BE MEMBERS OF THE DOMAIN

Established Standards

In order to access network resources, receive district-deployed patches/software automatically, and be subject to certain controls, computers must be made members of a ***domain*** or "family" of computers. Network security controls are significantly improved when computers are members of a domain structure. Due to weaknesses revealed during a 2007 external audit, ITS accelerated a migration project to bring all district computers under one domain. According to the NSS sections 4.1.1.5 and 5.0.17, all computers must be made members of the domain.



BigFix reports are available to quickly identify computers that have not been made members of the domain.

Observed Practice

Our audit found that eight (8) of the 20 schools reviewed (or 40%) had one or more computers that had not been made a member of the domain. This condition limits the performance and security benefits achieved through domain membership.

Some computers had been placed into service before being properly added to the domain, while others were found to have membership in domains that have been inactive for a number of years.

RECOMMENDATION:

3.1 Complete the migration of existing machines to the domain with an agreed upon deadline established for completion. In addition, develop procedures to ensure that new or serviced computers are made members of the domain prior to being placed into service.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this finding and has been actively pushing this standard through. In fact, since the time of this audit (November, 2010), this number has been reduced approximately 75% to just over 700 computers, out of the District total of 125,000 computers.

ITS Standards Implemented to resolve findings:

- ITS will continue to address this issue with TSTs at our monthly Operation Reviews and remind them of the importance of adhering to all District procedures and the NSS.

- ITS continues to programmatically check the number of computers which have not been migrated and continues to pass said information to affected TSTs.

3.2 Require TSTs to routinely review BigFix reports to proactively identify PCs that are not domained and to take the appropriate actions.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this finding and has been actively pushing this standard through. In fact, since the time of this audit (November, 2010), this number has been reduced approximately 75% to just over 700 computers, out of the District total of 125,000 computers.

ITS Standards Implemented to resolve findings:

- ITS will continue to address this issue with TSTs at our monthly Operation Reviews and remind them of the importance of adhering to all District procedures and the NSS.
- ITS continues to programmatically check the number of computers which have not been migrated and continues to pass said information to affected TSTs.

4. A CENTRALIZED TIME-OUT 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. ITS supports most school site technology, including workstations with the exception of workstations that are physically located at each school cafeteria. These computers typically run system updates once cafeteria staff has left for the day and are supported by the Department of Food and Nutrition personnel.

We examined a sample of critical workstations (teacher, server, administrative), which ITS has servicing responsibility over and found that at 11 of the 20 schools visited (or 55%), timeouts with password protection after authorized logon had not been enabled on all computers tested, leaving those unprotected computers vulnerable to tampering. In addition, we also examined eight (8) cafeteria computers, which are serviced by the Department of Food and Nutrition and found that seven (7) were not subject to a centralized timeout password protection policy. This function is being left to the discretion of individual users. Our experience finds 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:

4.1 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, not to 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 GPOs, it has not been fully accepted by all users. As a result, ITS has attended several seminars and webinars regarding security, but so far has not been made aware of industry standards in the education arena. ITS is working with the Council of Great City Schools (CGCS) to establish a baseline among large, urban districts to see where we fall. 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 count, based on job responsibilities and position. It is important to note that the NSS requires users lock their computers when they walk away, and indeed this is the best way to protect the data, as a timeout does not take immediate effect. A way needs to be established to hold individual users accountable for their actions. A recent Weekly Briefing (#10003) was sent out to remind users of their responsibilities in this area.

ITS Standards Implemented to resolved findings:

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

4.2 Implement a group policy that forces cafeteria workstations at schools to automatically lock after a preset period of user inactivity, not to exceed 15 minutes.

RESPONSIBLE DEPARTMENT: Department of Food and Nutrition

MANAGEMENT'S RESPONSE: The Department of Food and Nutrition with the assistance of ITS will install the lock after a preset period of time in a number of cafeteria computers on a pilot basis to determine the effect of this lock in the operation of the computer and the registers. This pilot will be conducted when school resumes in August 2011. If it is determined that the lock does not affect the continuous operation of the point of sale registers, it will then be installed at all cafeteria computers.

