Miami-Dade County Public Schools

Internal Audit Report

Audit of Virtual Private Network (VPN) - Security Controls and Access Management

Improved Documentation, Event Logging, Periodic Reviews, and Additional Controls will Strengthen the District's VPN Process and Related Security Efforts

July 2022

Office of Management and Compliance Audits

Mr. Jon Goodman, CPA, CFE
Chief Auditor

Contributors to This Report:

Audit Supervised by:
Mr. Luis O. Baluja, District Director - IT Audits, CISA

Audit Performed by:
Mr. Alejandro Santana-Alvarez, IT Auditor, MSCS
Mr. Erick Blanco, Cybersecurity Analyst I

Audit Reviewed by:
Mr. Richard A. Yanez, CPA, District Audit Director

Miami-Dade County Public Schools

giving our students the world

Superintendent of Schools
Dr. Jose L. Dotres

Chief Auditor
Jon Goodman, CPA, CFE

July 7, 2022

The Honorable Chair and Members of The School Board of Miami-Dade County, Florida
Members of the School Board Audit and Budget Advisory Committee
Dr. Jose L. Dotres, Superintendent of Schools

Ladies and Gentlemen:

We have completed our **Audit of Virtual Private Network (VPN) - Security Controls and Access Management**, in accordance with the 2021-2022 Fiscal Year Audit Plan.

The lockdown caused by the COVID-19 pandemic created a sudden need for mass remote work capabilities, resulting in a near 120% increase in the number of existing VPN accounts prior to the pandemic. The proliferation of this critical business tool also increases the risks associated with using this technology.

Our audit presents three findings and six corresponding recommendations, including the need for detailed process documentation, periodic reviews, and actionable audit/event logging. Furthermore, updating the organization's Network Security Standards document is required.

We have discussed certain confidential findings and recommendations with Management (excluded from this report) to further strengthen activities and process related to VPN.

We would like to thank management for the cooperation and courtesies extended to our staff during this audit.

Sincerely,

Jon Goodman

Jon Goodman, CPA, CFE
Chief Auditor

Table of Contents

		Page
Executive Summary		**1**
Internal Controls		**2**
Background		**3**
Partial Organizational Chart		**4**
Objectives, Scope, and Methodology		**5**
Glossary of Technical Terms and Acronyms		**7**
Findings, Conclusions, and Recommendations		
1	VPN Process/Infrastructure Documentation, and Updating of the M-DCPS Network Security Standards are Needed	**8**
2	Periodic Review of VPN Access	**10**
3	Lack of Audit and Incident Response Logs	**12**
4	Confidential Findings and Recommendations	**14**
Management's Response		**15**

Executive Summary

We have performed this **Audit of Virtual Private Network (VPN) - Security Controls and Access Management**, in accordance with the 2021-2022 Fiscal Year Audit Plan.

The objective of this audit was to provide assurances relative to the effectiveness of implemented VPN controls. Accordingly, we reviewed the procedures for provisioning and managing VPN technology, the supporting infrastructure, and adherence to applicable standards and best practices.

VPN technology allowed certain activities of the District's workforce and related critical functions to continue, despite the lockdown caused by the COVID-19 pandemic. When compared to the existing number of VPN accounts, the sudden need for mass remote work capabilities resulted in a near 120% increase of new accounts. The proliferation of this critical business tool also increases risk.

Our audit presents three findings and six corresponding recommendations, including the need for detailed process documentation, periodic reviews, and actionable audit/event logging. Furthermore, updating the organization's Network Security Standards document is required.

We have discussed certain confidential findings and recommendations with Management (excluded from this report) to further strengthen activities and process related to VPN.

Management's responses to our findings (and recommendations) are included on pages 8 through 14 following each individual finding, and in memorandum format as received by our office, beginning on page 15. We have also included a glossary of related technical terms and acronyms on page 7.

Internal Controls

The chart below summarizes our overall assessment of internal controls applicable to the VPN process.

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	Information systems are mostly secure but can be improved	Information 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 lockdown caused by the COVID-19 pandemic created a sudden need for mass remote work capabilities. The District responded to this need by leveraging Virtual Private Network (VPN) technology.

