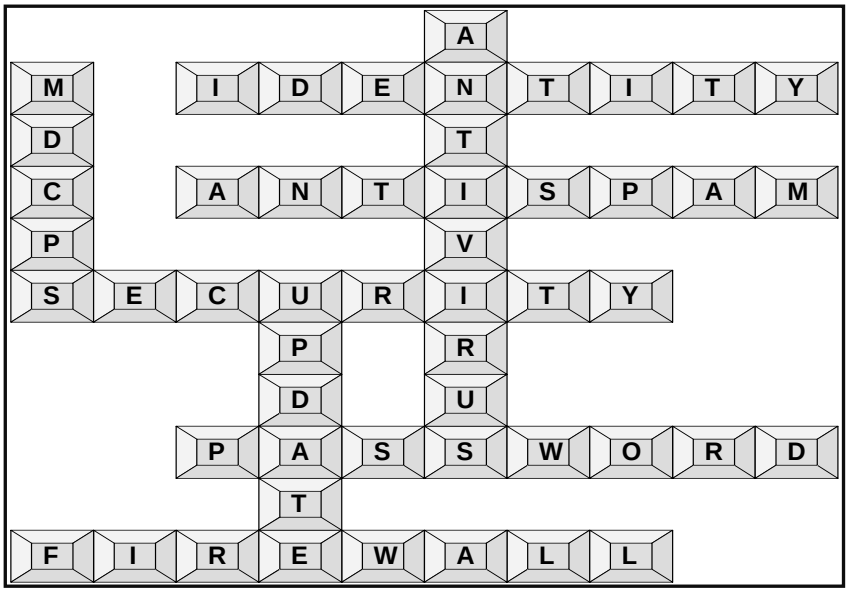
Internal Audit Report

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

ADMINISTRATIVE OFFICES NETWORK AND INFORMATION SECURITY AUDITS – SCHOOLS POLICE



Adherence to current Network Security Standards would reduce the risk of loss of critical information and improve network security

March 2011

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA

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

Mr. Alberto M. Carvalho
Superintendent of Schools

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

Contributors to This Report:

Audit Performed by:
Mr. Luis Baluja
Ms. Dina Pearlman, CISA, CIA

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

Supervised by:
Mr. Trevor L. Williams, CPA

Miami-Dade County Public Schools
giving our students the world

Superintendent of Schools
Alberto M. Carvalho

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

March 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 performed an audit of the Miami-Dade County Schools Police Department – Information and Network Security.

Our audit concludes that, while significant progress in technology and software security has been made since the new Chief of Police took office, closer adherence to the M-DCPS Network Security Standards and proper attention to network and computer maintenance would significantly reduce the potential risk of data loss in the district.

Our findings and recommendations were discussed with management. Their responses along with explanations are included herein. General concurrence by management and the auditors with the findings and recommendations were achieved. However, there were some responses from management that required further clarification. We have made such clarifications, specifically to management's responses to Recommendations 1.1, 1.2 and 3.1. We would like to thank management for the cooperation and courtesies extended to our staff during the audit.

Sincerely,

José F. Montes de Oca

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Miami-Dade County Schools Police Department (also referred to as M-DSPD and Schools Police) is entrusted to provide essential security for the students and staff of the Miami-Dade County Public Schools system. They use a sophisticated computer software system that is linked to the Florida Department of Law Enforcement (FDLE) to accomplish their mandates. All databases are housed at Information Technology Services (ITS) and protected by core security systems. Each officer has a laptop computer and uses wireless technology to access the Dadeschools and the FDLE networks.

Our audit objectives were to assess the level of information security afforded to students and employees by Schools Police information systems. In order to best meet this objective, our audit reviewed the current network and information security practices in the department. It focused primarily on compliance with established Miami-Dade County Public Schools (M-DCPS) Network Security Standards (NSS) and Information Technology (IT) leading practices.

This is the second of a series of network and information security audits being conducted in the District's administrative offices. We also acknowledge that network and information security is a district-wide concern and believe that the conditions reported herein as found in the M-DCPS Police Department are similar district-wide in their occurrence. Hence, collaboration with the District's Information Technology

OVERVIEW OF FINDINGS

- Non-Standard Local Administrator accesses are in use by the department to access 55% of the computers tested.
- Password requirements for certain law enforcement software lack the architecture and complexity typically found in leading practices.
- Accesses granted to district payroll applications (RSTR and PARS) do not always comply with district requirements and best practices.
- Some unit supervisors appeared not to have been appraised of or fully comprehend staff's roles and their limitation to certain software.
- Password-protected timeouts were not used on the majority of the department's computers tested.
- Computer maintenance issues exist, including:
  - Inadequate staff training;
  - Incomplete domain memberships;
  - Non-existing Organizational Unit (OU) in Active Directory;
  - The district's computer management software or updated antivirus software not installed on all computers; and
  - Improper computer naming conventions.

Services (ITS) department in addressing these conditions, both within Schools Police and the District as a whole is recommended.

Our findings indicate that Schools Police administrators and staff take information security seriously. However, improvements can be made to adhere to and to monitor the specific technology rules of M-DCPS. In some cases, not having full awareness of, or training with current Network Security Standards and leading practices may lead to an increased risk of data compromise or loss.

Additionally, staff shortages in both ITS and Schools Police have created a situation that may lead to potential breaches of security. With that said, our review did not disclose any security breaches to critical data or to the District's network. There is currently only one technology staff member in Schools Police. This staff member is tasked with maintaining the specialized law enforcement software in use by the Police department.

Active Directory (AD) is an organizational structure for both computer and user accounts. There is no Schools Police Organizational Unit (OU) in Active Directory for the proper organization and maintenance of Schools Police computer accesses. Many Schools Police computers are currently filed with the Maintenance Department OU. Others are scattered throughout the records. The single staff member responsible for IT resources does not have administrative access to manage AD and properly organize this equipment. There is no Schools Police Site Network Administration group (Admin Group) so he also does not have administrative access to the department's computers. Other than administration of the specialized law enforcement software, the Schools Police department depends on ITS support for maintenance of the computers and network security structure. Due to its own staff shortages, ITS has been unable to provide complete support to Schools Police systems.

We made 10 recommendations to correct control deficiencies and improve computer and network security in the Schools Police department. The detailed findings and recommendations begin on page seven.