The Department of Food and Nutrition utilizes the cafeteria computer station to run the Fastrak Software (software utilized at all cafeterias) for all point of sales processing student accounts as meals are served. An automated shut down would interfere with student meal services. This pilot will determine if the cafeteria computer can continue to run without interruption.

5. NON-STANDARD LOCAL ADMINISTRATOR ACCOUNTS ARE FOUND THROUGHOUT SOME SCHOOLS' NETWORKS

Established Standards

The standard method for accessing district computer resources 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 user's account by a network administrator.

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, (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 and 5.1.20.

Observed Practice

Our audit found that 11 of the 20 schools audited (or 55%) showed the presence of multiple computers having 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 and 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 to the computer.

Administrative access to computers should be limited to authorized technical staff and should be managed through group accounts. By adding or removing users through groups, permissions are efficiently managed when a user's role changes.

RECOMMENDATIONS:

5.1 Require TSTs 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: ITS concurs with this finding. In researching this issue, we found that although some computers had multiple LA accounts, all were secured accounts. Also certain accounts that are associated with services running on servers require a dedicated account to run automated tasks. For example a backup server may require the local admin account to run if the Domain is not available. These "service accounts" are password protected and documented.

ITS Standards Implemented to resolved findings:

- All new image creation and deployment now includes our desktop standards and security permissions.
- We have implemented a standard where we manage user permissions utilizing AD and not local admin accounts wherever possible.
- ITS will continue to use our monthly ORs' to remind all TSTs' the importance of following and adhering to all NSS policies.

5.2 Ensure that all LA access is managed through group memberships using accounts residing in the domain.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this finding. In researching this issue, we found that although some computers were found, which had multiple LA accounts, all were secured accounts. Also certain accounts that are associated with services running on servers require a dedicated account to run automated tasks. For example, a backup server may require the local admin account to run if the Domain is not available. Additionally, some of the individual accounts identified at some schools were servers that a vendor uses to access remote management of instructional software. In these specific cases, vendor connects to their server via a secure VPN account. These accounts are password protected and documented.

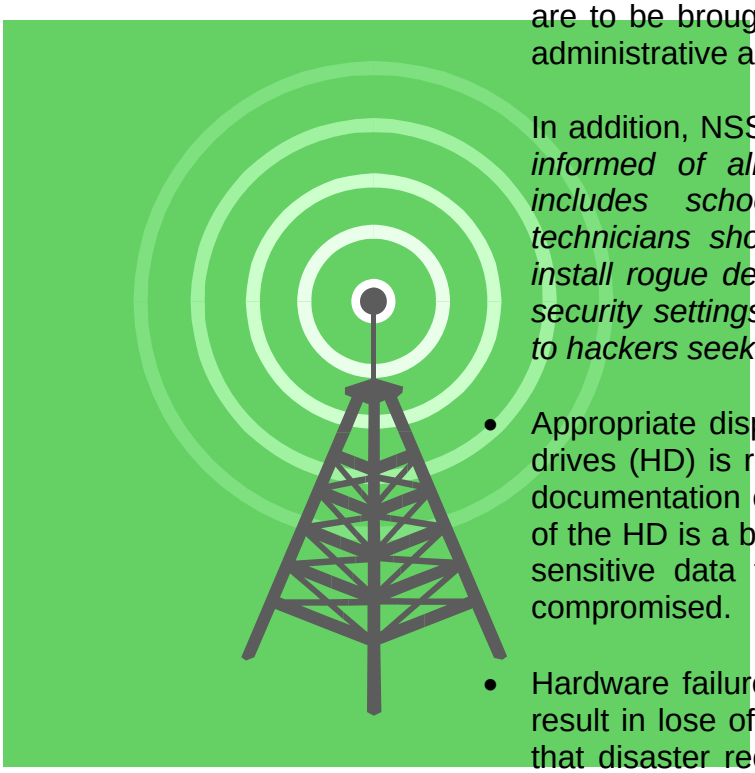
ITS Standards Implemented to resolved findings:

- We have implemented a standard where we manage user permissions utilizing AD and not local admin accounts wherever possible.
- ITS will perform random audit to verify Standards and procedures are being followed.