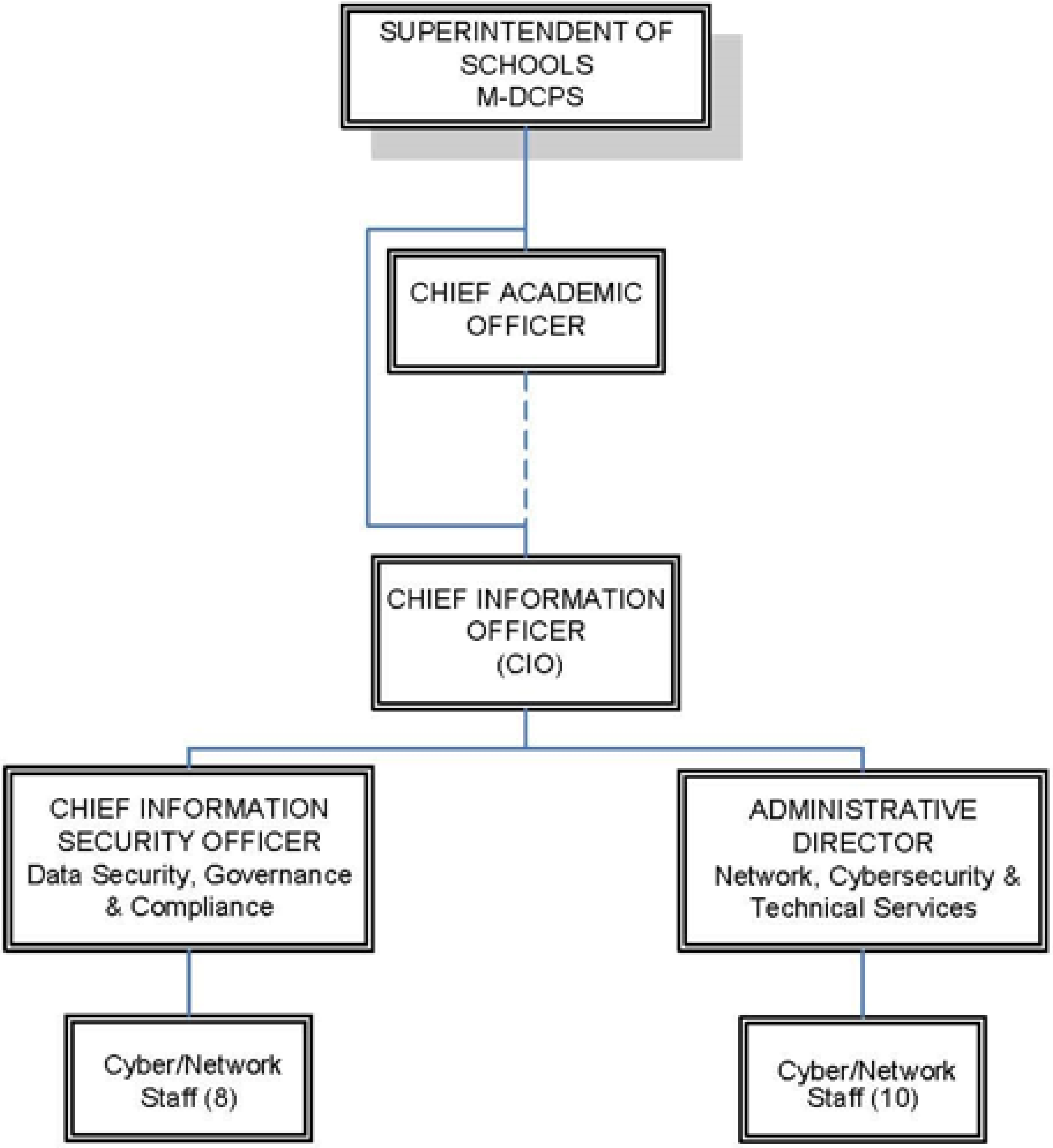
VPN allows authenticated users to remotely connect to the District's network resources from nearly anywhere, using a computer or mobile device. Once connected, the user can access data, files, and systems that would not otherwise be available from outside of the District's network. The user's device becomes a part of the M-DCPS network for the duration of the connection.

During the pandemic, requests for VPN accounts more than doubled from about 3,000 existing accounts to 6,578. When the District returned to a predominantly physical work reporting model, the VPN population decreased in tandem. Even so, the population at the conduct of this audit rose, and remains steady, at over 50% more to about 4,600 accounts.

The creation, disablement, overall management of VPN technology, and the enabling infrastructure are all under the direct responsibility of Information Technology Services (ITS). More specifically, the VPN process is administered jointly by the Data Security, Governance & Compliance and the Network, Cybersecurity & Technical Services divisions.

The following chart illustrates the general organizational structure applicable to the management and support of the District's VPN process.

Partial Organizational Chart


SUPERINTENDENT OF SCHOOLS M-DCPS
CHIEF ACADEMIC OFFICER
CHIEF INFORMATION OFFICER (CIO)
CHIEF INFORMATION SECURITY OFFICER Data Security, Governance & Compliance
ADMINISTRATIVE DIRECTOR Network, Cybersecurity & Technical Services
Cyber/Network Staff (8)
Cyber/Network Staff (10)

* Current Organizational Chart structure as of 6/1/22.

Objectives, Scope, and Methodology

The objective of this audit was to review and evaluate the procedures for the provisioning and general management of VPN technology, and adherence to applicable standards and best practices. We performed the following procedures to satisfy our objective:

- Obtained an understanding of the District's overall VPN process, as it relates to the scope of our audit:

    - Interviewed the owners and staff of the VPN process and those responsible for the management of VPN.
    - Conducted step-by-step walk-throughs of the entire VPN account management process, from creation to disablement.
    - Documented the enabling VPN infrastructure and hardware.
    - Identified the VPN population by general user type.
    - Reviewed and documented the mechanisms used for VPN account requests, including need-based rationale.
    - Reviewed audit, incident, and other reports used for incident response.

- Reviewed and identified criteria, standards, directives, policies, rules, and best practices applicable to the audited area, including:

    - Various National Institute of Standards and Technology (NIST) publications:
        - NIST Guide to SSL VPNs 800-113
        - NIST.SP.800-77r1 – Guide to IPsec VPNs
        - NIST.SP.800-52r2 -Guidelines for the Selection, Configuration, and Use of TLS implementations
        - NIST Special Publication 800-53, Revision 5 - Security and Privacy Controls for Information Systems and Organizations
        - NIST 800-46, Revision 2 – Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security

    - M-DCPS' Network Security Standards (NSS)
    - Vendor documentation and guidance applicable to the VPN infrastructure and appliances being used
    - VPN-related vendor security advisories and/or bulletins
    - DTLS protocol for VPN Clients – Remote Access VPN Tunnels
    - Prior audits or work performed by other entities in the audited area
    - Numerous VPN-related directives and/or informational communications (a.k.a. "Weekly Briefings")

- Performed various audit tests:

  - Verified operating system and firmware versions.
  - Verified the status of recommended/required hardware manufacturer updates.
  - Reviewed the various communications protocols in use.
  - Verified that updates or changes that affect VPN are properly vetted through a Change Management process.
  - Determined if VPN redundancy/continuity mechanisms were in place.
  - Examined certain elements of VPN usage for behavior and performance.
  - Tested the recently implemented Multi Factor Authentication (MFA) process relative to the VPN process.

