Internal Audit Report

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

AUDIT OF ELECTRONIC GRADE BOOK SECURITY AND CONTROLS

The Electronic Grade Book (EGB) application is facilitating and modernizing the recording of student academic data and making this information easily available to parents. However, there is a strong need for the implementation of certain controls, procedures, and best practices that would improve the security of student data and enhance overall use of the product.

March 2014

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA
Ms. Perla Tabares Hantman, Chair
Dr. Lawrence S. Feldman, Vice Chair
Dr. Dorothy Bendross-Mindingall
Ms. Susie V. Castillo
Mr. Carlos L. Curbelo
Dr. Wilbert "Tee" Holloway
Dr. Martin Karp
Dr. Marta Pérez
Ms. Raquel A. Regalado

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 O. Baluja, CISA

Audit Reviewed and Supervised 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

March 4, 2014

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:

In accordance with the approved audit plan for the 2012-13 Fiscal Year, we have completed an audit of Electronic Grade Book – Security and Controls.

In general, our audit shows that the District's use of the Electronic Grade Book (EGB) application is accomplishing the intended goal of facilitating and modernizing the recording of student academic data and making this information easily available to parents via the District's Parent Portal. However, our audit disclosed a strong need for the implementation of certain controls, procedures, and best practices that would improve the security of student data as well as enhance overall use of the product.

Other isolated or inconsequential matters that came to our attention during our audit were communicated to management for its follow up.

We would like to thank management for their input and contributions during the audit.

Sincerely,

José F. Montes de Oca

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

TABLE OF CONTENTS

Page

FINDINGS AND RECOMMENDATIONS

FINDINGS AND RECOMMENDATIONS (CONTINUED) Page

EXECUTIVE SUMMARY

Why We Did This Audit

EGB is a key system used by more than 21,000 district employees (and charter schools) and helps manage the academic data of over 350,000 students in all grade levels.

Parents and students are able to log into their respective portals and view student academic information in near real-time.

Given the District-wide use of this critical system and applying our annual risk assessment, we determined that it was warranted that we review the internal controls and processes in place over EGB.

This audit was endorsed by the School Board's Audit and Budget Advisory Committee (ABAC) and subsequently approved by the School Board.

What We Recommended

We are making 18 recommendations to management to strengthen internal controls, accountability, and overall security of EGB, including:

- ♦ *Incorporating policies and procedures into the existing EGB handbook to result in a comprehensive manual to document the organization's processes and basic security requirements.*
- ♦ *Implementing automated software controls to minimize certain risks to student data.*
- ♦ *Improving the accuracy of data used by reviewers charged with ensuring that systems access is appropriate.*
- ♦ *Offering recommendations that improve security and streamline critical processes by users of the system.*

What We Found

This audit primarily focuses on an assessment of EGB security controls to provide reasonable assurance that the integrity of the system is properly managed, prevents unauthorized use or inappropriate disclosure of sensitive information, and that access to the system is proper and in accordance with the role of the system user.

In general, our audit shows that the District's use of the EGB software is accomplishing the goal of facilitating and modernizing the recording of student academic data as well as supporting the reporting requirements of the No Child Left Behind (NCLB) Act. Furthermore, this innovation enables parents to continuously monitor the academic progress of their child by making information easily available via Parent Portal in near real-time.

Some of the issues described in this report may necessitate programming and/or enhancements to the EGB product by the vendor. Also important to management's consideration in developing an implementation schedule for the proposed recommendations is the risk exposures and their potential impact.

Other recommendations are directly addressable by the District, such as incorporating EGB policies, procedures, and best practices into the existing EGB handbook to generate a comprehensive set of guidance to formally document the organization's rules regarding appropriate use of the system.

Documented procedures will clearly identify necessary steps that must be taken in order to accomplish a specific task, helps maintain a controlled outcome, and brings uniformity to system use. Together, documented policies and procedures help meet the requirements of a quality improvement process, increases security awareness, and serve as a single source for the dissemination of current and future criteria.