6. REQUIRED DOCUMENTATION EVIDENCING THE PERFORMANCE OF WIRELESS ACCESS POINT SWEEPS, HARD DRIVE DISPOSAL AND DISASTER RECOVERY WERE NOT AVAILABLE FOR REVIEW

Established Standards

Internal policy, as well as best practices requires documentation regarding certain network management procedures be maintained.



- TSTs are required to perform routine sweeps throughout their assigned campuses to detect the installation of unapproved WAPs. Wireless Access Point (WAP) sweeps proactively address unauthorized installations. Rogue WAP installations are to be brought to the attention of the Principal for administrative action.

  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."*

- Appropriate disposal of administrative computer hard drives (HD) is required by NSS 4.1.2.13. Maintaining documentation evidencing the disposal or destruction of the HD is a best practice, which provides proof that sensitive data that may exist on the drive will not compromised.

- Hardware failure is a common occurrence and could result in lose of data. As such, best practices require that disaster recovery procedures be developed and maintained. In addition to establishing step-by-step recovery procedures, the goal of a documented disaster recovery plan is to provide source information from which data can be restored. NSS 4.1.1.7 requires that at a minimum, all M-DCPS data be backed-up weekly and mission-critical data be backed-up daily.

Observed Practice

At 17 of the 20 schools audited (or 85%), documentation of WAP sweep and HD disposal were not available for audit. In addition, nine (9) of the 20 schools audited had not yet

prepared a disaster recovery plan and seven (7) schools did not perform routine backup of M-DCPS data.

RECOMMENDATIONS:

6.1 Required TSTs to comply with NSS 4.1.2.11 and 4.2 by routinely performing sweeps for the presence of unauthorized WAPs and reporting documented results to the Principal and the appropriate ITS Administrator.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this finding. At the time of this audit (November 2010), the scanning for rogue WAP devices was a newly established procedure, which was instituted in October, 2010. As a result, not all schools were performing a regularly scheduled sweep. Since the time of this audit, all TSTs have been informed and trained on when and how to best perform wireless sweeps, in an effort to identify rogue WAP devices. All sites are now scheduled to perform monthly wireless sweeps. All TSTs are now in compliance of this guideline.

ITS Standards Implemented to resolved findings:

- Wireless Scan procedure implemented.
- ITS will perform random audits to verify standards and procedures are being followed.
- Monthly Operation Reviews are held with all TSTs in order to remind them of the importance of adhering to all District/Security Policies.

6.2 To strengthen the efficacy of compliance with NSS 4.1.2.13, require that when administrative computers are surplus, a record of the disposal of the HD and the efforts undertaken to properly "clean" it be maintained.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with said finding, and agrees that this is more of a procedural issue vs. a security one. ITS will continue to address this issue with TSTs, at our monthly Operation Reviews and remind them, of the importance of following procedures and having proper documentation.

ITS Standards Implemented to resolve findings:

- ITS schedules monthly Operations Review (OR), with all TSTs. At ORs, TSTs are informed of new procedures and are introduced to District standards.
- Management Audits has been invited to attend the ORs' and speak to the importance of adhering to all District Standards.

6.3 Require that TSTs 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 in a disaster recovery plan, with copies made available to the school Principal and the appropriate ITS Administrator.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this finding. All disaster recovery plans include backup procedures, but lack of funds has prevented many sites from purchasing the required hardware and or media to backup servers on a schedule. In the event that the automated backup failed or was not possible, the TSTs will perform a manual backup using alternative media or hardware provided by the site. ITS has developed a template, which all TSTs are asked to follow.