- Gauged the experience, practice, and needs of VPN users:

  - Interviewed administrative, school site, Charter School, and contractors that use VPN to obtain an understanding of:

    - User experiences and activities
    - Frequency of use
    - Rationale for initial and continued use of VPN
    - Compiled statistics, on a sample basis:
      - Initial need for VPN access
      - Continued need for access
      - VPN-related security awareness
      - MFA registration and process
      - VPN system use notification

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States of America Government Accountability Office (GAO). Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Glossary of Technical Terms and Acronyms

The following definitions are provided for abbreviations and acronyms used in this report:

VPN	**Virtual Private Network** – A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and information transmitted between networks
NSS	**Network Security Standards** - M-DCPS' network security document
SIEM	**Security Information and Event Management** – tool used to monitor network and systems activity
NIST	**National Institute of Standards and Technology** – A federal organization charged with developing information technology security standards and guidelines for governmental information systems
WB	**Weekly Briefings** - the District's centralized information distribution tool
PoLP	**Principle of Least Privilege –** allowing only minimal authorized access as needed for users to accomplish assigned organizational tasks
ITS	**Information Technology Services -** Central District IT facility
MFA	**Multi Factor Authentication -** authentication method that requires users to provide two or more verification factors to gain access to a network resource

Findings, Conclusions, and Recommendations

1. VPN Process/Infrastructure Documentation and Updating of the M-DCPS Network Security Standards are Needed

All control families discussed within *NIST Special Publication 800-53, R5 - Security and Privacy Controls for Information Systems and Organizations*, call for documenting the subject process or system. This includes the development of purpose, scope, responsibilities, and steps/actions required by assigned staff to properly manage the system.

Process/Infrastructure Documentation:

We requested and reviewed limited documentation governing the overall VPN process. We found that what was provided was decidedly insufficient and lacked meaningful detail.

Process and infrastructure documentation governing the entire VPN process supports the organization's rules and methods necessary to properly manage the technology. It ensures that the proper steps are performed each time throughout the entire account creation, management, and disablement of VPN accounts.

Documenting the hardware infrastructure and configuration, along with the physical and logical flows of data, is also a best practice and should be an integral component.

Such documentation is conducive to creating a reliable process that helps eliminate errors and generates repeatable outcomes. This is particularly important when assigning new staff to manage the VPN process and helps mitigate problems that arise from a drain of institutional knowledge.

Network Security Standards (NSS):

The NSS is a publicly available document that summarizes the general procedures and security posture of the District's networked resources and data. This document is also incorporated by reference into several School Board Policies.

This critical document has not been updated since 2017.

Responsible Department: **Information Technology Services**

Recommendations:

1.1 Detailed internal process/infrastructure documentation governing the entire VPN process should be developed, to include steps in the overall provisioning and disabling of VPN accounts. This information may be incorporated into existing internal documentation as a new chapter and should be revisited and updated as needed.

Management's Response:

The District concurs with this finding and has completed the requisite updates of the internal process and infrastructure documentation presented in the recommendation.

1.2 The NSS document should be updated as soon as possible, incorporating critical changes and/or new procedures that have accumulated since 2017. VPN-related procedures and/or guidance should also be incorporated into the NSS update. Once updated and approved, this document should be proactively disseminated and posted to relevant District websites as needed. The NSS should be revisited annually at a minimum and updated, as necessary.

Management's Response:

The District concurs with this finding, the Network Security Standards have been revised, reviewed internally by ITS staff from various functional areas, and have subsequently been reviewed by staff from Management and Compliance Audits as well and are currently pending review by the Board Attorney's Office. The NSS has been used and referenced a number of times since last publication for purposes such as disciplinary action and legal/contractual purposes, and the District has been able to successfully defend or enforce the Standards in every situation to date. Many of the changes to user processes and procedures (i.e., 12-character complex password requirements, etc.) are enforced by technical policies; as such, users are essentially forced to adhere to these policies in order to use District resources. Historically, proposed revisions to the document are made periodically as a result of situations such as audit engagements, District policy/process changes, etc. This has resulted in significant delays in the timely publication of the document. The District concurs with this finding, and ITS is proposing a more frequent revision cadence to avoid the accumulation of revisions and the subsequent delay of the release of the document. (ITS is proposing that any changes to processes or policies that necessitate a Weekly Briefing will also result in an immediate revision of the NSS to simplify the overall review and publication process.)

2. Periodic Review of VPN Access

NIST Special Publication 800-53, R5 family of Access Controls (AC-6) and best practices follow the Principle of Least Privilege (PoLP) relative to systems and data access. The PoLP generally states that users (or systems), should only be granted the minimum accesses needed to perform assigned organizational tasks.

Currently, users that have been provisioned with a VPN account, continue to have access indefinitely. Although VPN access was critical during the work-from-home stages of the COVID-19 lockdown, continued access may not be necessary for certain users now that the District has returned to an in-person work model.