INTERNAL CONTROLS

The charts below summarize our overall assessment of the network and information security controls in place in the Miami-Dade County Schools Police Department.

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 reliable.**	**Data systems are mostly accurate but can be improved.**	**Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions.**
External Risk	**None or low.**	**Potential for damage.**	**Severe risk of damage.**

BACKGROUND

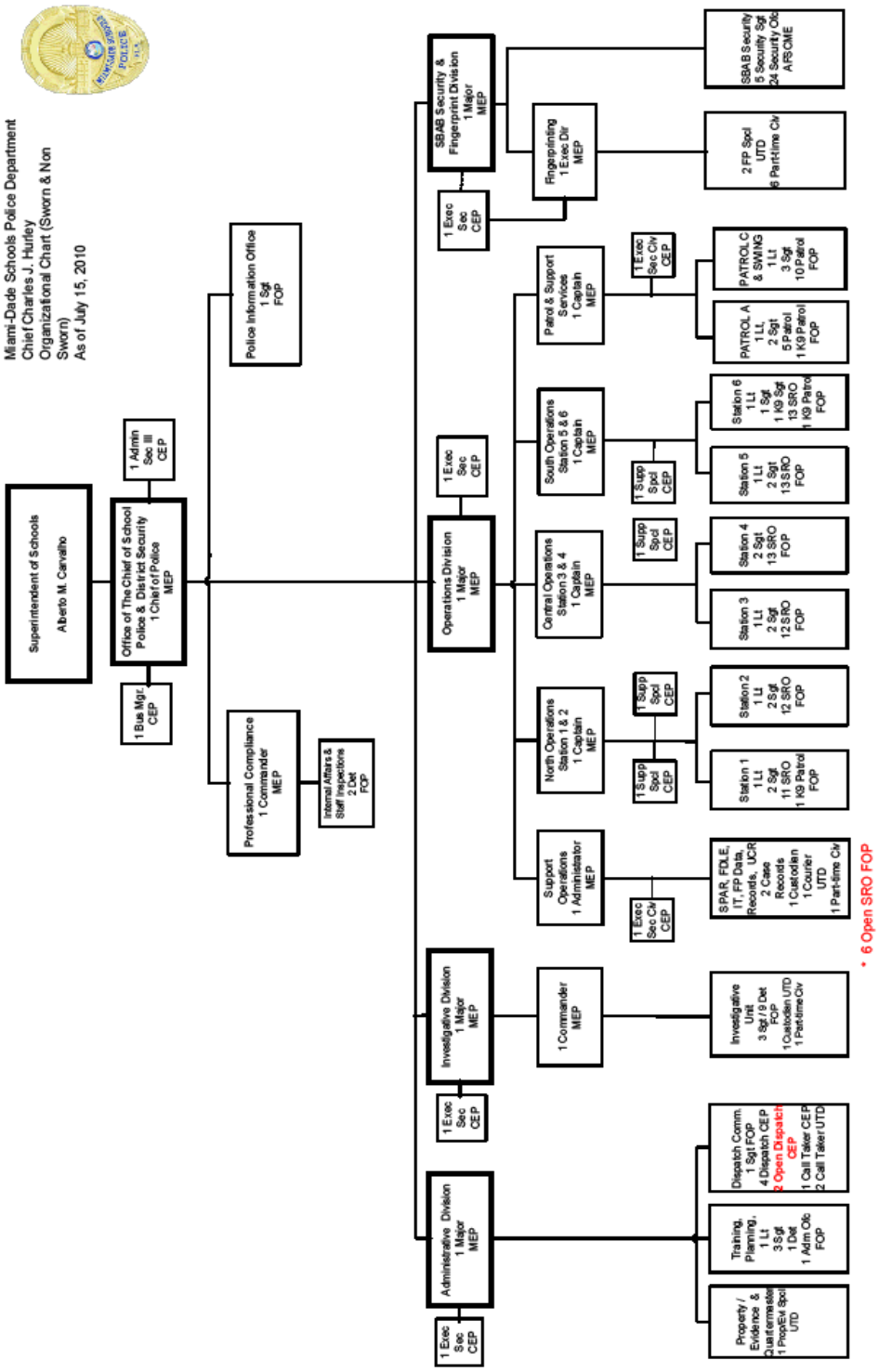
The Miami-Dade Schools Police Department (M-DSPD) has an authorized force of approximately 150 sworn law enforcement personnel. The current organizational structure is presented in the organizational chart on page 5. The department is organized into 11 work locations, including Central Administration, the School Board Administration Building (SBAB) Security and Fingerprinting, Internal Investigations, Patrol, support operations and six remote stations for school resource officers.

The current Chief of Police began serving in this capacity in 2008. The department has one technology staff member who is responsible for maintaining the specialized law enforcement software and the computers and equipment used in the department.

Beginning in 2005 the department converted its reporting, overtime management, and dispatching systems from paper-based, hand written systems to 100% computer-structured systems. This has significantly streamlined and enhanced the efficiency of the reporting process, freeing officer's time for the performance of their primary duties, as well as providing a more equitable assignment structure for overtime duties.

All servers in use by Schools Police are housed, maintained and backed up by ITS and protected as part of M-DCPS core systems. One of the specialized law enforcement software packages used by Schools Police is linked to and secured by FDLE systems and standards. We did not audit the FDLE systems, and as such, do not issue any conclusions on the security of that system.

Schools Police Organizational Chart



OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with the approved Audit Plan for the 2010-11 Fiscal Year, we have performed an audit of the Miami-Dade Schools Police Department (M-DSPD) information and network security. The objectives of the audit were to determine whether adequate internal controls are in place to protect critical information and whether M-DSPD is adhering to current District Network Security Standards. Our audit covered the current IT security practices in place in the department. We performed the following audit procedures to satisfy our audit objectives:

- Requested that the department complete a site assessment survey of its IT landscape and analyzed the survey results;
- Interviewed Miami-Dade Schools Police Department's staff;
- Examined and analyzed various computer reports such as Resource Access Control Facility (RACF), Active Directory (AD), and BigFix (the District's IT Management Tool);
- Examined and tested a random sample of desktop and laptop computers for compliance with standards; and
- Performed various other audit procedures as deemed necessary.