ITS Standards Implemented to resolve findings:

- ITS schedules monthly Operations Review (OR), with all TSTs. At ORs, TSTs are informed of new procedures and are introduced to District standards.
- Management Audits has been invited to attend the ORs' and speak to the importance of adhering to all District Standards.
- Automated backup Standards in place.
- Notify Principals to purchase required equipment to perform backups.
- ITS will perform random audit to verify Standards and procedures are being followed.

7. INTRUSION PREVENTION SYSTEM DEVICE IS NOT INSTALLED AND/OR OPERATIONAL

Established Standards

All physically independent work locations are required to have a functional Intrusion Prevention System (IPS) device on the network. An IPS helps in proactively defending the network from both internal and external attacks, viruses, and quarantines computers that are non-compliant with various policies or exhibiting undesirable activity.

Observed Practice

Our audit found that at four (4) of the 20 schools audited (or 25%), the IPS device was either out for repair or was not installed. The related repair orders reviewed showed that the orders were between three and eight months old.

RECOMMENDATION:

7.1 Require TSTs to routinely check the IPS to ensure the device is installed and operational. Staff responsible for managing repair should monitor repair order status to ensure that repairs are completed and the device is placed back into service within a reasonable period of time from the date of removal. A loaner device should be installed while the original is being repaired to protect the network in the interim.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this finding. Circumstances were beyond the ITS' control. Several years ago, ITS implemented the deployment and installation of an IPS device, at all schools. This was done in order to provide a first layer of defense against viruses and worms. The device used was called Tipping Point (TP) and was originally manufactured by 3Com Technologies. Several years after the purchase of the TP devices, 3Com was purchased by Hewlett Packard (HP). As a result, the TP devices were manufacturer discontinued by HP. Recently, due to ITS' efforts, HP began supporting the TP device and has begun to swap out defective units. However, at the time of this audit, November, 2010 there were several months when TP devices and components were not available. Please note, that although 4 schools were affected by the backlog of TP devices, ITS also has IPS devices installed at the core network. This allows ITS to maintain redundancy, therefore providing an additional layer of security. This allows ITS to always keep the Enterprise Network protected.

ITS Standards Implemented to resolved findings:

- Several meetings were held with the Enterprise Account Manager and several high ranking officials from HP, and as a result, ITS was ensured product would be readily made available.
- ITS performs regular, automated random scans of the network, in order to identify any school that may not have an operational TP device.

MANAGEMENT'S RESPONSE – Information Technology Services

M E M O R A N D U M June 22, 2011
DK #116/2010-2011

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

FROM: Debbie Karcher, Chief Information Officer
Information Technology Services

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

Below are the Information Technology Services (ITS) responses to the 7 items on the ISS AREA V selected school sites field audit. It should be noted that it is very difficult to maintain an absolute, 100% secure posture in classrooms, especially considering that the student users we deal with every day are not only very tech savvy, but are often actively trying to evade our efforts. It should also be noted that there are 125,000 District-owned computers connected to the network, with many more personally-owned devices coming on-line all the time. The local computers' protective applications are merely the first line of defense in a many-layered approach to security. Computers that are breeched are quickly identified, isolated, shut down, and scheduled for cleaning. This protects the rest of the network and occurs because of our Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Additionally, please note that at the time this audit began (November, 2010), ITS was still dedicating a large amount of resources, reconnecting computers, computer labs and technology, back online. This was caused as a result of having no technicians in schools over the summer. Nevertheless, ITS and the TSTs continue to strive to be 100% free of issues. As the number of computers and technology continue to grow in our schools, ITS is developing more programmatic and automated strategies in order to address variances between virtual and authentic discrepancies. We realize that we cannot always count on physical inspections, in order to maintain compliance. Going forward, ITS has also requested to see and sign-off on the Field Audit worksheets, and both parties agreed, since some discrepancies have been identified.