It should be noted that access to an authorized VPN account continues to provide the same access and permissions to networked resources and/or systems that the user already has access to. In addition, the District's recent implementation of a Multi-Factor Authentication (MFA) process, helps to strengthen VPN security.

Requesting VPN Access:

The District published Weekly Briefing # 27201 on March 12, 2020. This briefing updated and clarified the procedures and requirements for VPN access. For example, a work location administrator must submit the request on behalf of staff, along with the business rationale supporting the need for VPN access. We noted inconsistencies with meeting these requirements.

Responsible Department: **Information Technology Services**

Recommendations:

2.1 Periodic reviews of access to systems and data via a remote VPN connection should be conducted by each work location's administrator. This review should consider any existing and/or changes in user roles.

Similarly, ITS staff responsible for vetting/granting VPN access should ensure that the proper support accompanies the request, including that the request comes from a work location administrator and incorporates appropriate business-based rationale for access.

Management's Response:

The District concurs with this finding; the current process of determining appropriate VPN access often requires ITS staff to engage with requestors to further clarify the need for VPN access and/or the functions required by the end user. ITS will publish additional communications (i.e., Weekly Briefings) to assist users with providing the appropriate narrative to facilitate the process.

2.2 Periodic review of VPN access requires the work location administrator to have access to, and review, real-time information that summarizes VPN users and activity at their location, including last connection date.

Accounts that are no longer deemed necessary by the work location administrator should be disabled or removed via a documented request mechanism such as a help ticket or email to ITS. The rationale for such action should be included in the request.

Management's Response:

The District concurs with this finding and is currently in the process of researching potential mechanisms to allow for site reviews.

2.3 The NSS should be updated to account for periodic VPN review. In addition, work location administrators should be informed and proactively reminded of the need to conduct said review.

Management's Response:

The Network Security Standards currently under review already have language regarding the potential review process; this language has already been reviewed by MCA.

3. Lack of Audit and Incident Response Logs

NIST contains multiple areas that fall under and address the need for continuous systems monitoring, including remote access monitoring relative to VPN technology.

Data captured as a result of audit and incident response records are important when attempting to determine the cause of errors or system failures. Specifically, incident response logs become critical when identifying or responding to unusual/unauthorized activity and crucial evidence during investigations.

The District currently has a tool used for monitoring and logging that produces limited information. However, the District procured a new Security Information and Event Management (SIEM) tool in July of 2021 that, according to management and in concert with the aforementioned tool, is expected to generate significantly improved metrics and capturing of information across multiple systems.

We requested reports/metrics/data generated from the existing monitoring process but found the information to be limited and difficult to analyze.

According to ITS management, the new SIEM tool, as it pertains to the VPN process and related monitoring, should be fully implemented by the beginning of the 2022-2023 school year.

Recommendation:

3.1 We recommend that ITS expedite and continue its work of configuring and implementing the referenced tools to generate actionable data supporting ongoing monitoring, logging, and incident response activities relative to VPN.

Responsible Department: **Information Technology Services**

Management's Response:

The District does not concur with this finding. ITS acknowledged the shortcoming of the previous log aggregation tool and is aware of the NIST standards regarding continuous system monitoring; as such, the District procured a SIEM solution well in advance of the inception of this audit. Installation of the solution is complete, and tuning and configuration is currently under way. ITS is confident that the new SIEM, once fully tuned and configured, will significantly exceed the information previous solution.

Auditor’s Comment:

While Management has assured us that the District’s new SIEM solution will generate robust audit and incident logs when fully implemented, evidence of such logs was limited at the time of our testing. In addition, auditing standards call for follow-up of management’s actions. Formal reporting of the stated condition as a finding serves as a follow-up mechanism to ensure management’s stated corrective actions were implemented and completed timely.

4. Confidential Findings and Recommendations

We discussed with ITS management various issues regarding certain controls that yield additional layers of protection for systems and data accessed remotely via a VPN connection. NIST and vendor-related recommendations related to the VPN process were also discussed.