We conducted this compliance 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, 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, based on our audit objectives. This audit included an assessment of applicable internal controls and compliance with the requirements of policies, procedures and rules to satisfy our audit objectives.

FINDINGS AND RECOMMENDATIONS:

As M-DCPS moves from storing and transferring sensitive information used within M-DCPS in a "closed" network architecture utilizing private and/or leased lines to an "open" network architecture using the Internet and TCPIP/IP network, employees must pay particular attention to the security of these assets. The security must include both physical and logical layers of protection.

There are a number of controls in place to assure security of M-DCPS processes. These include the Network Security Standards (NSS), State statutes, Federal regulations, and software controls built into the information systems. Departmental senior administrators are ultimately responsible for enforcing these controls, granting access to sensitive data and programs, and informing authorized staff and users of these policies and staff's responsibilities (NSS 5.0.10, 5.0.11 and 5.0.12).

1. ADMINISTRATIVE RIGHTS ON LOCAL MACHINES AND PASSWORD ISSUES IN SPECIALIZED ACCESSES

The M-DCPS NSS 4.1.1.13 states: *"Access to critical resources should be managed by assigning individuals to a group. The group should be set up with the authority necessary to do the specific job/task or access specific data... Group membership should be reviewed on a regular basis to ensure all members are appropriate. Under no circumstances should users be assigned data folder or application rights as an individual, except for home folders."*

1.1 Non-standard personalized and generic Local Administrator account accesses are in use in the department

The standard method outlined for login into District computers requires the user to provide a user ID and personalized password. This process grants access to computer and network resources based on permissions that have been applied to a user's account by the network administrator through membership in an Administrative Group. Through this method, computer and network activity is easily traceable to the specific user, and privilege levels can be assigned and maintained easily through levels set for the specific group (or groups) of which the individual is a member.

District computers may also be accessed through a Local Administrator (LA) account. An LA login is a powerful account, which allows a user unrestricted access to the computer. Typically, LA accounts are restricted to the "Administrator" account provided

with the operating system, and the "dadeschools" network group that has LA rights granted as part of it's access definition. Membership in this group is generally granted only to the network manager and site technology support personnel, and is used to install/uninstall software and hardware, and for troubleshooting purposes. In some cases, Local Administrator rights are granted to the individual who works on the specific computer. In those instances, the Local Administrator account should be via that individual's employee ID and network access. During the normal course of operations, an individual should sign on to his/her computer via his/her "dadeschools" account, rather than directly through another account. Direct access should only be allowed to correct network access or hardware issues in the individual computer.

Twenty-Five of the 45 department computers (55%) physically checked by the auditors had non-standard individual login ID's and a Local Administrator group account with a generic login ID (e.g., "GUEST". Officers routinely logged into their laptop computers using the generically named LA account, which was originally created to resolve a technical issue, as well as to simplify the login process, rather than logging in using their personalized official user ID.

Having a large number of individual users (i.e., officers) login into District computers through this generically name LA account significantly increases the risk of allowing unlimited access to confidential information to individuals who are not authorized to have such access. It also introduces the potential for each user to knowingly or unknowingly reconfigure computer and network settings. Moreover, in addition to being out of compliance with the NSS, this method is not an industry best practice.

Three (6%) additional computers in our sample had administrative access login ID's other than those described above that did not comport with the login naming protocol delineated in the NSS.

1.2 Log-on to one of the specialized law enforcement software does not require standard password of specific length, complexity and frequency of password reset.

Information Technology best practices for password management typically require that password be a specify length (e.g., at least 8

characters), complexity (e.g., alpha and numeric characters), and reset frequently (e.g., every 90 days).

We noted that currently, users logging on to the specialized Computer Aided Dispatch (CAD)/Records Management Systems (RMS) law enforcement software used by Schools Police are not required to reset their password at specific time intervals. Using a static password increases the potential risk that an individual who has obtained knowledge of a static password, which disclosure has been unknowingly compromised, could have continued unauthorized access to the system and not locked out within a time period. Limitations with the existing version of this application require manual configuration and password management by the department's network administrator for each user account.

RECOMMENDATIONS:

1.1 Standardize employees' account user ID to comply with the current Network Security Standards and require all employees to log into the network using their official user ID. As part of this standardization process, the generically named Local Administrator account should be removed from the local computers. Due to the unique environment within the M-DSPD, this recommendation should be thoroughly tested prior to implementation.

Responsible Department: Miami-Dade County Schools Police

Management's Response: The Local Administrator (LA) login does not grant access to critical District network resources, nor does it have network administrator rights. Miami-Dade Schools Police Department (M-DSPD) police reports are encrypted, so there are no noted vulnerabilities.

On Wednesday, February 16, 2011, members from Office of Management and Compliance Audits (OMCA), M-DSPD and the Office of Information Technology Services (ITS) met to discuss the testing of an alternative laptop configuration login process that would meet the recommended preference of OMCA. While the current practice is not a violation of any Florida Department of Law Enforcement (FDLE) standards, it is not considered a best practice. M-DSPD will work with OMCA and ITS personnel to explore this process. Should the testing confirm the recommendation can be implemented, and not violate FDLE standards, create an even greater breach of security or significantly increase the level of technical support beyond that which is available, M-DSPD will adopt and implement this process.

Auditors' Comment:

As already stated, the Local Administrator's (LA) login is a powerful account, which allows a user unrestricted access to the local computer. While not giving direct access to the network, the LA account allows the user to make specific changes to the local machine settings or to install spy software. Using these changes, an unauthorized individual may in fact be able to record and transmit access information to an outside location. Additionally, an authorized but not technically proficient user may inadvertently make changes that compromise network security.

1.2 Login password to specialized Police application(s) should require periodic changes and minimum complexity requirements to meet IT industry password management standards.

Responsible Department: **Miami-Dade County Schools Police**

Management's Response: M-DSPD currently meets and exceeds the requirements set forth by FDLE. The Department recently completed an audit by FDLE, which was provided to OMCA. The audit findings, which entailed password security and user access, indicated a one-hundred percent compliance rating.

M-DSPD utilizes specialized law enforcement software, which is scheduled for normal routine maintenance updates in June, 2011. During these updates, the vendor will be upgrading the password complexity to conform to emerging Federal standards and best practices. This action will position the specialized law enforcement software used by M-DSPD in alignment with the District's own network requirements and standards.