Since the beginning of the school based "Field Audits", ITS has incorporated monthly meetings with all TSTs, where procedures and standards are reviewed. Said meetings are called our ***Operations Review*** and in order to keep all TSTs updated, several members of Management Audit were invited and during these meetings, audit and security procedures was discussed with all TSTs.

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 for the AD counts to be greater than the Big Fix counts:
  - Computers with corrupted Big Fix and/or Sophos clients not showing on Big Fix counts.
  - Computers pending repair and/or service still showing in AD.
  - New computers deployment and imaging in progress.
  - Wireless labs and off-site loaner devices not being actively used when Big Fix reports run

ITS Standards Implemented to resolve the findings:

- Require TST to run Monthly Big Fix and AD reports in order to correlate reports and fix any corrupted clients, with the goal to have less than a 10% delta.
- Require TST to document reasons for delta, which can be provided to ITS and auditors on request.
- Require TST to run any unused wireless labs every few months in order to ensure, wireless devices receive their updates, in a timely fashion and be counted by Big Fix. Also 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 audit to verify Standards and procedures are being followed.
- ITS continues to hold monthly Operations Review, with all TSTs, in an effort to provide up to date information and remind TSTs to adhere too and 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 note any schools which did not have the required AV software installed. Only a few computers at some schools had corrupted Big Fix and/or Sophos clients which prevented them from receiving the latest AV updates. These corrupted machines are re-imaged or manually corrected in an on-going process as they appear.

ITS Standards Implemented to resolve findings:

- Require TST to run Monthly AV Reports utilizing Big Fix.
- Recommend implementing Window Update Services Server (WSUS) as backup to Big Fix.
- ITS will perform random audits to verify Standards and procedures are being followed.

3.1 Complete the migration of existing machines to the M-DCPS domain with an agreed deadline established for completion. In addition, develop procedures to ensure that new or serviced computers are made members of the domain prior to being placed into service.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Move all computers under the domain.

Audit Response:

- ITS concurs with this finding and has been actively pushing this standard through. In fact, since the time of this audit (November, 2010), this number has

been reduced approximately 75% to just over 700 computers, out of the District total of 125,000 computers.

ITS Standards Implemented to resolve findings:

- ITS will continue to address this issue with TSTs at our monthly Operation Reviews and remind them of the importance of adhering to all District procedures and the NSS.
- ITS continues to programmatically check the number of computers which have not been migrated and continues to pass said information to affected TSTs.

3.2 Require TSTs to routinely review BigFix reports to proactively identify PCs that are not domained and to take the appropriate actions.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Move all computers under the domain.

Audit Response:

- ITS concurs with this finding and has been actively pushing this standard through. In fact, since the time of this audit (November, 2010), this number has been reduced approximately 75% to just over 700 computers, out of the District total of 125,000 computers.

ITS Standards Implemented to resolve findings:

- ITS will continue to address this issue with TSTs, at our monthly Operation Reviews and remind them of the importance of adhering to all District procedures and the NSS.
- ITS continues to programmatically check the number of computers, which have not been migrated and continues to pass said information to affected TSTs.

4.1 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 GPOs, it has not been fully accepted by all users. As a result, ITS has attended several seminars and webinars regarding security, but so far has not been made aware of industry standards in the education arena. ITS is working with the Council of Great City Schools (CGCS) to establish a baseline among large, urban districts to see where we fall. 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 count, based on job responsibilities and position. It is important to note that the NSS requires users lock their computers when they walk away, and indeed this is the best way to protect the data, as a timeout does not take immediate effect. A way needs to be established to hold individual users accountable for their actions. A recent Weekly Briefing (#10003) was sent out to remind users of their responsibilities in this area.

ITS Standards Implemented to resolved findings:

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

4.2 Implement a group policy that forces cafeteria workstations at schools to automatically lock after a preset period of user inactivity, not to exceed 15 minutes.