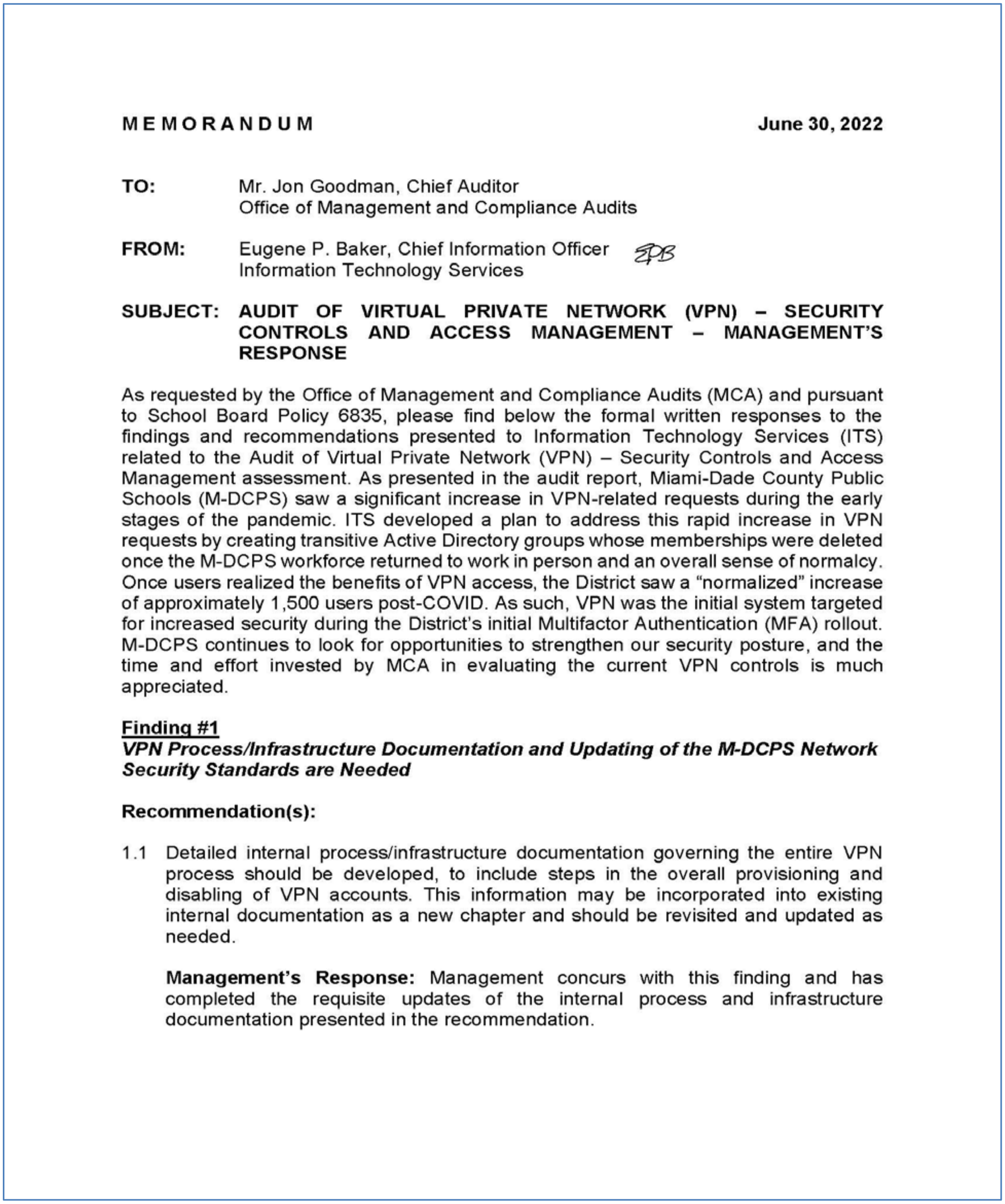
The details of the findings and recommendations have been omitted from this report for security purposes pursuant to Section 281.301, Florida Statutes, Security systems; records and meetings exempt from public access or disclosure.

Responsible Department: **Information Technology Services**

Management's Response:

ITS has discussed the confidential findings with MCA and concurs with the findings. The findings under direct control of ITS have already been resolved and/or mitigated. An additional finding will require the assistance of an external vendor to address.

Management's Response



MEMORANDUM **June 30, 2022**

TO: Mr. Jon Goodman, Chief Auditor
Office of Management and Compliance Audits

FROM: Eugene P. Baker, Chief Information Officer EPB
Information Technology Services