In reviewing M-DCPS NSS 5.0, *Staff Security Responsibilities,* and 5.1, *User IDs and Passwords,* there are no requirements governing vendors that have not been met.

Auditors' Comment:

We acknowledge that the FDLE application systems used by the M-DSPD recently underwent a security compliance audit, performed by another agency, and were deemed to be compliant. However, as a point of clarification, the specialized law enforcement application referenced in our audit finding is not the application that was recently audited by the other agency and is different from the FDLE application referred to above.

As a further point of clarification, the M-DCPS NSS stresses the need to secure the District's systems and data from internal and external threats. The NSS 4.1.2, *Data*

Access, Transfer and Communication, requires new purchased software that handles confidential data to meet the security capabilities documented in section 5.1 of the NSS.

2. INCOMPATIBLE PAYROLL DATA ENTRY AND APPROVAL ACCESS ISSUES

The segregation of work responsibilities is a fundamental control in preventing abuse and possible fraud. Without adequate segregation of duties and monitoring of role assignments for conflicts, the risk is increased that one person could circumvent internal controls.

In the case of entering and approving the payroll, both the Network Security Standards (Section 4.1.4.1) and the Payroll Processing Procedures Manual (Chapter 3) mandate strict limits on the quantity, job roles, and administrative levels of authorized personnel.

Since the current Chief of Police took office, a commendable effort has been taken to reduce the conflicting software accesses and to control future assignments. However, there are still some issues that need to be further addressed:

2.1 Access was granted to RSTR to individuals below the level of Director and some individuals were granted access to both RSTR and PARS.

At the beginning of our fieldwork, our initial review of access rights assigned to employees within Schools Police disclosed that there were two employees below the Director level with access to Payroll Approval (RSTR). Also, four of 11 departments had multiple employees in addition to the Chief of Police with both RSTR and PARS access.

Before concluding our fieldwork, RSTR and PARS accesses were checked again and there was still one individual below the Director level with RSTR access. Additionally, there were then six departments (an increase of two departments) having multiple employees in addition to the Chief of Police with both RSTR and PARS access. This is a role conflict, allowing the same individual to both enter employee time and approve payroll.

We are aware that due to programmatic limitations with the legacy mainframe software, the Senior Authorization and Access Administrative Application (AAAA) Administrator of each work location needs to have access to both the Payroll Time Records – PARS and Payroll Approval – RSTR applications in order to grant access to his/her employees. This is a level of risk the District has accepted. However, although there are software controls embedded in the program that prevent a single individual from

both entering and approving the same payroll information, these controls can be more easily circumvented with an increased number of employees having this dual access.

2.2 In some cases, individuals in Schools Police whose jobs do not include entering personnel time were granted access to PARS.

In one department, 10 of the 18 employees (56%) have PARS access. Job titles of these individuals included three executive secretaries, a Police Major, a Police Commander, a Supervisor of Police Support Ops Personnel, a Senior Fingerprint Technician, and three Community Liaison Specialists. Most of these employees do not perform payroll time input as part of their job function; therefore, they have no need for this access.

The district uses the network security standard concept of "least privilege" (NSS 4.0) for access to all system level resources such as databases. "Least privilege" is defined as a default of no access to these resources and the requirement of explicit permission and authorization based on need.

2.3 Individual Schools Police unit supervisors do not appear to have been apprised of the role requirements that limit access to certain software.

The M-DCPS NSS 5.0.12 states*: "Site supervisors are also responsible for informing authorized staff and users of these policies and staff security responsibilities. In addition, site supervisors are required to review and retain a signed copy of the most recent RACF report showing that the authorizations held by site staff are appropriate, especially in regard to high risk authorizations..."*

One department supervisor requested inappropriate accesses for employees in her department. This condition resulted when the department was moved from one location to another location under Schools Police. Upon the move, security accesses for all employees in the department were terminated. The department supervisor requested that all previously assigned network accesses be reassigned under the new location. Some of the accesses granted to some of the employees, although previously granted under the

old location, were inappropriate at the new location and presented some security issues.

RECOMMENDATIONS:

2.1 Review Software accesses on a monthly basis and maintain a signed copy for the records. This review should encompass ensuring that only employees at the appropriate level are given payroll approval authorization and that only the senior AAAA Security Access administrator has both RSTR and PARS access, in order to grant these accesses to appropriate personnel.

Responsible Department: Miami-Dade County Schools Police

Management's Response: Immediately upon assuming command of the agency in August 2008, this was one of the first areas of the Department which was identified as a concern and immediately addressed. Shortly thereafter, a request was sent from the Office of the Chief of Police to the ITS apprising their staff that all requests for the granting of modules must be approved by the Chief of Police. M-DSPD provided those correspondences to OMCA. It was discovered that there were some requests which were inadvertently granted without the appropriate authorization. These have since been revoked.

With the implementation of the new ERP/SAP system, the Department has only two Quad A security administrators for eleven work location codes. Within one of those work locations is the District's Office of Fingerprinting, a division with joint functions between the police department and Office of Human Resources. There are also several other functions within the agency and some of its work locations where certain functions are merged e.g., Office of the Chief of Police, Internal Affairs, etc. The roles described in the audit finding do not present a conflict.

In the instance of a Department supervisor requesting "inappropriate" accesses for employees within her area; this occurred immediately after a reorganization of the agency. Had the request from the Office of the Chief of Police to ITS been followed, this request would have been rejected. Nonetheless, this finding is valid yet not systemic, and will be addressed through a monthly review process (*Administrative Directive CJH#11-01Monthly Access Report*), which has been issued to affected staff (attached).

M-DSPD has scheduled a training session for the aforementioned Monthly Access Report procedures in April 2011, and will implement an annual refresher at the start of each school year, directing all personnel to review the District's current NSS.

2.2 Review each employee's job functions and network security accesses and ensure that employee's security accesses are appropriately matched to their job functions. Employees should be granted access only to specific software required for them to carry out their assigned duties.

Responsible Department: **Miami-Dade County Schools Police**

Management's Response: See the department's response to Recommendation 2.1.

2.3 Develop a process to periodically inform senior administrators of district network security standards and policies, especially in regards to software access levels and approvals.