RESPONSIBLE DEPARTMENT: Department of Food and Nutrition

MANAGEMENT'S RESPONSE:

5.1 Require TSTs 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:

Audit Finding:

- Non-standard local administrator accounts are found throughout some school networks.

Audit Response:

- ITS concurs with this finding. In researching this issue, we found that although some computers had multiple LA accounts, all were secured accounts. Also certain accounts that are associated with services running on servers require a dedicated account to run automated tasks. For example a backup server may require the local admin account to run if the Domain is not available. These "service accounts" are password protected and documented.

ITS Standards Implemented to resolve findings:

- All new image creation and deployment now includes our desktop standards and security permissions.
- We have implemented a standard where we manage user permissions utilizing AD and not local admin accounts wherever possible.
- ITS will continue to use our monthly ORs' to remind all TSTs' the importance of following and adhering to all NSS policies.

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

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Non-Standard local administrator accounts are found throughout some schools networks.

Audit Response:

- ITS concurs with this finding. In researching this issue, we found that although some computers were found, which had multiple LA accounts, all were secured accounts. Also certain accounts that are associated with services running on servers require a dedicated account to run automated tasks. For example, a backup server may require the local admin account to run if the Domain is not available. Additionally, some of the individual accounts identified at some schools were servers that a vendor uses to access remote management of instructional software. In these specific cases, vendor connects to their server via a secure VPN account. These accounts are password protected and documented.

ITS Standards Implemented to resolve findings:

- We have implemented a standard where we manage user permissions utilizing AD and not local admin accounts wherever possible.
- ITS will perform random audit to verify Standards and procedures are being followed.

6.1 Required TSTs to comply with 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:

Audit Finding:

- Perform reviews for the presence of unauthorized wireless access points and document results.

Audit Response:

ITS concurs with this finding. At the time of this audit (November 2010), the scanning for rogue WAP devices was a newly established procedure, which was instituted in October, 2010. As a result, not all schools were performing a regularly scheduled sweep. Since the time of this audit, all TSTs have been informed and trained on when and how to best perform wireless sweeps, in an effort to identify rogue WAP devices. All sites are now scheduled to perform monthly wireless sweeps. All TSTs are now in compliance of this guideline.

ITS Standards Implemented to resolve findings:

- Wireless Scan procedure implemented.
- ITS will perform random audits to verify standards and procedures are being followed.
- Monthly Operation Reviews are held with all TSTs in order to remind them of the importance of adhering to all District/Security Policies.

6.2 To strengthen the efficiency of compliance with NSS 4.1.2.13 requires that when administrative computers are surplus, a record of the disposal of the HD and the efforts undertaken to properly "clean" it be maintained.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding
Auditor was not provided documentation regarding disposal of hard-drives

Audit Response

ITS concurs with said finding, and agrees that this is more of a procedural issue vs. a security one. ITS will continue to address this issue with TSTs, at our monthly Operation Reviews and remind them, of the importance of following procedures and having proper documentation.

ITS Standards Implemented to resolve findings:

- ITS schedules monthly Operations Review (OR), with all TSTs. At ORs, TSTs are informed of new procedures and are introduced to District standards.
- Management Audits has been invited to attend the ORs' and speak to the importance of adhering to all District Standards.

6.3 Require that TSTs 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 in a disaster recovery plan, with copies made available to the school Principal and the appropriate ITS Administrator.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- Servers need to be routinely backed up.

Audit Response:

- ITS concurs with this finding. All disaster recovery plans include backup procedures, but lack of funds has prevented many sites from purchasing the required hardware and or media to backup servers on a schedule. In the event that the automated backup failed or was not possible, the TSTs will perform a manual backup using alternative media or hardware provided by the site. ITS has developed a template, which all TSTs are asked to follow.

ITS Standards Implemented to resolve findings:

- ITS schedules monthly Operations Review (OR), with all TSTs. At ORs, TSTs are informed of new procedures and are introduced to District standards.

