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 IV – SELECTED SCHOOL SITES

There were no significant trends or findings noted while auditing the school locations sampled within this support area.

June 2012

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA

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

Mr. Alberto M. Carvalho
Superintendent of Schools

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

Contributors to This Report:

Audit Performed by:
Mr. Luis Baluja, CISA

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

Miami-Dade County Public Schools
giving our students the world

June 14, 2012

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

Ladies and Gentlemen:

In accordance with the approved Audit Plan for the 2011-12 Fiscal Year, we have completed an Information Technology (IT) audit at various schools within Information Technology Services (ITS) Infrastructure and Systems Support (ISS) Area IV to assess network security and evaluate the mechanisms in place at those schools to protect critical systems and data.

This is the fifth in a series of reports that address information and network security practices at school sites. This report covers 20 of the 59 schools located within ISS Area IV. An assessment of the remaining 39 schools within ISS Area IV will be reported on at a future date.

We are pleased to report that, based upon the scope of the audit, no significant trends or findings were noted while auditing the school locations sampled within this support area. This noteworthy accomplishment is in line with a steady progress in the declining number of findings related to this series of audits. Other isolated or inconsequential matters that came to our attention during our audit were communicated to management for its follow up.

We support the administration and staff's continuing efforts towards attaining a standardized, secure computing environment that embodies the M-DCPS Network Security Standards.

We would like to acknowledge management's positive, prompt and efficient response and thank management for the cooperation and courtesies extended to our staff during the audit.

Sincerely,

José F. Montes de Oca

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

TABLE OF CONTENTS

Page

CONCLUSION AND RECOMMENDATIONS

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 fifth 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.

The results reported in this series indicate that compliance with basic IT concerns within the scope of the audit, are being addressed. Management's awareness of previously reported trends of audit exceptions and their responsiveness in addressing findings have resulted in greater compliance with the above-stated standards.

CONCLUSIONS

- Continue to move towards centralized management and standardization of network resources.
- Continue effective oversight of technical support staff.
- Consider using ISS Service Area IV methodology as a model to be applied District-wide.

INTERNAL CONTROLS

The charts below summarize our overall assessment of network, data and systems security found at the 20 schools located within ISS Area IV. An assessment of the remaining 39 schools within this area will be reported at a future date.

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

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

BACKGROUND

M-DCPS currently utilizes approximately 125,000 computers at over 400 different physical locations across an enterprise-level network. This large network connects students, teachers, administrators and parents with a vast amount of information and educational tools. For example, student grades and attendance are reported via an electronic grade book system. Business transactions such as the procurement of goods and services as well as employee payroll are also processed on the District's network. Webinars, which allow principals to participate in important district meetings without having to leave the school campus where they are most needed, are accessed through the network. Parents and students can review student progress using district's portal. These and many other extremely critical district functions rely on the availability of a robust network with properly managed resources and equipment.