Responsible Department: **Miami-Dade County Schools Police**

Management's Response: See the department's response to Recommendation 2.1.

3. PASSWORD PROTECTED TIMEOUTS ARE NOT CONSISTENTLY IN USE ON DEPARTMENT COMPUTERS

The M-DCPS NSS 4.1.1.10 states: *"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. Users should also be in the habit of locking their computer or logging off when they are finished or leaving the computer unattended, even for a brief time..."*

Additionally, M-DCPS NSS 5.1.3 states*: "Users are responsible for all activity associated with their user-id. When a user is finished using a computer or will be leaving the computer unattended, they must log off or lock the computer (CTRL-ALT-DELETE, Lock Computer) to prevent their account from being compromised."*

3.1 Password-protected timeouts are not consistently being used by the department.

We examined 27 desktop computers dispersed throughout eight Schools Police sites and found that while password-protected timeouts were manually set on eight (8) of these computers (30%), the remaining 19 computers (70%) did not have password-protected timeouts set. We also examined 15 laptop computers dispersed to officers throughout the eight Schools Police sites and found that all 15 laptops (100%) did not use password-protected timeouts. The reason given for officers not utilizing password-protected timeouts was that when driving or during an emergency, having the screen unavailable for immediate viewing could create a safety issue. However, the content on the laptop screen, which might be highly sensitive, is viewable to anyone while the vehicle is in the parked position and especially when the vehicle is unattended.

RECOMMENDATION:

3.1 Implement an Active Directory Organizational Unit (OU) rule that sets password protected timeouts for all departmental computers where that timeout would not affect officer or student safety.

Responsible Department: Miami-Dade County Schools Police

Management's Response: It is the position of the M-DSPD that the District revisit M-DCPS NSS 4.1.1.10 as it applies to screen timeouts and password issues applying to School Police mobile laptops. Exceptions have been granted to police officers with mobile communications devices in motor vehicles, and the same should apply with police mobile laptops. M-DSPD laptops do not currently have this function activated, and the Department will not implement a password protected screen timeout. The laptops utilize a screen timeout, which will continue to be our practice. The Department's Standard Operating Procedure, Administration 11.3, Data Access Devices, has been revised to direct sworn personnel to lower or tilt the laptop screen while not in the vehicle (attached).

There are numerous driving hazards and distractions that a password protected timeout would pose to sworn personnel if implemented on the laptop devices. The likelihood of information being compromised by a person peering into the vehicle from the outside, or in police custody is remote, particularly when compared to ensuring safe vehicle operations.

The implementation of screen timeouts and passwords, as it relates to M-DSPD workstations, will be put into practice upon receiving additional support from ITS in conjunction with finding #4 below.

Auditors' Comment:

In framing our audit recommendation, we were sensitive to safety concerns involving officers' interaction with his/her laptop while driving. As such, we have recommended that any measure implemented by management must consider, and by extension, assure the safety of the officer or student. Management's proposed action regarding safeguarding information visible on officer's laptop screen is welcomed and appreciated. However, the need to protect similarly sensitive information displayed on the screens of desktop computers through an Organizational Unit (OU) policy is a desired outcome.

4. COMPUTER MAINTENANCE ISSUES

There is currently no trained individual assigned responsibility for providing standard computer support to the Schools Police departments. ITS is depended on to provide basic technology support but there is no specific group or individual tasked for Schools Police department computer support. Computers sent to ITS for imaging services are being received back by the department without basic issues being resolved. These newly-imaged computers are not being joined to the Dadeschools domain, have BigFix or Sophos installed, or had the generic image name properly changed and assigned in Active Directory.

This disconnect in support assignment has played a role in the issues described below. It should be noted that some of the computers in the subsets are affected by multiple issues.

4.1 Schools Police technical support staff was not trained in ITS systems management function.

The supervisor for technical support for Schools Police is tasked with maintaining the specialized law enforcement software used in the department. He has had no training in, or access to the administrator roles in individual computers or in Active Directory. He is not familiar with internal network protocols. He can place, but not respond to HEAT tickets. No other technical support personnel is assigned to this department.

4.2 Some Schools Police computers are not members of the "dadeschools" domain.

The M-DCPS NSS 4.1.1.5 states: *"All locations must migrate from the original school and District networks to the new dadeschools network. Most of these are old networks with weak security and must be removed from production immediately."*

Five of the 45 department computers (11%) we examined were not members of the "dadeschools" domain, as required by the NSS. Not being a member of the "dadeschools" domain deprives these computers of the firewalls and other sophisticated security measures in force for the District network.

4.3 A Schools Police Organizational Unit (OU) does not exist in Active Directory

The NSS (4.1.1.3) describes the use and structure of Active Directory Organizational Units (OUs). It places responsibility on the Local OU administrators to strictly limit access to their OU from other OUs as well as the outside. An OU for Schools Police is not in place, and the current technology person in the Schools Police department has no administrative access or rights to Active Directory. Consequently, this employee is not able to carry out his responsibility of effectively managing and maintaining Schools Police computers.

4.4 Some Schools Police computers do not have BigFix installed and running or the current Sophos antivirus software and definitions and were not named properly.

The M-DCPS NSS 5.0.17 states: *"District-wide initiatives such as loading anti-virus software, patch management software, user registration in the P-Synch password reset application, spyware detection/removal software, Intrusion Prevention Systems (IPS), power management, wireless WAN management, and migration to the dadeschools domain must be complied with. Future District-wide initiatives may include desktop management. In addition, all computers must be named according to the M-DCPS naming convention, which requires the location number be the first four digits of the name."*

Additionally, the M-DCPS NSS 5.0.8 states: *"Security software (anti-virus programs, patch management software, spyware, and hacking software detectors, domain and local computer policy) should be loaded and running on all computers sharing files over the network."*

Five of the 45 department computers (11%) examined by the auditors did not have "BigFix" management software installed and running. BigFix is the name of the management software selected by the District to run on its computers. The software runs continuously in the background of the computer and provides system updates and protection against computer threats.

Seven of the 45 department computers (16%) we examined did not have Sophos Antivirus software installed and running. Sophos is the antivirus software selected by the District to run on its computers. The software runs continuously in the background of the computer and provides protection against computer viruses.