SUBJECT: AUDIT OF VIRTUAL PRIVATE NETWORK (VPN) – SECURITY CONTROLS AND ACCESS MANAGEMENT – MANAGEMENT'S RESPONSE

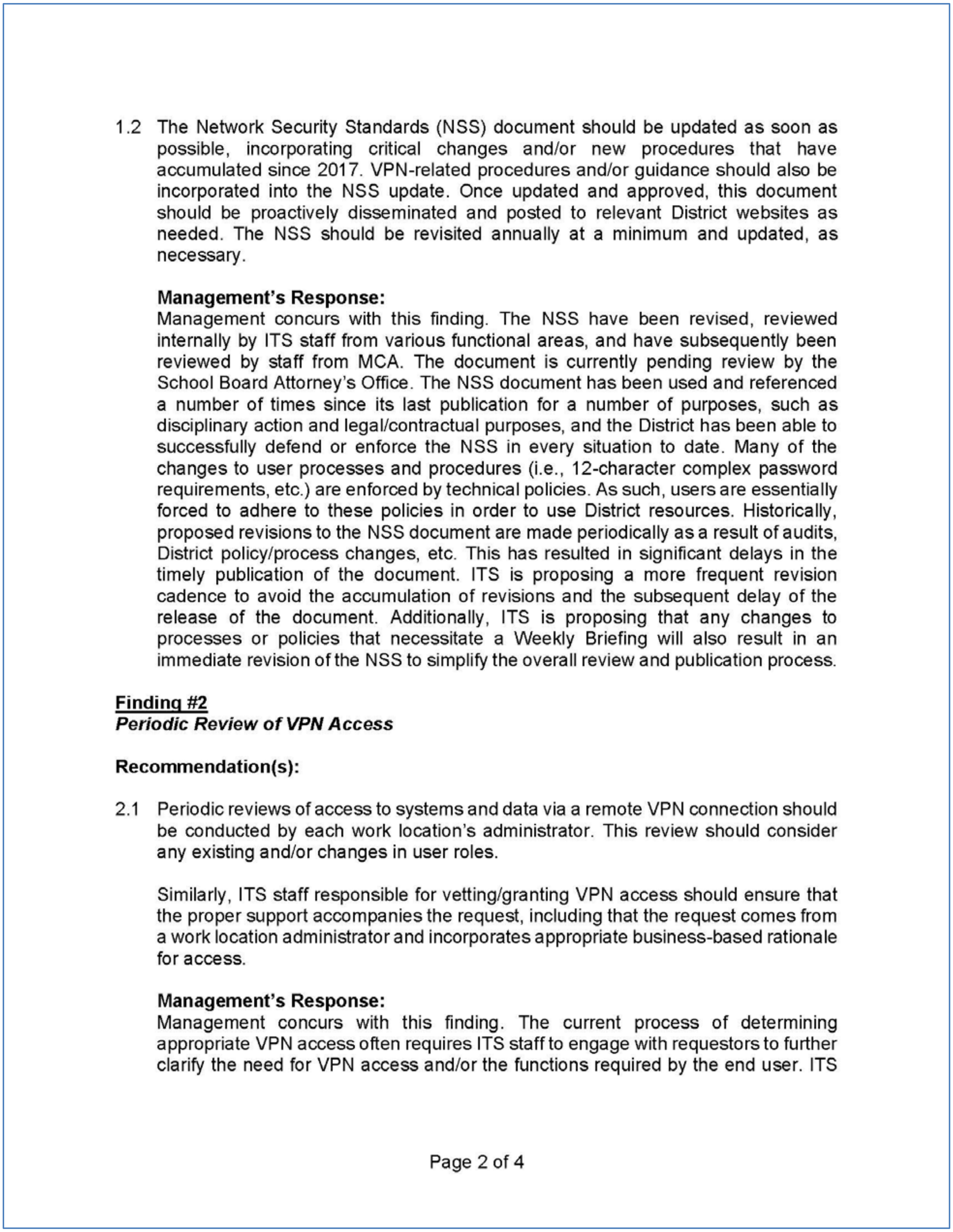
As requested by the Office of Management and Compliance Audits (MCA) and pursuant to School Board Policy 6835, please find below the formal written responses to the findings and recommendations presented to Information Technology Services (ITS) related to the Audit of Virtual Private Network (VPN) – Security Controls and Access Management assessment. As presented in the audit report, Miami-Dade County Public Schools (M-DCPS) saw a significant increase in VPN-related requests during the early stages of the pandemic. ITS developed a plan to address this rapid increase in VPN requests by creating transitive Active Directory groups whose memberships were deleted once the M-DCPS workforce returned to work in person and an overall sense of normalcy. Once users realized the benefits of VPN access, the District saw a "normalized" increase of approximately 1,500 users post-COVID. As such, VPN was the initial system targeted for increased security during the District's initial Multifactor Authentication (MFA) rollout. M-DCPS continues to look for opportunities to strengthen our security posture, and the time and effort invested by MCA in evaluating the current VPN controls is much appreciated.

Finding #1
VPN Process/Infrastructure Documentation and Updating of the M-DCPS Network Security Standards are Needed

Recommendation(s):

1.1 Detailed internal process/infrastructure documentation governing the entire VPN process should be developed, to include steps in the overall provisioning and disabling of VPN accounts. This information may be incorporated into existing internal documentation as a new chapter and should be revisited and updated as needed.

Management's Response: Management concurs with this finding and has completed the requisite updates of the internal process and infrastructure documentation presented in the recommendation.



1.2 The Network Security Standards (NSS) document should be updated as soon as possible, incorporating critical changes and/or new procedures that have accumulated since 2017. VPN-related procedures and/or guidance should also be incorporated into the NSS update. Once updated and approved, this document should be proactively disseminated and posted to relevant District websites as needed. The NSS should be revisited annually at a minimum and updated, as necessary.

Management's Response:
Management concurs with this finding. The NSS have been revised, reviewed internally by ITS staff from various functional areas, and have subsequently been reviewed by staff from MCA. The document is currently pending review by the School Board Attorney's Office. The NSS document has been used and referenced a number of times since its last publication for a number of purposes, such as disciplinary action and legal/contractual purposes, and the District has been able to successfully defend or enforce the NSS in every situation to date. Many of the changes to user processes and procedures (i.e., 12-character complex password requirements, etc.) are enforced by technical policies. As such, users are essentially forced to adhere to these policies in order to use District resources. Historically, proposed revisions to the NSS document are made periodically as a result of audits, District policy/process changes, etc. This has resulted in significant delays in the timely publication of the document. ITS is proposing a more frequent revision cadence to avoid the accumulation of revisions and the subsequent delay of the release of the document. Additionally, ITS is proposing that any changes to processes or policies that necessitate a Weekly Briefing will also result in an immediate revision of the NSS to simplify the overall review and publication process.

