Internal Audit Report

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

Audit of Security Controls – Certain District-Issued Mobile Devices

The Mobile Device and BYOD Initiative have been fully deployed throughout the District successfully. Updates to existing policies and standards will help achieve compliance with requirements and best practices.

September 2016

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA

Ms. Perla Tabares Hantman, Chair
Dr. Dorothy Bendross-Mindingall, Vice Chair
Ms. Susie V. Castillo
Dr. Lawrence S. Feldman
Dr. Wilbert "Tee" Holloway
Dr. Martin Karp
Ms. Lubby Navarro
Ms. Raquel A. Regalado
Dr. Marta Pérez Wurtz

Mr. Alberto M. Carvalho
Superintendent of Schools

Mr. José 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

Superintendent of Schools
Alberto M. Carvalho

Chief Auditor
José F. Montes de Oca, CPA

Miami-Dade County School Board
Perla Tabares Hantman, Chair
Dr. Lawrence S. Feldman, Vice Chair
Dr. Dorothy Bendross-Mindingall
Susie V. Castillo
Dr. Wilbert "Tee" Holloway
Dr. Martin Karp
Lubby Navarro
Dr. Marta Pérez
Raquel A. Regalado

September 13, 2016

The Honorable Chair and 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:

We have completed our audit of the District's Mobile Device Initiative. Our audit objective focused on evaluating existing mechanisms for mitigating risk related to the Mobile Device Initiative, including network segregation strategies, device protection (virus/malware), managing loss/theft of devices, privacy controls/filtering, and over-the-air (OTA) device management. This audit centered primarily on ensuring that the aforementioned risks are being mitigated by measuring compliance with standards, policies, procedures, and best practices.

For purposes of this audit, "mobile device" means a District-issued student or staff tablet with wireless network connection capabilities. Personally-owned student and staff devices—Bring Your Own Device (BYOD)—are excluded from the scope of this audit. Reference to BYOD in our findings and recommendations are made in the context of the District's wireless technology initiative, which includes a coupling of both District-issued and personally owned mobile devices. Additionally, District-issued administrative staff devices (smart phones) are not managed by the District's IT department and are also excluded from the scope of this audit. Such devices are issued and managed by the Department of Energy Management and will be subject to an audit to be performed at a later date.

Our audit found that the Mobile Device and BYOD Initiative is safely delivering digital educational benefits to students in a controlled manner.

Sincerely,

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

Table of Contents

Executive Summary

Why We Did This Audit

The use of Smart phones, tablets, and other wireless network-capable mobile devices have become established within M-DCPS as an integral means of communicating, accessing real-time information, and supporting the mission and educational goals of both staff and students. These devices also introduce new risks to the organization.

This audit focused primarily on ensuring that risks are mitigated by measuring compliance with standards, policies, procedures, and industry best practices.

What We Found

Overall, we are pleased to report that the Mobile Device and BYOD Initiative has been fully deployed throughout the District and, as per our modified objectives and testing procedures, is safely delivering digital educational benefits to students in a controlled manner. (See Appendix A, page 15).

Contained in this report are our observations, which we believe will further solidify the successful deployment of mobile devices by strengthening the associated policies and procedures governing this initiative. Our findings mostly dealing with compliance, procedural, and documentation matters, are listed below:

1. *The District's Network Security Standards (NSS), issued October 15, 2012, predates the District's implementation of its Mobile Device and BYOD Digital Convergence Initiative and has not been updated to include improvements stemming from lessons learned during the implementation, management of mobile device infrastructure, and emergent standards, policies and procedures. It must be noted that at the conclusion of this audit, ITS was in the process of updating the NSS. As the name implies, the NSS is the District's fundamental document used to advise employees of necessary compliance in order to protect network resources and data, including the Mobile Device and BYOD Initiative. Although the current version contains a section on portable devices, it comprises only a rudimentary introduction to Mobile Devices and BYOD related requirements.*

2. *The State of Florida **WIRELESS TECHNOLOGY GUIDELINES** recommends that all schools have an active Acceptable Use Policy (AUP), approved by their individual school board, which includes a **Wireless Communications Section.** The District does have AUP's for students and staff in the form of School Board policies. However, those policies currently do not include a wireless communications section. Most elements of the recommended guidelines are addressed in the District's NSS; however, that document is not approved by the School Board. In our opinion, those elements, which provide details about the District's security posture, should not be included in a public document such as the AUP or NSS. We shared this concern with the FLDOE who concurs that security information is exempt from Florida's Public Records Act.*

Other matters that were deemed not significant enough to be included in this report were discussed with management separately for their follow-up.