Twenty-three of the 45 department computers (51%) we examined were not named according to proper naming conventions delineated in the NSS. Further analysis found that the number of computers assigned to the department in Active Directory (AD) did not agree with the number of computers listed by BigFix. For example, our analysis found 423 computers listed in AD and only 184 in Bigfix. This makes them more difficult to locate and manage in Active Directory. BigFix, the District's desktop management software, also uses Active Directory to locate and push security patches and software updates to district computers. The lack of up-to-date security patches could potentially leave the network open to security breaches.

RECOMMENDATIONS:

4.1 Provide the current technology personnel in Schools Police the appropriate training and accesses to enable him to effectively manage the Schools Police organizational unit. Along with training the existing staff, efforts should be made to provide Schools Police the additional standard hardware and M-DCPS network and security technical support by leveraging the pool of ITS-trained technicians.

Responsible Department: **Miami-Dade County Schools Police**
Information Technology Services

Management's Response:

Miami-Dade County Schools Police – There was an initial meeting held on January 19, 2011, with members from M-DSPD and ITS to examine the findings and recommendations of this audit. On Wednesday, February 16, 2011, members from OMCA, M-DSPD and ITS attended a follow-up meeting to discuss the appropriate corrective actions to be taken.

It should be noted that findings 4.1 – 4.4 are outside the current authority of the M-DSPD. As such, ITS has agreed to the following:

4.1 – Provide training to the Department's sole technology administrator/staff member.

4.2 – M-DSPD will be retiring the current inventory of laptop computers, as it has recently been awarded a COPS technology grant to replace the aged and often malfunctioning devices. The discrepancies involving the computers that were not part of the dadeschools domain were as a result of our Department not having the authority to perform this function.

4.3 – ITS has agreed to create an Organizational Unit (OU) for the M-DSPD, and will either designate an ITS representative to administer the OU, or authorize the Department's technology administrator to administer the OU with support from ITS.

4.4 – Once 4.1 – 4.3 are implemented, it is anticipated that compliance with 4.4. will occur.

It is the position of the M-DSPD that both parties collaborate to address these recommendations, and that they be immediately implemented. The District should also consider revisiting the NSS to make sure it meets the needs of the M-DSPD, conduct workshop training and ensure the document remains accessible to all employees.

Information Technology Services – The Police Department is scheduled to bring in 150 new laptops for field use. ITS will work with the Police Technical Staff to analyze how to best create a new Organizational Unit (OU) that encompasses all the Department locations, bring the new laptops into compliance as far as naming and security applications, and set up procedures to keep those laptops in compliance without interrupting police operations.

4.2 Review the department's inventory of computers and ensure that all computers are included in the "dadeschools" domain.

Responsible Department: **Miami-Dade County Schools Police**

Management's Response: See the department's response to Recommendation 4.1.

4.3 Establish and maintain a Schools Police OU in Active Directory and ensure that local administration rights to the OU is given to Schools Police.

Responsible Department: **Miami-Dade County Schools Police**
Information Technology Services

Management's Response:

Miami-Dade County Schools Police – See the department's response to Recommendation 4.1.

Information Technology Services – See the department's response to Recommendation 4.1.

4.4 Bring all department computers into compliance with District Standards by ensuring that the District's approved computer management software and antivirus (currently BigFix and Sophos) are installed on all computers; and that all computers are named according to the NSS naming convention. Further, as this effort is completed, reconcile the department's computer inventory to Active Directory.

Responsible Department: **Miami-Dade County Schools Police**
Information Technology Services

Management's Response:

Miami-Dade County Schools Police – See the department's response to Recommendation 4.1.

Information Technology Services – See the department's response to Recommendation 4.1.

MANAGEMENTS' RESPONSES

MEMORANDUM

CJH/2010-11/#390
March 23, 2011
CJH/305-757-7708

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

FROM: Charles J. Hurley, Chief
Miami-Dade Schools Police Department

SUBJECT: RESPONSE TO INFORMATION AND NETWORK SECURITY/ TECHNOLOGY AUDIT OF MIAMI-DADE SCHOOLS POLICE DEPARTMENT

Attached, you will find the responses prepared by the Miami-Dade Schools Police Department (M-DSPD) regarding the audit of Information and Network Security.

The Department's technology is aged, obsolete, no longer under warranty, and at times, poses a potential risk to the day-to-day functions of the agency. Throughout the years, this critical component of the Department had received very little support, and was left in a state of disarray. Despite these concerns, the system continues to support the 151 officer department.

M-DSPD operates with only one technology administrator/staff member, who deploys over 150 mobile laptop devices; 50 desktop work stations; conducts repairs and provides technical support, often from his residence; supports the Communications and Dispatch Center; provides crime statistics and data analysis; submits mandatory Uniform Crime Reports (UCR) and School Environmental Safety Incident Reporting System (SESIR) reports; and oversees the District's Fingerprinting technology.

I anticipate that many of the recommendations will be addressed with the support of the Office of Information Technology Services, who has kindly agreed to provide assistance. M-DSPD appreciates the input from your staff, as this will lead to an improvement in the delivery of our services to the District.

Should you have any questions or require any additional information, please contact me directly at (305) 757-7708.

/CJH
Attachments (2)

c: Mr. Alberto M. Carvalho
Ms. Deborah Karcher
Mr. James P. O'Donnell
Mr. Trevor Williams
Mr. Craig Rinehart
Mr. Jose Cardelle

Audit Findings and Recommendations for Information and Network Security of Miami-Dade Schools Police Department

1. ADMINISTRATIVE RIGHTS ON LOCAL MACHINES AND PASSWORD ISSUES SPECIALIZED ACCESSES

The Miami-Dade County Public Schools (M-DCPS) Network Security Systems (NSS) 4.1.1.13 states: Access to critical resources should be managed by assigning individuals to a group. The group should be set up with the authority necessary to do the specific job/task or access specific data. Group membership should be reviewed on a regular basis to ensure all members are appropriate. Under no circumstances should users be assigned data folder or application rights as an individual except for home folders.

1.1 Non-standard personalized and generic local Administrator account accesses are in use within the Department.

M-DSPD Response

The Local Administrator (LA) login does not grant access to critical District network resources, nor does it have network administrator rights. Miami-Dade Schools Police Department (M-DSPD) police reports are encrypted, so there are no noted vulnerabilities.