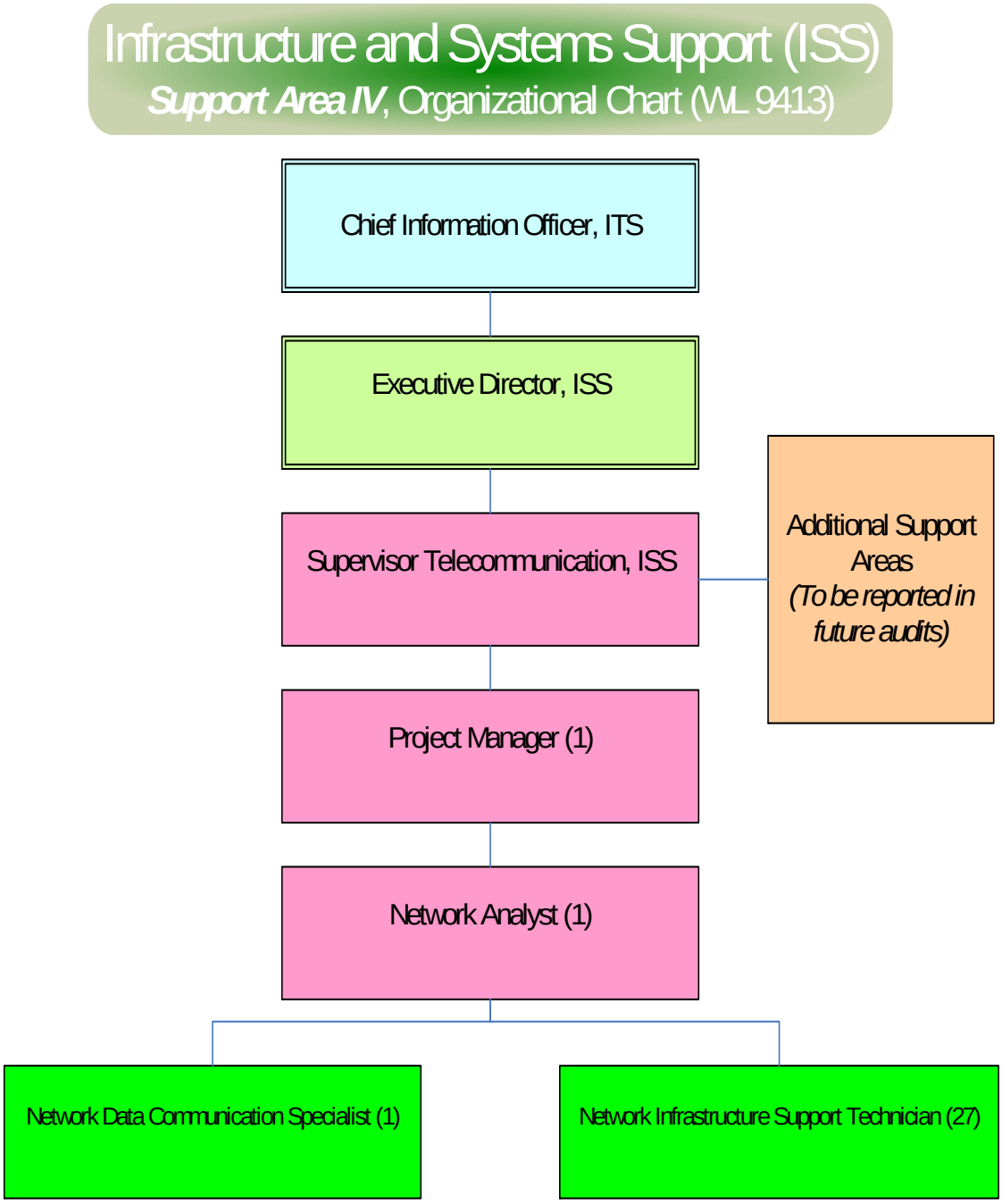
Network Infrastructure Support Technicians (NIST) are the primary source of technical support at each school site. On June 17, 2009, the School Board of Miami-Dade County approved agenda item D-26, which realigned the reporting structure for technicians from the school-site administrator (i.e., principal) to a centralized model under ITS. Under this model, technicians typically are assigned one or more schools and provide assistance to other nearby schools if needed. ITS is now in its second year of operating under this model and has been able to work through the associated challenges.

Infrastructure and Systems Support (ISS) is a subdivision of ITS and is responsible for managing technicians and providing all school site IT support. ISS has created six support areas, each maintained by a technical team that serves an average of about 60 schools. ISS Area IV (59 schools) is staffed as follows:

ISS Support Area IV (as of May 3, 2012)	
Title	**Quantity**
Network Infrastructure Support Technicians (**NIST**)	27
Network Data Communication Specialist (**NDCS**)	1
Network Analyst (**NA**, Administrator)	1
Project Manager (**PM**, Administrator)	1
TOTAL	**30**

NISTs 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. NIST and NDCS report to a Project Manager.

PARTIAL ORGANIZATIONAL CHART



OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with the approved Audit Plan for FY 2011-2012, we have performed an audit of network data and systems security at 20 of the 59 schools located within ISS Area IV. 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 Area IV.

We performed the following procedures to satisfy our audit objectives:

- Analyzed site assessments of each school submitted by ISS Project Managers with input from NIST's, NDCS staff, and other data, and selected a sample of schools for examination;
- Reviewed the District's NSS and other third party reports on IT best practices;
- Interviewed district staff identified in the organizational chart;
- Utilized software such as Active Directory, Tivoli, 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.

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, summarized as follows:

- 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.

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".

CONCLUSION AND RECOMMENDATIONS:

1. CENTRALIZED MANAGEMENT OF NETWORK RESOURCES AND TOOLS HAS MARKEDLY IMPROVED

A steady decline in audit findings covering a timeframe of several years indicates a favorable movement by the Administration towards standardization and centralization. For example, earlier audits found that no timeout policy was in place at school sites to help protect critical computers. After authorized users logon to the M-DCPS network, many district functions, network resources, and confidential data are made accessible. Unsupervised and unlocked computers pose a threat to the integrity of district and student information. At all 20 school locations tested, a centralized policy was enabled that automatically locks users' computer after a predetermined period of inactivity.