Through our audit tests, we found that EGB sessions do not “time out,” but remain active unless the computer was powered off or the user explicitly logs off. Also, multiple EGB sessions could be launched by the same user on different computers. In addition, the browser’s BACK feature will return the system to the last active EGB session if the user did not specifically log off of EGB or terminated the Internet session. The attendant risks are further increased due to the fact that EGB can be access by any browser on unsecure devices and networks. Combined, these factors increase the likelihood of having unauthorized open access to student information.

A particularly concerning deficiency with EGB is that a teacher can be “impersonated” by a grade book manager, who may change data that were initially input by that teacher without the teacher being notified of the change. A system-generated notification protocol should be developed to address this deficiency.

The length of the interval for the expiration of the network password, a matter previously reported on, continues to be a matter of concern to us. We continue to believe that shortening the existing network password change interval would improve EGB security.

Our audit also found the need to strengthen access controls. For example, we found numerous discrepancies regarding the number of users with elevated access and the role of these users as reported in the Resource Access Control Facility (RACF) report, a lack of awareness by charter school users of the policy regarding granting access to EGB, and inconsistent compliance review of the RACF report. There is a need for employing the principle of least privilege to EGB access.

We also found multiple methodologies – some inefficient – being used by school staff to reconcile daily student attendance and inconsistency in the timeliness of assigning permanent substitute teachers. Operationally, each of these conditions negatively impacts EGB and the accuracy of the information it contains. The impact on EGB could be minimized or contained if a functionally effective and appropriate method is developed for handling both of these routines.

We have made 18 recommendations, which would result in improved EGB security and accountability, for management's consideration and implementation.

Lastly, we plan on initiating a follow-up review of this system after some of the recommendations have been implemented, as this overview only addresses basic security measures and accountability.

TERMINOLOGY

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

EGB	Electronic Grade Book system
SOR	System of Record
ISIS	Integrated Student Information System
GBM	Grade Book Manager - an individual with elevated privileges within the EGB system
NSS	M-DCPS Network Security Standards – delineates security guidelines for M-DCPS
NIST	National Institute of Standards and Technology – a national organization charged with developing Information Technology (IT) security standards and guidelines for governmental information systems
COBIT	Control Objectives for Information and Related Technology - an internationally recognized framework of IT best practices, representing the consensus of experts, and is a generally accepted internal control framework for IT
VPN	Virtual Private Network (creates a secure path for the exchange of data for a user located in a remote location that is outside of the private network)
RACF	Resource Access Control Facility (provides systems access and controls)
PoLP	Principle of Least Privilege (generally accepted method of providing systems access based on need)

INTERNAL CONTROLS

This chart below summarizes our overall assessment of EGB security and controls:

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 secure	Data systems are mostly secure but can be improved	Systems are vulnerable to unauthorized access which may expose sensitive information
External Risk	None or low	Potential for damage	Severe risk of damage

BACKGROUND

In 2005, Miami-Dade County Public Schools (M-DCPS) began phasing out the traditional hand-written grade book format used to record student academic information. Global Scholar's Pinnacle Electronic Grade Book (EGB) was gradually implemented and is used today throughout the District in over 500 school sites, including charter schools.