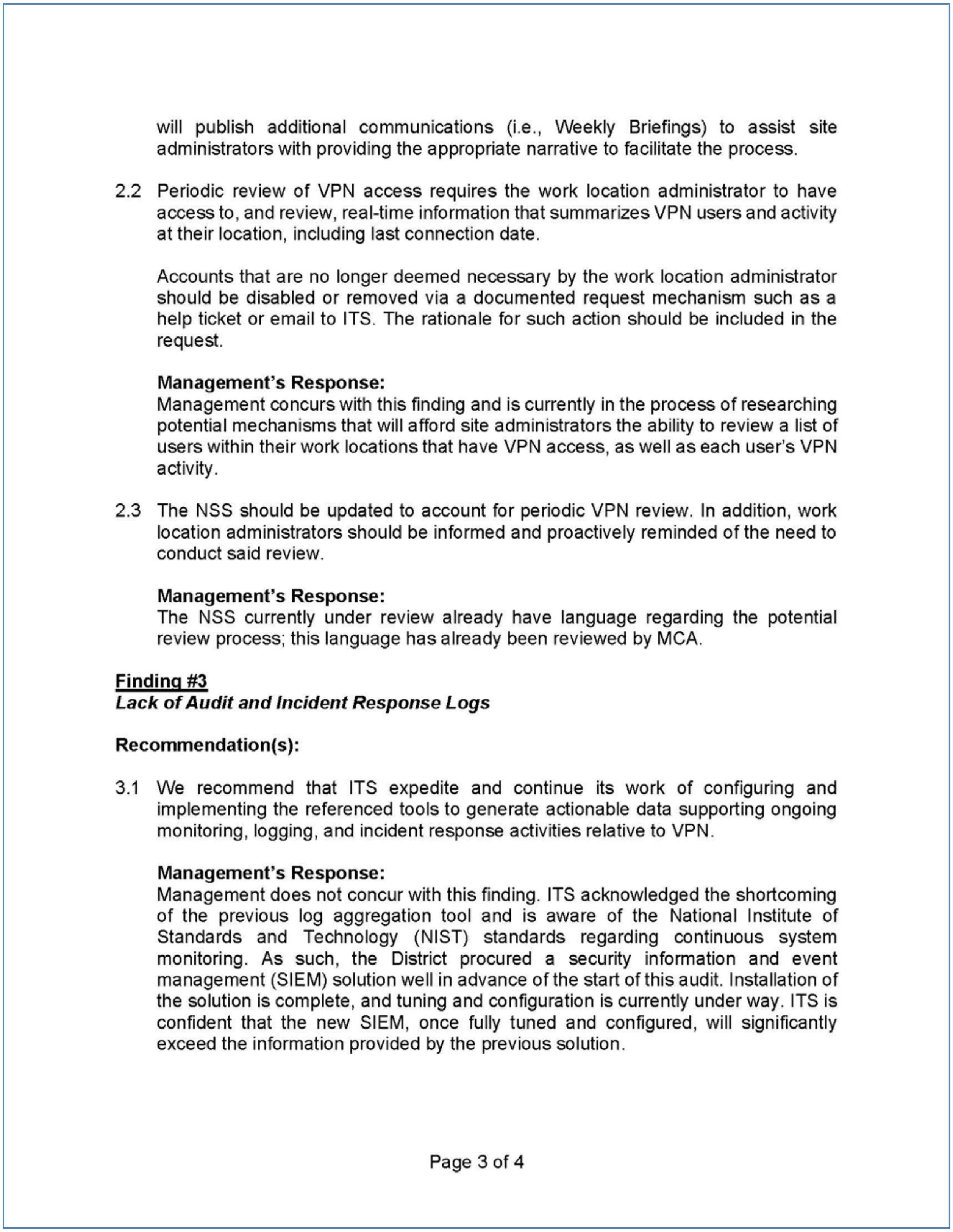
<u>Finding #2</u>
Periodic Review of VPN Access

Recommendation(s):

2.1 Periodic reviews of access to systems and data via a remote VPN connection should be conducted by each work location's administrator. This review should consider any existing and/or changes in user roles.

Similarly, ITS staff responsible for vetting/granting VPN access should ensure that the proper support accompanies the request, including that the request comes from a work location administrator and incorporates appropriate business-based rationale for access.

Management's Response:
Management concurs with this finding. The current process of determining appropriate VPN access often requires ITS staff to engage with requestors to further clarify the need for VPN access and/or the functions required by the end user. ITS



will publish additional communications (i.e., Weekly Briefings) to assist site administrators with providing the appropriate narrative to facilitate the process.

2.2 Periodic review of VPN access requires the work location administrator to have access to, and review, real-time information that summarizes VPN users and activity at their location, including last connection date.

Accounts that are no longer deemed necessary by the work location administrator should be disabled or removed via a documented request mechanism such as a help ticket or email to ITS. The rationale for such action should be included in the request.

Management's Response:
Management concurs with this finding and is currently in the process of researching potential mechanisms that will afford site administrators the ability to review a list of users within their work locations that have VPN access, as well as each user's VPN activity.

2.3 The NSS should be updated to account for periodic VPN review. In addition, work location administrators should be informed and proactively reminded of the need to conduct said review.