What We Recommend

Based on our audit conclusions, we have made two recommendations, as follows:

1. *In order to incorporate the District's policies, procedures, and best practices supporting the successful deployment of the Mobile Device and BYOD Initiative, we recommend that the NSS document be updated to include the organization's latest Mobile Device and BYOD requirements as soon as possible.*

2. *In order to comply with the FLDOE's Wireless Technology Guidelines, the appropriate AUP's should be updated to incorporate the NSS by reference and subsequently submitted to the School Board approval. In addition, security characteristics that would not be appropriate for inclusion in a public document such as the AUP or NSS should be documented internally, kept on file, and updated as needed.*

Internal Controls

The chart below summarizes our overall assessment of internal IT controls applicable to the District's Mobile Device Initiative related to District-issued, school-based devices.

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 for improvement	Non-existent or unreliable
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 secure but can be improved	Systems produce incomplete or inaccurate data which may cause inappropriate decisions.
External Risk	None or low	Potential for damage	Severe risk of damage

Background

The District embarked on a "Digital Convergence" goal to ensure that students had the tools and skills necessary to be successful in a world that is increasingly connected by technology. In June of 2013, President Barack Obama called on the Federal Communications Commission to implement **ConnectEd** across America. ConnectEd focused on bringing upgraded connectivity via high-speed broadband connections to all schools within five years, ensuring that teachers are trained to use and deliver education using technology, and leveraging private-sector innovation.

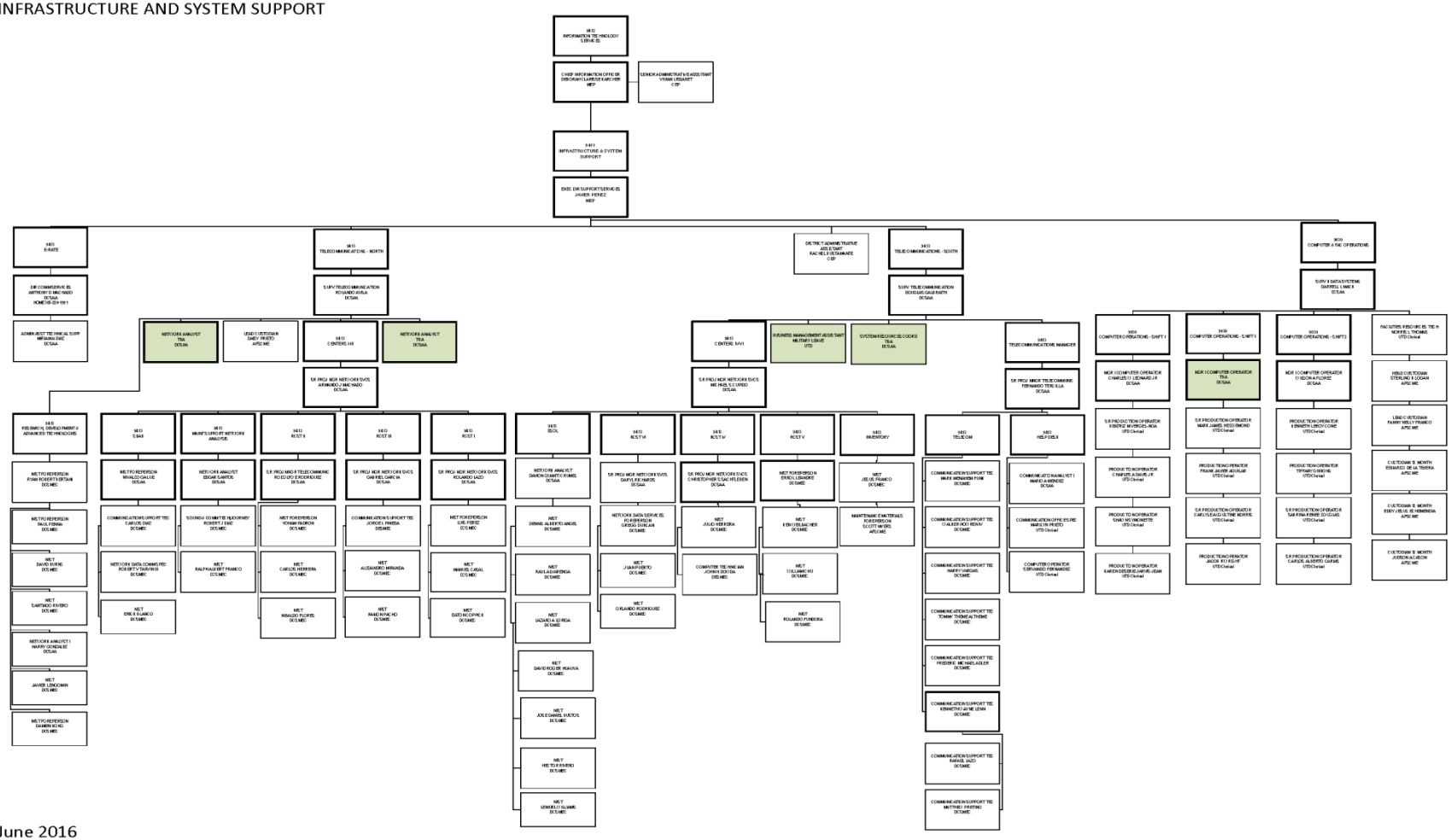
Today, wireless connectivity is deployed at all schools with over 18,000 wireless access points (WAPs), 360 controllers used to manage the WAPs, and over 104,000 District-issued wireless devices, according to ITS staff and documents reviewed.