On Wednesday, February 16, 2011, members from Office of Management and Compliance Audits (OMCA), M-DSPD and the Office of Information Technology Services (ITS) met to discuss the testing of an alternative laptop configuration login process that would meet the recommended preference of OMCA. While the current practice is not a violation of any Florida Department of Law Enforcement (FDLE) standards, it is not considered a best practice. M-DSPD will work with OMCA and ITS personnel to explore this process. Should the testing confirm the recommendation can be implemented, and not violate FDLE standards, create an even greater breach of security or significantly increase the level of technical support beyond that which is available, M-DSPD will adopt and implement this process.

1.2 Log-on to one of the specialized law enforcement software does not require standard password of specific length, complexity and frequency of password reset.

M-DSPD Response

M-DSPD currently meets and exceeds the requirements set forth by FDLE. The Department recently completed an audit by FDLE, which was provided to OMCA. The audit findings, which entailed password security and user access, indicated a one-hundred percent compliance rating.

M-DSPD utilizes specialized law enforcement software, which is scheduled for normal routine maintenance updates in June, 2011. During these updates, the vendor will be upgrading the password complexity to conform to emerging Federal standards and best

practices. This action will position the specialized law enforcement software used by M-DSPD in alignment with the District's own network requirements and standards.

In reviewing M-DCPS NSS 5.0, *Staff Security Responsibilities,* and 5.1, *User IDs and Passwords,* there are no requirements governing vendors that have not been met.

2.1 Access was granted to RSTR to individuals below the level of Director and some individuals were granted access to both RSTR and PARS.

2.2 In some cases, individuals in Schools Police whose jobs do not include entering personnel time were granted access to PARS.

2.3 Individual School Police unit supervisors do not appear to have been apprised of the role requirements that limit access to certain software.

M-DSPD Response

Immediately upon assuming command of the agency in August 2008, this was one of the first areas of the Department which was identified as a concern and immediately addressed. Shortly thereafter, a request was sent from the Office of the Chief of Police to the ITS apprising their staff that all requests for the granting of modules must be approved by the Chief of Police. M-DSPD provided those correspondences to OMCA. It was discovered that there were some requests which were inadvertently granted without the appropriate authorization. These have since been revoked.

With the implementation of the new ERP/SAP system, the Department has only two Quad A security administrators for eleven work location codes. Within one of those work locations is the District's Office of Fingerprinting, a division with joint functions between the police department and Office of Human Resources. There are also several other functions within the agency and some of its work locations where certain functions are merged e.g., Office of the Chief of Police, Internal Affairs, etc. The roles described in the audit finding do not present a conflict.

In the instance of a Department supervisor requesting "inappropriate" accesses for employees within her area; this occurred immediately after a reorganization of the agency. Had the request from the Office of the Chief of Police to ITS been followed, this request would have been rejected. Nonetheless, this finding is valid yet not systemic, and will be addressed through a monthly review process (*Administrative Directive CJH#11-01Monthly Access Report*), which has been issued to affected staff (attached).

M-DSPD has scheduled a training session for the aforementioned Monthly Access Report procedures in April 2011, and will implement an annual refresher at the start of each school year, directing all personnel to review the District's current NSS.

3. PASSWORD PROTECTED TIMEOUTS ARE NOT CONSISTENTLY IN USE ON DEPARTMENT COMPUTERS

Audit Findings and Recommendations for Information and Network Security of Miami-Dade Schools Police Department

The M-DCPS NSS 4.1.1.10 states: 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. Users should also be in the habit of locking their computer or logging off when they are finished or leaving the computer unattended, even for a brief time.

Additionally, M-DCPS NSS 5.1.3 states: Users are responsible for all activity associated with their user-id. When a user is finished using a computer or will be leaving the computer unattended, they must log off or lock the computer (CTRL-ALT-DELETE, Lock Computer) to prevent their account from being compromised.

3.1 Password protected timeouts are not consistently being used by the Department

M-DSPD Response

It is the position of the M-DSPD that the District revisit M-DCPS NSS 4.1.1.10 as it applies to screen timeouts and password issues applying to School Police mobile laptops. Exceptions have been granted to police officers with mobile communications devices in motor vehicles, and the same should apply with police mobile laptops. M-DSPD laptops do not currently have this function activated, and the Department will not implement a password protected screen timeout. The laptops utilize a screen timeout, which will continue to be our practice. The Department's Standard Operating Procedure, Administration 11.3, Data Access Devices, has been revised to direct sworn personnel to lower or tilt the laptop screen while not in the vehicle (attached).

There are numerous driving hazards and distractions that a password protected timeout would pose to sworn personnel if implemented on the laptop devices. The likelihood of information being compromised by a person peering into the vehicle from the outside, or in police custody is remote, particularly when compared to ensuring safe vehicle operations.

The implementation of screen timeouts and passwords, as it relates to M-DSPD workstations, will be put into practice upon receiving additional support from ITS in conjunction with finding #4 below.

4. COMPUTER MAINTENANCE ISSUES

M-DSPD currently does not have anyone trained and/or assigned with the responsibility of providing standardized computer support to the School Police. ITS is depended upon to provide basic technology support; however, there is no specific group, unit or individual tasked for the Department to provide computer support. Computers sent to ITS for imaging services are being returned back to the Department without basic issues being resolved. These newly-imaged computers are not being joined to the

dadeschools domain, do not have BigFix or Sophos installed, or had the generic image name improperly changed and assigned in Active Directory. This disconnect in support assignment has played a role in the issues described below. It should be noted that some of the computers in the subsets are affected by multiple issues.

4.1 Schools Police technical support staff was not trained in ITS systems management function.

4.2 Some Schools Police computers are not members of the "dadeschools" domain.

4.3 A Schools Police Organizational Unit (OU) does not exist in Active Directory

4.4 Some Schools Police computers do not have BigFix installed and running or the current Sophos antivirus software and definitions and were not named properly.

M-DSPD Response

There was an initial meeting held on January 19, 2011, with members from M-DSPD and ITS to examine the findings and recommendations of this audit. On Wednesday, February 16, 2011, members from OMCA, M-DSPD and ITS attended a follow-up meeting to discuss the appropriate corrective actions to be taken.