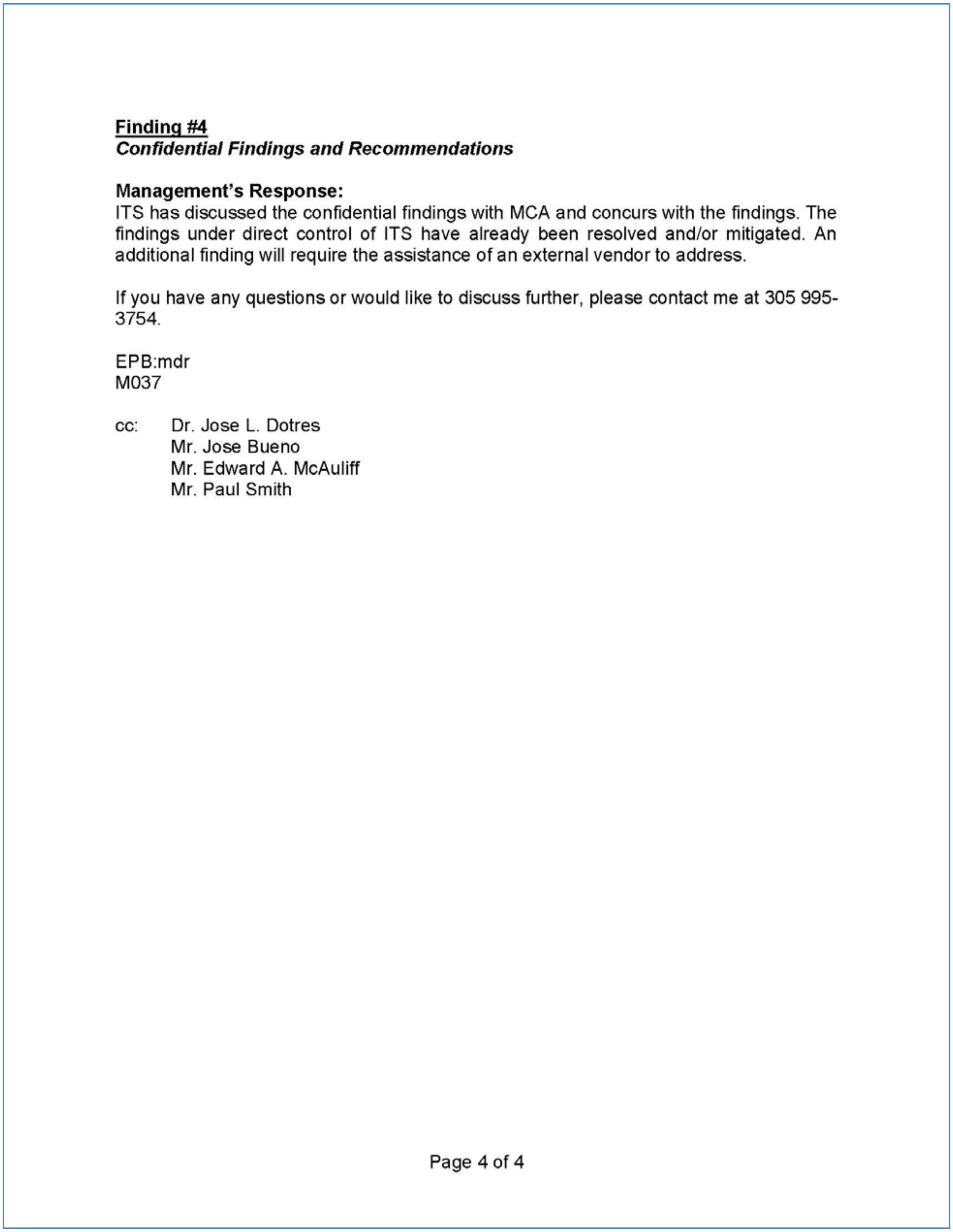
Management's Response:
The NSS currently under review already have language regarding the potential review process; this language has already been reviewed by MCA.

Finding #3
Lack of Audit and Incident Response Logs

Recommendation(s):

3.1 We recommend that ITS expedite and continue its work of configuring and implementing the referenced tools to generate actionable data supporting ongoing monitoring, logging, and incident response activities relative to VPN.

Management's Response:
Management does not concur with this finding. ITS acknowledged the shortcoming of the previous log aggregation tool and is aware of the National Institute of Standards and Technology (NIST) standards regarding continuous system monitoring. As such, the District procured a security information and event management (SIEM) solution well in advance of the start of this audit. Installation of the solution is complete, and tuning and configuration is currently under way. ITS is confident that the new SIEM, once fully tuned and configured, will significantly exceed the information provided by the previous solution.



Finding #4

Confidential Findings and Recommendations

Management's Response:

ITS has discussed the confidential findings with MCA and concurs with the findings. The findings under direct control of ITS have already been resolved and/or mitigated. An additional finding will require the assistance of an external vendor to address.

If you have any questions or would like to discuss further, please contact me at 305 995-3754.

EPB:mdr
M037

cc: Dr. Jose L. Dotres
Mr. Jose Bueno
Mr. Edward A. McAuliff
Mr. Paul Smith

Anti-Discrimination Policy

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. M-DCPS does not discriminate on the basis of sex in any education program or activity that it operates as required by Title IX. M-DCPS also does not discriminate on the basis of sex in admissions or employment.

Age Discrimination Act of 1975 - prohibits discrimination based on age in programs or activities.

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 years old.

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 race, color, ethnic or national origin, religion, marital status, disability, genetic information, age, political beliefs, sexual orientation, sex/gender, gender identification, social and family background, linguistic preference, pregnancy, citizenship status, and any other legally prohibited basis. Retaliation for engaging in a protected activity is also prohibited.

For additional information about Title IX or any other discrimination/harassment concerns, contact the U.S. Department of Education Asst. Secretary for Civil Rights or:

Office of Civil Rights Compliance (CRC)
Executive Director/Title IX Coordinator
155 N.E. 15th Street, Suite P104E
Miami, Florida 33132
Phone: (305) 995-1580 TDD: (305) 995-2400
Email: crc@dadeschools.net **Website:** https://hrdadeschools.net/civilrights Revised 07/2020

Miami-Dade County Public Schools

Internal Audit Report

Audit of Virtual Private Network (VPN) - Security Controls and Access Management

July 2022

Office of Management and Compliance Audits
1450 N. E. 2nd Avenue, Room 415
Miami, Florida 33132
Tel: (305) 995-1318 • Fax: (305) 995-1331
http://mca.dadeschools.net