ITS is responsible for managing the various tools used to ensure compliance with connectivity, security, and safe access. Managing the District's Mobile Device Initiative involves many different components that work together to produce a comprehensive management strategy for all District-issued devices, including:

- Antivirus/malware software installed onto all District-issued devices
- Ensuring device domain membership (a grouping of managed devices)
- Content filtering to protect students from inappropriate material
- Intrusion Prevention System (IPS) used to protect the borders of the District's network and segregate suspicious device activity
- Management and maintenance of an enterprise-level wireless infrastructure
- Centralized operating system and software patching
- Hardened devices to protect against the physical rigors of student use
- Device inventory and repair process

Organizational Chart

INFRASTRUCTURE AND SYSTEM SUPPORT



June 2016

Objectives, Scope, and Methodology

Our objective focused on evaluating existing mechanisms for mitigating risk related to the Mobile Device Initiative, including network segregation strategies, device protection (virus/malware), managing loss/theft of devices, privacy controls/filtering, and over-the-air (OTA) device management. This audit centered primarily on ensuring that the aforementioned risks are mitigated by measuring compliance with standards, policies, procedures, and best practices.

For purposes of this audit, "mobile device" means a District-issued student or staff tablet with wireless network connection capabilities. Personally-owned student and staff devices (BYOD) are excluded from this Audit. Although the District cannot directly manage personally-owned student, staff, or visitor devices, many of the mitigation strategies and tools used to manage District-issued devices also provide simultaneous protection against threats from, and some limited management of, personally-owned devices connecting to the wireless network. In addition, reference to BYOD in our findings and recommendations are made in the context of the District's wireless technology initiative, which includes a coupling of mobile devices, both District-issued and personally owned, BYOD.

The initial scope of our audit was revised to exclude District-issued smart phones, as these devices are not managed by the District's IT department.[1] Smart phones are issued and managed by the Department of Energy Management and will be the subject of an audit to be performed at a later date.

[1] The title of this audit was also revised from the stated title, "Security Controls – Bring Your Own Device (BYOD)," in the 2015-16 Annual Audit Plan to better align with staff and our mutually agreed upon definition of our area of audit coverage and information learned during the audit.

To satisfy our audit objectives, we performed the below audit procedures:

- We obtained an understanding of the mobile devices deployment, management, and monitoring process by interviewing school and District staff.

