



# AUDITOR GENERAL

WILLIAM O. MONROE, CPA



## MIAMI-DADE COUNTY DISTRICT SCHOOL BOARD Information Technology Audit

### SUMMARY

The Miami-Dade County District School Board (District) Information Technology Services office (ITS) administers and delivers infrastructure and application support to the District. Our audit focused on evaluating management controls and selected information technology (IT) functions related to ITS during the period February 2004 through May 2004, including selected general controls; determining the effectiveness of management’s configuration policies and procedures for promoting a secure network infrastructure; and determining management’s assessment of Health Insurance Portability and Accountability Act of 1996 (HIPAA) applicability to the District and evaluating the effectiveness of selected IT-related actions taken to promote compliance with HIPAA.

Certain deficiencies were noted in the District’s management controls over selected IT functions. Specifically, these deficiencies included:

**Finding No. 1:** The District lacked centralized IT administration controls necessary to ensure that network configuration and security standards and procedures were applied and performed with adequacy, consistency, and appropriateness.

**Finding No. 2:** Improvements were needed in the District’s network management practices.

### BACKGROUND

The District’s wide area network (WAN) included approximately 400 school and administrative sites. WAN connectivity provided the pathway for these client sites to access critical business systems as well as student educational research. The District was guided by a school-based management philosophy wherein each school principal functioned as a site supervisor maintaining all authority and responsibility for his or her school. As such, ITS’ Network Services department was responsible solely for the

administration and support of the ITS core network, including the administrative local area networks (LANs) within the ITS physical work location and the downtown School Board Administration Building location. Microsystems Technicians or Computer Specialists, hereafter referred to as technicians, reported directly to the principal(s) of the school(s) which they serviced. The District continued to support critical business operations and manage resulting data through mainframe-based legacy systems.

**Finding No. 1:**  
**Centralized Information Technology Administration**

Effective security and management strategies are coordinated across the enterprise with all components of a WAN managed as a cohesive unit. The danger of security dilution exists in decentralizing computing without making an appropriate commitment in resources and training. Security and management strategies must be coordinated across the enterprise. Leaving network administration functions to untrained personnel positioned at low organizational levels and isolated from one another and from management support will likely result in inefficient and ineffective network configuration and security.

Under the District's WAN structure, each school existed as a separate site and child domain on the network. The child domains functioned as LANs administered individually by a technician. Each school-site network was under direct administrative supervision and control of the principal serving the school.

The District's Network Security Standards addressed standards and responsibilities for network administration, including data and physical security controls. While ITS provided technical guidance and support to technicians as requested, the District had not instituted a formal technician training program for execution of its standards and procedures.

The Network Security Standards existed as a living document with ITS primarily responsible for review and revision of the standards to ensure adequate protection of the District's data. However, ITS did not retain official responsibility for or control of the daily operation of school-site networks. While ITS periodically scanned these networks for vulnerabilities, the District did not have measures in place to ensure that each network was configured and managed in accordance with stated standards such as user account administration, prescribed security settings, and data back-up requirements.

Reliance was placed on the school principals for ensuring that all policies were observed and that all policies and staff security responsibilities were known by authorized staff and users. The standards defined acceptable use, password configuration and control standards, and use of lock-out mechanisms specific to users. However, the District had not instituted a formal, structured method of directly disseminating new and revised standards applicable to user responsibility, including written acknowledgement of accountability for compliance.

During our fieldwork, the District was in the process of preparing for a reorganization of its Active Directory Services (ADS) structure whereby each school-site network would be configured as an organizational unit under a single domain controlled by ITS. ITS would then extend a more centralized management philosophy by controlling all employee accounts, including creation, deletion, and policies related to these accounts. Additionally, ITS was developing templates for domain group policies to be used by school sites as a basis for their network configuration. While the single domain model required delegation of some local administrative tasks to school and other site administrators, membership in each site administrator group would be determined by and controlled by ITS. The District had also drafted a Security Audit Checklist to be utilized by the Office of Management and Compliance Audits (OMCA), the District's

internal audit function, during the course of its annual school audits. Subsequent to our fieldwork, ITS provided its proposed school site support reorganization plan whereby technicians would be hired and trained by ITS during a probationary period prior to being placed at school sites.

The lack of centralized IT administration diminishes assurance that control procedures, including user training and acknowledgement of accountability, designed to promote a sound, consistent network security posture will be followed. Further, without formal technician training, the risk increases for system-related vulnerabilities and compromise of District equipment, data, and network availability.