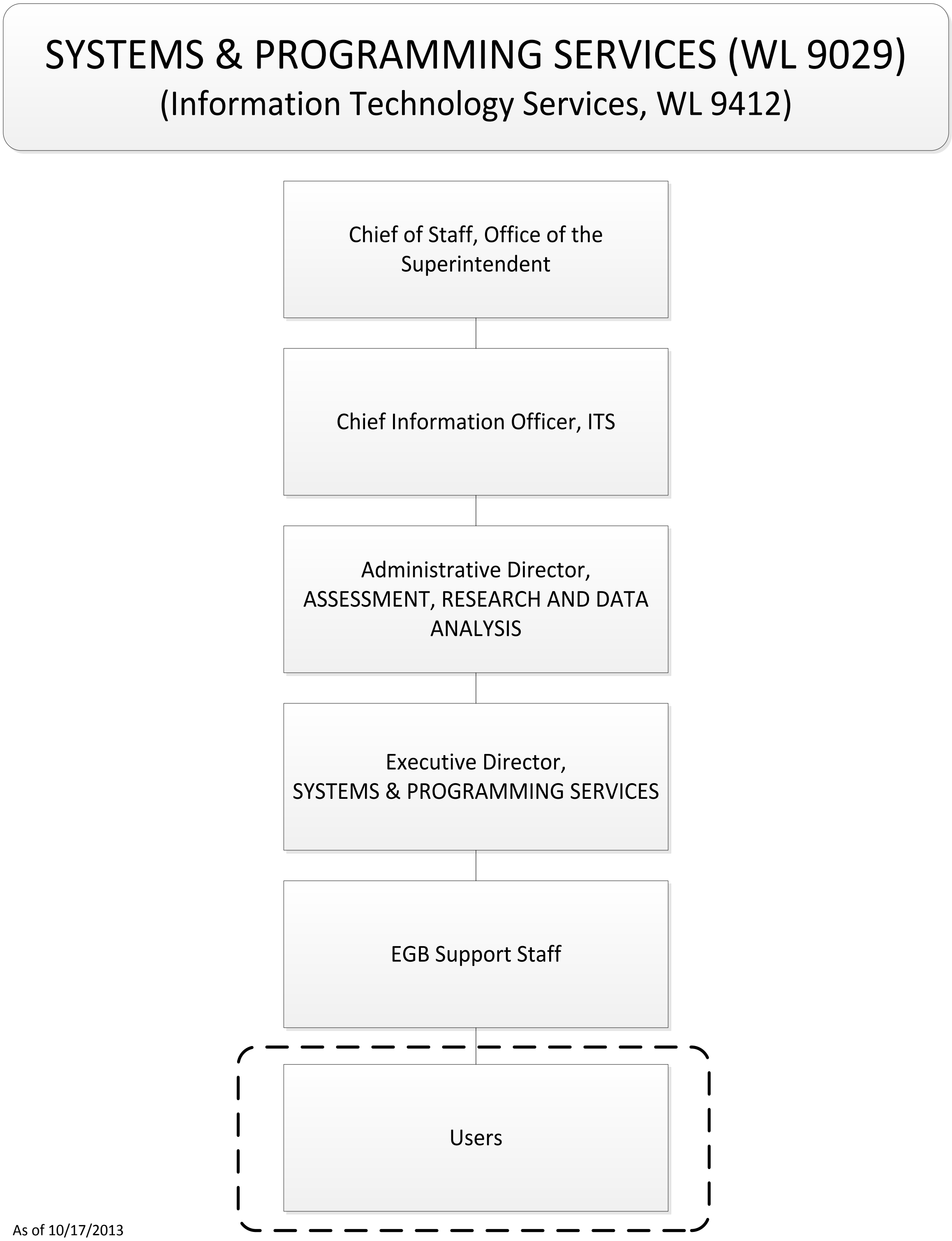
EGB is used for the recording of daily student attendance, grades, conduct, effort, and teacher comments. Authorized employees can access EGB via a website link embedded in the employee's Portal and requires no local installation. This implementation was a significant leap from the initial deployment, which required schools to manage their own EGB server.

EGB is essentially a front-end user interface (a "middle-man") to the system of record (SOR), ISIS (Integrated Student Information System), which is where EGB data ultimately resides. Instead of office staff entering student grade, attendance, and other data into ISIS on behalf of a teacher, the teacher enters the information directly into EGB which then transfers that data to ISIS.

Each school Principal designates certain staff members as primary contacts and administrators of the EGB, collectively referred to as grade book managers (GBMs). The attendance manager is responsible for managing student attendance data, including updating of attendance, and uploading the data daily to ISIS. The grades manager is similarly involved with the management of teacher profiles, grade updates, and overall support. These two distinct roles work together to manage the system and data of all students enrolled at the school. Each of these roles has at least one staff member designated as a backup.