- We reviewed applicable policies, standards, and best practices, including the following:

  - ❖ National Institute of Standards and Technology (NIST):

    - ✓ Special Publication 800-124, Revision 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise
    - ✓ Special Publication 800-128: Guide for Security-Focused Configuration Management of Information Systems

  - ❖ Florida Statutes: 1001.20 (4) (a)1. a. - d. – Department Under Direction of State Board, *Office of Technology and Information Services*

  - ❖ Florida Department of Education:
    - ✓ Strategic Technology Plan, 2014 – 2019
    - ✓ Wireless Technology Guidelines Technology Guidelines

  - ❖ The Children's Internet Protection Act (CIPA)

- ❖ M-DCPS Documents:

  - ✓ Network Security Standards (NSS), October 15, 2012
  - ✓ Miami-Dade County Public Schools Mobile Device Project Implementation Guide 2015-2016
  - ✓ Literature Review One-to-One and Bring Your Own Device Technology Programs: School District Experiences and Summary of Best Practices
  - ✓ School Board Policy 7530.01 – Staff Use of Wireless Communication Devices
  - ✓ School Board Policy 7540 – Computer Technology and Networks
  - ✓ School Board Policy 7540.01 – Technology Privacy
  - ✓ School Board Policy 7540.03 – Student Responsible Use of Technology, Social Media, and District Network Systems
  - ✓ School Board Policy 7540.04 – Staff Responsible Use of Technology, Social Media, and District Network Systems

- We physically inspected a sample of devices to ensure compliance with the above policies, standards, and best practices.

- We conducted a survey to gather information related to the District's Mobile Devices.

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, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives.

A performance audit is an objective analysis, based on sufficient and appropriate evidence, to assist management and those charged with governance and oversight to improve program performance and operations, reduce costs, facilitate decision-making and contribute to public accountability. Performance audits encompass a wide variety objectives, including assessments of program effectiveness, economy and efficiency; internal control; compliance; and prospective analyses.[2] Planning is a continuous process throughout the audit. Therefore, auditors may need to adjust the audit objectives, scope and methodology as work is being conducted.[3]

We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based on our audit objectives.

[2] Comptroller General of the United States, *Government Auditing Standards*, 2011 Revision, (Washington D.C.: United States Government Accountability Office, 2011), pp. 17-18.

[3] *Ibid.*, p. 126.

Findings, Conclusions, and Recommendations

1. THE DISTRICT'S NETWORK SECURITY STANDARDS (NSS) DOCUMENT SHOULD BE UPDATED	
Issue	The NSS is the District's fundamental document used to advise employees of compliance necessary in order to protect network resources and data, including mobile devices. The latest version, dated October 15, 2012, predates the District's implementation of its Mobile Device and BYOD Digital Convergence Initiative and has not been updated to include improvements stemming from lessons learned during the implementation, management of mobile device infrastructure, and emergent standards, policies and procedures. Although the document contains sections on Portable Devices and BYOD, the latter section is only a rudimentary introduction to the BYOD initiative and related requirements.
Recommendation& Management Response	**1.1 Given that the NSS document was last revised prior to the implementation of the Mobile Device and BYOD Initiative, the District should update the NSS as soon as possible, specifically as it relates to Mobile Devices and BYOD policies, procedures, and best practices.**

Responsible Department	**Information Technology Services**
Management's Response	*Revisions to the Network Security Standards (NSS) are pending upon completion of the review conducted by the Board Attorney. The existing section of the NSS pertaining to BYOD (4.4 BYOD-Bring Your Own Device) will be reviewed to ensure that information pertaining to the Mobile Device and BYOD initiatives is updated as appropriate and added to the pending revisions for the document. Proposed revisions pertaining to this concern will be submitted to the Office of Management and Compliance Audits for review prior to appending to the final draft to ensure that this concern is addressed in a satisfactory manner.*

2. ADDITIONAL DOCUMENTATION IS NECESSARY IN ORDER TO COMPLY WITH THE FLORIDA DEPARTMENT OF EDUCATION (FLDOE) RECOMMENDED GUIDELINES

Issue

The FLDOE publishes recommended guidelines to assist schools and school districts in making their wireless infrastructure decisions, including those used by mobile devices. The State's WIRELESS TECHNOLOGY GUIDELINES recommend:

> **State of Florida WIRELESS TECHNOLOGY GUIDELINES** *(in pertinent part)*
>
> ***Security and Access Management Policies:*** *All schools should have an active Acceptable Use Policy* ***approved by their individual school board that includes a wireless communications section.*** *[emphasis added] Network filtering applications should be in place to comply with the Children's Internet Protection Act (CIPA).*

Audit tests, including inquiry of ITS personnel responsible for the Mobile Device and BYOD Initiative and a review of existing School Board Policies found that the District's Acceptable Use Policies (AUP's) for students and staff, which are approved by the School Board, do not contain a wireless communications section. However, we found that five out of the seven minimum requirements recommended in the State's guidelines are generally addressed within the District's NSS document. However, the NSS is not approved by the School Board.