---

---

**Recommendation: The District should continue its efforts in promoting centralized control measures to ensure each school site is in compliance with network- and data-related standards, policies, and procedures through implementation of the ADS reorganization plan and OMCA's use of the Security Audit Checklist. Users should be directly informed of security standards required and acknowledge in writing their responsibility for adherence. Specifically, in accordance with ITS' proposed school site reorganization plan, the District should place increased authority with ITS for the hiring, training, and supervision of technicians to ensure a defined level of knowledge, skill, performance, and commitment to user awareness.**

---

---

**Finding No. 2:  
Network Management**

Managing an entity’s network requires identification of and accounting for all IT components, including recovery of, monitoring of, and proper disposal of IT assets.

We noted deficiencies in the District’s network management controls related to recovery planning, identification of network components, monitoring of system events, and disposal of IT assets. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate personnel have been notified of the deficiencies.

**Recommendation: The District should strengthen network configuration management controls to provide increased assurance of the integrity, confidentiality, and availability of the District’s information resources.**

**OTHER MATTERS**

**Health Insurance Portability  
and Accountability Act of  
1996 (HIPAA)**

HIPAA<sup>1</sup> addresses data interchange, privacy, and information security standards for personal health information. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards, privacy, and security. The final Transaction Rule, which contains electronic data interchange standards, was incorporated as a Federal regulation and had a compliance date of October 16, 2002. The final Privacy Rule was incorporated as a Federal regulation and compliance was required by April 14, 2003, and April 14, 2004, for small health plans. The final Security Rule was incorporated as Federal regulation and has a compliance date of April 21, 2005. HIPAA also provides for civil and criminal penalties for noncompliance.

Working with consultants retained to assist the District in analyzing HIPAA legislation, evaluating applicability, and implementing necessary actions for compliance, management determined that the District did not engage in covered HIPAA electronic transactions or activities requiring compliance with either the Transaction Rule or Security

<sup>1</sup> Public Law 104-191

Rule. However, the District determined that it sponsors two small health plans subject to the Privacy Rule compliance requirements. During our audit, we noted that in accordance with the rule, the District had designated a Privacy Officer, distributed Notices of Privacy Practices, developed and documented policies and procedures, and conducted training of appropriate personnel. The District further noted that it would continue to monitor its activities related to protected health information and, in the event circumstances change, take necessary steps to ensure compliance.

---

---

### **OBJECTIVES, SCOPE, AND METHODOLOGY**

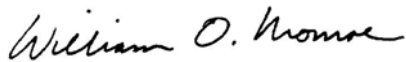
---

---

The objectives of this IT audit were to determine the effectiveness of selected District IT controls; to determine the effectiveness of management's configuration policies and procedures for promoting a secure network infrastructure; and to determine management's assessment of HIPAA applicability to the District and evaluate the effectiveness of selected IT-related actions taken to promote compliance. Our scope focused on evaluating management controls and selected IT functions during the period February 2004 through May 2004. In conducting our audit, we interviewed appropriate District personnel, observed District processes and procedures, and performed various other audit procedures to test selected IT controls.

**AUTHORITY**

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.



William O. Monroe, CPA  
Auditor General

**DISTRICT'S RESPONSE**

In a letter dated August 27, 2004, the Superintendent provided responses to our preliminary and tentative findings. This letter is included in its entirety at the end of this report.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Heidi Burns, CPA\*, CISA, and Vikki Mathews and supervised by Nancy Reeder, CPA\*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA\*, CISA, Audit Manager, via e-mail at [joningram@aud.state.fl.us](mailto:joningram@aud.state.fl.us) or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (<http://www.state.fl.us/audgen>); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

\*Regulated by State of Florida.





**Miami-Dade County Public Schools**

*giving our students the world*

**Superintendent of Schools**  
Rudolph F. Crew, Ed.D.

**Miami-Dade County School Board**  
Dr. Michael M. Krop, Chair  
Dr. Robert B. Ingram, Vice Chair  
Agustin J. Barrera  
Frank J. Bolaños  
Frank J. Cobo  
Perla Tabares Hantman  
Betsy H. Kaplan  
Dr. Marta Pérez  
Dr. Solomon C. Stinson

August 27, 2004

Mr. William O. Monroe, CPA  
Auditor General, State of Florida  
G74 Claude Pepper Building  
111 West Madison Street  
Tallahassee, Florida 32399-1450

**SUBJECT: REVISED RESPONSE TO MIAMI-DADE COUNTY DISTRICT SCHOOL BOARD INFORMATION TECHNOLOGY AUDIT**

Dear Mr. Monroe:

Thank you for the opportunity to respond to your draft report(s) dated July 13<sup>th</sup>, 2004 on information technology at Miami-Dade School District. Below, we will address the procedural and organizational issues that you have identified. But first, I would like to express our pleasure that there were no 'Critical Issues' identified by your auditors.