It should be noted that findings 4.1 – 4.4 are outside the current authority of the M-DSPD. As such, ITS has agreed to the following:

4.1 – Provide training to the Department's sole technology administrator/staff member.

4.2 – M-DSPD will be retiring the current inventory of laptop computers, as it has recently been awarded a COPS technology grant to replace the aged and often malfunctioning devices. The discrepancies involving the computers that were not part of the dadeschools domain were as a result of our Department not having the authority to perform this function.

4.3 – ITS has agreed to create an Organizational Unit (OU) for the M-DSPD, and will either designate an ITS representative to administer the OU, or authorize the Department's technology administrator to administer the OU with support from ITS.

4.4 – Once 4.1 – 4.3 are implemented, it is anticipated that compliance with 4.4. will occur.

It is the position of the M-DSPD that both parties collaborate to address these recommendations, and that they be immediately implemented. The District should also consider revisiting the NSS to make sure it meets the needs of the M-DSPD, conduct workshop training and ensure the document remains accessible to all employees.

MEMORANDUM

CJH/2010-11#382
March 22, 2011
CJH/305-757-7708

TO: Distribution

FROM: Charles J. Hurley, Chief
Miami-Dade Schools Police Department

SUBJECT: COVER MEMORANDUM – ADMINISTRATIVE DIRECTIVE #11-01 AUTHORIZED APPLICATIONS FOR EMPLOYEES BY LOCATION REPORT

Attached is Administrative Directive #11-01, *Authorized Applications for Employees by Location Report*.

Upon receipt of this directive, please review as it is effective immediately. A training session will be scheduled for all affected personnel.

CJH/
Attachments: Administrative Directive #11-01, Authorized Applications for Employees by Location Report
Administrative Directive Acknowledgement Log

Distribution: Majors (4)
Captains (4)
Commanders (2)
Lieutenants (8)
Ms. Sigilenda Miles
Mr. Jose Cardelle

MEMORANDUM

TO: Distribution DATE: March 22, 2011

FROM: Charles J. Hurley, Chief of Police
Miami-Dade Schools Police Department

SUBJECT: AUTHORIZED APPLICATIONS FOR EMPLOYEES BY LOCATION REPORT

ADMINISTRATIVE DIRECTIVE #11-01

The Miami-Dade County Public Schools (M-DCPS), Customer Information Control System (CICS) is the means by which District personnel can access various informational applications, e.g., student information, personnel, payroll, SPAR, etc. The information available through CICS is confidential and therefore, restricted to designated personnel. As such, worksite administrators are responsible for identifying, authorizing and monitoring their employees' access to the system. As an example of unauthorized access, personnel with PARS Payroll **Input** access must not have access to PARS Payroll **Approval**, and vice versa. Also, location supervisors must ensure that all officers have access to SPAR, ISIS and PERS applications. In an effort to ensure accountability at all levels, specific procedures have been established.

Effective immediately, all Miami-Dade Schools Police Department (M-DSPD) worksite administrators will review the *Authorized Applications for Employees by Location Report* every 3rd Friday of each month to ensure personnel are assigned the appropriate levels of access. When reviewing the report, site administrators must print and review it to make certain their employees have access to the appropriate applications and also to identify any employees with unauthorized access. On the hard copy, highlight any employees identified with unauthorized access, or employees that need access to any applications, and then sign and date the first page. The signed report will be maintained at the worksite. Once the review is complete, the site administrator must send an e-mail confirming the review to the Mr. Jose Cardelle, Police Operations Support Supervisor, with information specific to the identified concerns. The e-mail confirmation must be sent no later than 1200 hours on the first Monday following the review. These correspondences will be maintained for one school year.

The Administrative Division will coordinate a training session for all M-DSPD site administrators to assist in this process. An instruction package will be distributed during this training session.

Distribution: Majors (4)
Captains (4)
Commanders (2)
Lieutenants (8)
Ms. Sigilenda Miles
Mr. Jose Cardelle

M E M O R A N D U M

January 24, 2011
305-995-3734

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

FROM: James P. O'Donnell, Chief Information Security Officer
Financial Services

SUBJECT: RESPONSE TO OMCA DRAFT OF POLICE DEPARTMENT AUDIT

Below is the Information Technology Services (ITS) response to the three items on the Police Department Audit that included ITS.

RECOMMENDATIONS:

4.1 Provide the current technology personnel in Schools Police the appropriate training and accesses to enable him to effectively manage the Schools Police organizational unit. Along with training the existing staff, efforts should be made to provide Schools Police the additional standard hardware and M-DCPS network and security technical support by leveraging the pool of ITS-trained technicians.

Responsible Department: **Miami-Dade County Schools Police**
Information Technology Services

Management's Response:

ITS RESPONSE:
The Police Department is scheduled to bring in 150 new laptops for field use. ITS will work with the Police Technical Staff to analyze how to best create a new Organizational Unit (OU) that encompasses all the Department locations, bring the new laptops into compliance as far as naming and security applications, and set up procedures to keep those laptops in compliance without interrupting police operations.

4.3 Establish and maintain a Schools Police OU in Active Directory and ensure that local administration rights to the OU is given to Schools Police.

Responsible Department: **Miami-Dade County Schools Police**
Information Technology Services

Management's Response:

(See ITS response to item 4.1 above).

4.4 Bring all department computers into compliance with District Standards by ensuring that the District's approved computer management software and antivirus (currently BigFix and Sophos) are installed on all computers; and that all computers are named according to the NSS naming convention. Further, as this effort is completed, reconcile the department's computer inventory to Active Directory.

Responsible Department: **Miami-Dade County Schools Police**
Information Technology Services

Management's Response:

(See ITS response to item 4.1 above).

If you have any questions, please contact me at 305-995-3734.

JOD

cc: Ms. Debbie Karcher
Mr. Trevor L. Williams
Mr. Craig Rinehart
Mr. Javier Perez

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

Administrative Offices Network and Information Security Audits – Schools Police

MIAMI-DADE COUNTY PUBLIC SCHOOLS
Office of Management and Compliance Audits
1450 N.E. 2nd Avenue, Room 415
Miami, Florida 33132
Telephone: (305)995-1318 ♦ Fax: (305)995-1331
http://mca.dadeschools.net