We believe the omitted information is important to documenting components that are integral to the wireless network infrastructure; however, since some information are directly related to the District's wireless network security posture, such security details would not be appropriate for inclusion in public documents such as the AUP or NSS. We shared this concern with the FLDOE who concurs that security information is exempt from Florida's Public Records Act.

Recommendation & Management Response	**2.1 In order to comply with the FLDOE guidelines, we recommend that the District:** **a) Update the AUP's to incorporate the NSS by reference and submit the updated policies for approval by the School Board.** **b) Update the appropriate documentation regarding the pending exceptions not addressed by the NSS pertaining to 1) Staff Training and 2) Management and Monitoring.** **c) Generate internal documentation, which memorializes those security characteristics that would not be appropriate for inclusion in a public document, to be kept on file and updated as needed.**
Responsible Department	**Information Technology Services**
Management's Response	*Both the Student and Staff Responsible Use Policies (formerly known as the Acceptable Use Policy or AUP) will be updated to incorporate the NSS by reference in order to comply with the FLDOE recommendation that the District's AUP be approved by the School Board. Security information that is exempt from Florida's Public Record Act will be properly documented and updated as necessary, but it shall not appear in the NSS or District AUP documents.*

APPENDIX A – SUMMARY RESULTS OF TEST OF COMPLIANCE				
Item No.	**Description of Standard and (Applicable Standard)**	**Compliant**		**Comment**
		Yes	**No**	
1.	Availability and use of monitoring tools - (FLDOE Wireless Technology Guidelines)	✓		
2.	Annually revised Wireless Network Plan - (FLDOE Wireless Technology Guidelines)	✓		Discussed certain aspect of this requirement with management
3.	The AUP contains a wireless communications section - (FLDOE Wireless Technology Guidelines)		✓	See Finding No. 2
4.	The AUP defines user base - (FLDOE Wireless Technology Guidelines)	✓		
5.	The AUP identifies appropriate usage - (FLDOE Wireless Technology Guidelines)	✓		
6.	Evidence of periodic monitoring and correction of the wireless network for performance/interference exists - (FLDOE Wireless Technology Guidelines)	✓		
7.	Evidence of Wireless Intrusion Prevention System (WIPS) monitoring for "rogue" devices exists - (FLDOE Wireless Technology Guidelines)	✓		
8.	If mobile devices are being used for testing, confirm compliance with minimum hardware/software standards - (FLDOE Technology Guidelines)	✓		
9.	Tools are in place to achieve compliance with the Federal Children's Internet Protection Act - (CIPA)	✓		
10.	Evidence exists of monitoring - (CIPA)	✓		
11.	Evidence exists of educating minors - (CIPA)	✓		
12.	Filtering can be disabled for authorized purposes - (CIPA)	✓		
13.	The organization has a mobile device security policy - (NIST Publication 800-124 Revision 1)	✓		
14.	The organization utilizes basic security measures - (NIST publication 800-124 Revision 1)	✓		