**Finding No. 1: Centralized IT Administration Controls**

**Management Response:** The security model for our mainframe computer operations has served the District well over time. It authorizes and limits access to appropriate/authorized users for applications. We believe we can emulate it closely in "Active Directory". Our current security model has advantages in that it enables a local administrator (in the case of the schools, the principal or his/her designee) to assign authorizations to their users. The principal, or his/her designee, is responsible for and knows their staff's level of authorization.

Information Technology Services (ITS) recently updated and formalized the District's network rules and regulations and distributed Network Security Standards. ITS will soon establish a process whereby all employees will acknowledge receipt and understand the network rules and security standards.

ITS further acknowledges that past technician training has lacked some degree of formality, however considerable training, some mandatory, has been made available by ITS to school technicians in the last couple of years. This training includes:

- \* Use of Microsoft's System Update Server (SUS)
- \* Wireless
- \* Windows XP
- \* Windows 2000 Server Essentials
- \* Networking Essentials and Wiring
- \* A+ (technicians) class
- \* Policy Editor and Anti-Virus
- \* Exchange 5.5 class
- \* Windows 2000 Server Advanced

**School Board Administration Building • 1450 N.E. 2nd Avenue • Miami, Florida 33132**  
305-995-1430 • Fax 305-995-1488 • [www.dadeschools.net](http://www.dadeschools.net)

Page 2 of 2

- \* Installation and use of E-Policy Orchestrator (EPO), the district's anti-virus application for McAfee (all school techs and principals received this training).

Additionally, your recommendation for more centralized control over technicians was already underway prior to your review. Beginning this school year a hiring and mentoring plan for new and existing technicians will ensure that new technicians are technically qualified to be hired and existing technicians are qualified to hold their existing positions. ITS is developing a management model that will provide procedural and operational controls of the schools and technicians.

#### **Finding No. 2 District Network Practices**

*Management Response:* ITS has demonstrated to your auditors its plan for the District's systems restoration. The plan is now complete and will be reviewed by all system stakeholders including all of my direct reports. We plan to award a contract by July 31st, 2004 to adequately address this item.

Our current Network Security Standards require that prior to disposing of a computer, data and applications must be erased from the hard drives. It should be noted that this was already being done as a matter of course for all computers purchased through the Ed-Fund, an agency that refurbishes the District's used computers. Subsequent to your review this procedure has been implemented at Stores & Distribution. ITS will work with all offices concerned to be sure that this policy is being adhered to.

ITS is currently piloting a product that has shown promise in addressing your concerns in identifying network components. The product, a software package, is called "Big Fix." "Big Fix" has so far demonstrated an ability to itemize computers on the network. It was originally intended to handle operating system patch management automatically without user intervention by identifying operating system vulnerabilities and pushing updates to each machine. We have found, however, that it may provide many other benefits. Among these are:

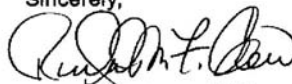
- It provides centralized management of school and departmental servers and related desktops.
- It works with a network scanning tool we use called "Retina" to identify all network components (servers and workstations).
- It identifies all software and vulnerabilities on each of those components, not just the operating system.
- It provides information about software use that will allow locations to track potential licensing violations.
- This same functionality also allows us to identify "cracked" software, games, peer-to-peer programs and other prohibited applications.
- It allows us to push fixes, data and "in-house" applications to the server and desktop level for all the hardware and software piloted thus far.

A different, and very promising suite of products ITS is currently researching from Quest software (formerly Aelita) will provide a complete event logging package, Active Directory reporting and network monitoring applications as well as the Microsoft Exchange migration tool.

We expect that all of these "state-of-the-art" networking tools will allow the School District to maintain the highest standard of due diligence in network administration to ensure adequate monitoring, transaction review and follow up of detectable violations.

Thank you again for the opportunity to respond to your observations. I look forward to a close working relationship as we move forward.

Sincerely,



Rudolph F. Crew, Ed.D.  
Superintendent of Schools

RFC:js  
L154(R144)

cc: School Board Members  
Ms. Ofelia San Pedro  
Ms. Deborah Karcher