- Management Audits has been invited to attend the ORs' and speak to the importance of adhering to all District Standards.
- Automated backup Standards in place.
- Notify Principals to purchase required equipment to perform backups.
- ITS will perform random audit to verify Standards and procedures are being followed.

7.1 Require TSTs to routinely check the IPS to ensure the device is installed and operational. Staff responsible for managing repair should monitor repair order status to ensure that repairs are completed and the device is placed back into service within a reasonable period of time from the date of removal. A loaner device should be installed while the original is being repaired to protect the network in the interim.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- All schools should have an IPS in place.

Audit Response:

ITS concurs with this finding. Circumstances were beyond the ITS' control. Several years ago, ITS implemented the deployment and installation of an IPS device, at all schools. This was done in order to provide a first layer of defense against viruses and worms. The device used was called Tipping Point (TP) and was originally manufactured by 3Com Technologies. Several years after the purchase of the TP devices, 3Com was purchased by Hewlett Packard (HP). As a result, the TP devices were manufacturer discontinued by HP. Recently, due to ITS' efforts, HP began supporting the TP device and has begun to swap out defective units. However, at the time of this audit, November, 2010 there were several months when TP devices and components were not available. Please note, that although 4 schools were affected by the backlog of TP devices, ITS also has IPS devices installed at the core network. This allows ITS to maintain redundancy, therefore providing an additional layer of security. This allows ITS to always keep the Enterprise Network protected.

ITS Standards Implemented to resolve findings:

- Several meetings were held with the Enterprise Account Manager and several high ranking officials from HP, and as a result, ITS was ensured product would be readily made available.
- ITS performs regular, automated random scans of the network, in order to identify any school that may not have an operational TP device.

DK:jp

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

MANAGEMENT'S RESPONSE – Department of Food and Nutrition

DEPARTMENT OF FOOD AND NUTRITION

MEMORANDUM

June 22, 2011
PP/2010-2011/#2093
786-275-0420

TO: Mr. Trevor Williams, Assistant Chief Auditor
Office of Management and Compliance Audits

FROM: Penny Parham, Administrative Director
Department of Food and Nutrition

SUBJECT: **NETWORK AND INFORMATION SECURITY INFORMATION TECHNOLOGY SERVICES (ITS) INFRASTRUCTURE AND SYSTEMS SUPPORT AREA V – SELECTED SCHOOLS REPORT**

The following information is in response to the Audit Finding for the Department of Food and Nutrition.

4.2 Implement a group policy that forces cafeteria workstations at schools to automatically lock after a preset period of user inactivity, not to exceed 15 minutes.

RESPONSIBLE DEPARTMENT: Department of Food and Nutrition

MANAGEMENT'S RESPONSE:

The Department of Food and Nutrition with the assistance of ITS will install the lock after a preset period of user inactivity to pilot the effect of this lock in the cafeteria computer. This pilot is to determine if the lock will interfere with the operation of the cafeteria computer to run the point of sale registers. This pilot installation will be done once school resumes in August 2011.

The Department of Food and Nutrition utilizes the cafeteria computer station to run the Fastrak Software (software utilized at all cafeterias) for all point of sales processing student accounts as meals are served. An automated shut down would interfere with student meal services. This pilot will determine if the cafeteria computer can continue to run without interruption.

RECOMMENDATION:

The Department of Food and Nutrition with the assistance of ITS will install the lock after a preset period of time in a number of cafeteria computers on a pilot basis to determine the effect of this lock in the operation of the computer and the registers. This pilot will be conducted when school resumes in August 2011. If it is determined that the lock does not affect the continuous operation of the point of sale registers, it will then be installed at all cafeteria computers.

If additional information is required, please contact me at 786-275-0420, thank you.

PP:ayw

cc: Dr. Marcos M. Moran
Ms. Olga Botero
Mr. Thomas Holmberg

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 V:
Selected School Sites

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