APPENDIX A – SUMMARY RESULTS OF TEST OF COMPLIANCE				
Item No.	**Description of Standard and (Applicable Standard)**	**Compliant**		**Comment**
		Yes	**No**	
15.	The organization conducted piloting prior to implementation - (NIST publication 800-124 Revision 1)	✓		
16.	The organization secured devices prior to issuing - (NIST publication 800-124 Revision 1)	✓		
17.	The organization performs routine maintenance (updates, etc.) - (NIST publication 800-124 Revision 1)	✓		
18.	The organization includes needed changes to mobile device-related issues via a change/configuration management process - (NIST publication 800-128)	✓		
19.	Test District-issued student devices for presence of mitigation software for threats from virus/malware - (NSS)	✓		NSS addresses this issue, but has not been updated for lessons learned and other matters stemming from the mobile device and BYOD rollout. See Finding No. 1
20.	Mobile devices have an inactivity time-out feature - (NSS)	✓		See Comment No. 19
21.	Devices must support WPA2-PSK - (NSS)	✓		See Comment No. 19
22.	The capability to remotely "lock down" wirelessly connected mobile devices both during testing and if the device is reported lost or stolen - (NIST Publication 800-124 Revision 1 and FLDOE Technology Guidelines)	✓		
23.	Users are prevented from performing unauthorized device changes - (NIST Publication 800-124 Revision 1)	✓		
24.	The device locks or wipes after a specific number of unsuccessful authentication attempts - (NIST Publication 800-124 Revision 1)	✓		
25.	If device is a Windows OS, is device a member of the domain - (NSS)	✓		See Comment No. 19

APPENDIX A – SUMMARY RESULTS OF TEST OF COMPLIANCE				
Item No.	**Description of Standard and (Applicable Standard)**	**Compliant**		**Comment**
		Yes	**No**	
26.	Availability and use of management tools are in place - (NIST Publication 800-124 Revision 1 and FLDOE Technology Guidelines)	✓		
27.	District-issued mobile device software is being updated (OS versions, updates, vulnerability patches, AV, etc.) - (NIST Publication 800-124 Revision 1)	✓		
28.	The organization follows device inventory management procedures - (NIST Publication 800-124 Revision 1)	✓		
29.	Capabilities and general remote management and updating of wireless infrastructure (WAPs, Routers, Switches) exist - (NIST Publication 800-124 Revision 1 and NSS)	✓		

Management's Response (Complete Text)

Miami-Dade County Public Schools

giving our students the world

September 12, 2016

Dear Mr. Montes de Oca,

Below are the Office of Academics and Transformation's management responses regarding the findings, conclusions, and recommendations stemming from the Audit of Security Controls—Certain District Issued Mobile Devices.

If you have any questions, please contact Marie Izquierdo, Chief Academic Officer, Office of Academics and Transformation, at 305 995-1451, or Deborah Karcher, Chief Information Officer, Division of Information Technology Services, at 305 995-3750.

Sincerely,

Marie Izquierdo, Chief Academic Officer
Office of Academics and Transformation

MI:eg
L024

School Board Administration Building • 1450 N.E. 2nd Avenue • Miami, Florida 33132
305-995-1000 • www.dadeschools.net

Audit of Security Controls/Management Response

Office of Academics and Transformation

Although there were two audit recommendations stemming from the recent Audit of Security Controls-Certain District-Issued Mobile Devices, Miami-Dade County Public Schools was a recent recipient of the Trusted Learning Environment (TLE) Seal, a coveted award recognizing the District for demonstrating that measurable steps have been taken to help ensure the privacy of student data and the protections of our networked resources. Security is a dynamic entity, and the District is continually refining its approach in order to properly safeguard our students, their data, and our systems.

1.1 Management Response:

Revisions to the Network Security Standards (NSS) are pending upon completion of the review conducted by the Board Attorney. The existing section of the NSS pertaining to BYOD (4.4 BYOD-Bring Your Own Device) will be reviewed to ensure that information pertaining to the Mobile Device and BYOD initiatives is updated as appropriate and added to the pending revisions for the document. Proposed revisions pertaining to this concern will be submitted to the Office of Management and Compliance Audits for review prior to appending to the final draft to ensure that this concern is addressed in a satisfactory manner.

2.1 Management Response:

Both the Student and Staff Responsible Use Policies (formerly known as the Acceptable Use Policy or AUP) will be updated to incorporate the NSS by reference in order to comply with the FLDOE recommendation that the District's AUP be approved by the School Board. Security information that is exempt from Florida's Public Record Act will be properly documented and updated as necessary, but it shall not appear in the NSS or District AUP documents.

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.

Boy Scouts of America Equal Access Act of 2002 – no public school shall deny equal access to, or a fair opportunity for groups to meet on school premises or in school facilities before or after school hours, or discriminate against any group officially affiliated with Boy Scouts of America or any other youth or community group listed in Title 36 (as a patriotic society).

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.

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.

INTERNAL AUDIT REPORT

Audit of Security Controls – Certain District-Issued Mobile Devices

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