RECOMMENDATION:

1.1 Continue moving towards centralized management and standardization aimed at protecting administrative and teacher work stations and servers.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this recommendation and is ensuring the standardization of technology at all district locations.

2. IMPROVED OVERSIGHT OF TECHNICAL STAFF HAS RESULTED IN GREATER OVERALL COMPLIANCE WITH DESKTOP AND NETWORK SECURITY

Previous audits showed that some technical support staff was unaware of policies and procedures necessary to comply with the M-DCPS Network Security Standards. Due to the reorganization described in the Background section of this report, technical staff now report to ITS. This realignment placed the delivery of technical support provided to schools directly under the District's IT Management staff. This step has resulted in resource centralization, significantly improved oversight of support staff, and the ability to deploy technicians where they are most needed. Furthermore, technicians can communicate more effectively with technical management who understand and frequently deal with resolving technical demands at school sites.

RECOMMENDATION:

2.1 None

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with the narrative provided in the Internal Audit Report for ISS Area IV.

MANAGEMENT'S RESPONSE

MEMORANDUM

June 14, 2012
DK #50/2011- 2012

TO: José 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 AND SYSTEMS SUPPORT (ISS) AREA IV- SELECTED SCHOOL SITES**

Below are the Information Technology Services (ITS) responses to the three items on the Infrastructure and Systems Support (ISS) AREA IV selected school sites field audit. ITS is very proud of earning an exception-free audit and although difficult to sustain, we have enhanced standards and processes throughout the year to ensure continued successes. It should be noted that it is very difficult to maintain an absolute, 100% secure environment 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 online 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 this audit was the fifth set of schools audited, in a series of six School/Service Area audits. The previous four sets of school audits, which included Area I, Area II, Area III, and Area V, each contained a number of exceptions. Due to the reorganization of School-Based Technicians (SBTs) and ITS' continuous effort to standardize technology at all schools, Area IV Schools' Audit encountered no audit exceptions. Nevertheless, ITS and the SBTs 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.

Since the beginning of the school based "Field Audits," ITS has incorporated monthly meetings with all SBTs, where procedures and standards are reviewed. Said meetings are called ***Operations Review*** and in order to keep all SBTs updated, audit findings and issues as well as security procedures were discussed with all SBTs.

RECOMMENDATIONS:

1.1 Continue moving towards centralized management and standardization aimed at protecting Administrative and Teacher work stations and Servers.

RESPONSIBLE DEPARTMENT: Information Technology Services
MANAGEMENT'S RESPONSE:

Audit Finding:

- None

ITS Audit Response:

- ITS concurs with this recommendation and is ensuring the standardization of technology at all district locations.

2.1 None

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- None

Audit Response:

- ITS concurs with the narrative provided in the Internal Audit Report for ISS Area IV.

3.1 ITS should consider utilizing the similar methodology and processes used to achieve compliance with the M-DCPS NSS within ISS Service Area IV.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE:

Audit Finding:

- None

Audit Response:

- ITS concurs with this recommendation and has implemented similar methodologies and process for all ISS School/Service Areas.

DK:jp

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

2. CONSIDER EMULATING ISS AREA IV METHODOLOGY AS A MODEL TO BE APPLIED DISTRICT-WIDE FOR USE IN COMPLIANCE WITH THE M-DCPS NSS AND INDUSTRY BEST PRACTICES

As the fifth audit in this series, various trends resulting in findings for other ISS Service Areas were not found in ISS Service Area 4. For example, 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. Some previous audits showed an unacceptable number of endpoints that were not part of "the family". All computers sampled within ISS Area 4 were members of the required domain, hardening school site network security and complying with previously issued external and internal auditors' recommendations.

RECOMMENDATION:

3.1 ITS should consider utilizing the similar methodology and processes used to achieve compliance with the M-DCPS NSS within ISS Service Area IV.

RESPONSIBLE DEPARTMENT: Information Technology Services

MANAGEMENT'S RESPONSE: ITS concurs with this recommendation and has implemented similar methodologies and process for all ISS School/Service Areas.

MIAMI-DADE COUNTY PUBLIC SCHOOLS ANTI-DISCRIMINATION POLICY

Federal and State Laws

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In Addition:

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

Revised: (07-11)

INTERNAL AUDIT REPORT

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

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