The system is supported by technical staff from the District's IT department (ITS) as well as the product's vendor.

PARTIAL ORGANIZATIONAL CHART


SYSTEMS & PROGRAMMING SERVICES (WL 9029)
(Information Technology Services, WL 9412)
Chief of Staff, Office of the Superintendent
Chief Information Officer, ITS
Administrative Director, ASSESSMENT, RESEARCH AND DATA ANALYSIS
Executive Director, SYSTEMS & PROGRAMMING SERVICES
EGB Support Staff
Users

As of 10/17/2013

OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with the approved audit plan for FY 2012-2013, we have performed an audit of security and accountability controls for the District's Electronic Grade Book (EGB). The objectives of the audit were to provide reasonable assurance that the integrity of EGB and dependent systems is properly managed to prevent unauthorized use, inappropriate disclosure of sensitive information, and that access to the system is proper and in accordance with the role of the system user.

Accordingly, we reviewed existing policies and procedures including M-DCPS' Network Security Standards (NSS) as well as other applicable standards, namely the National Institute of Standards and Technology (NIST) Special Publication 800-53-R4, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4 and Control Objectives for Information and Related Technology (COBIT) 4.1.

The NIST is a national organization that is charged with developing Information Technology (IT) security standards and guidelines for governmental information systems. COBIT, an internationally recognized framework of IT best practices, represents the consensus of experts, and is a generally accepted internal control framework for IT.

We also reviewed various EGB literature, as well as internal and external[1] audit reports that may contain prior recommendations relevant to the current audit.

The scope of this audit encompasses current practices and procedures in place for the secure utilization and maintenance of the EGB and, to the extent they impact EGB, dependent systems.

[1] Florida Auditor General Report # 2011-099

We performed the following procedures to satisfy our audit objectives:

- Obtained an understanding of EGB and how other dependent systems interact with EGB.
- Performed specific tests of system operation.
- Analyzed methods used to grant and/or disable user access to the system.
- Reviewed the roles of users to determine appropriateness of user access based on need or role.
- Reviewed existing controls to ensure that student information entered into both the EGB and supporting systems is accurate, reported as intended by instructors, and protected.
- Analyzed the duties of users with elevated access to ensure that adequate segregation of duties exists.
- Interviewed school principals, teachers, and school support staff.

We visited 51 randomly selected schools, derived from a universe of 510 total schools currently utilizing EGB at the time of this audit.

We conducted this performance audit in accordance with generally accepted *Government Auditing Standards* issued by the Comptroller General of the United States of America. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives.

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 of 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 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.

This audit also included an assessment of applicable IT internal controls and compliance with the requirements of established policies, procedures and generally accepted standards and best practices.

[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 AND RECOMMENDATIONS:

1. POLICIES, PROCEDURES AND BEST PRACTICES SHOULD BE INCORPORATED INTO A CENTRALIZED EGB MANUAL

REFERENCED STANDARD
NIST AC-1 (ACCESS CONTROL POLICY AND PROCEDURES): *The organization should develop, document, and disseminate an access control policy that addresses: purpose, scope, roles, responsibilities, management's commitment, coordination among organizational entities, compliance, procedures to facilitate the implementation of the access control policy and associated access controls; and reviews and updates the current access control policy and procedures.*

We interviewed over 200 users, at various levels of EGB. Ninety-three percent (93%) of respondents interviewed indicated they were unaware of a policy and procedures manual for EGB. We performed follow-up auditing procedures, which corroborated interview responses that a comprehensive policy and procedures manual for EGB does not exist.

Rather than there being a single source for guidance for EGB users regarding acceptable use, we found that as the product and the District's use of it have matured over time, individual policies, procedures and directives have been distributed via email, weekly briefings (the District's information distribution tool), or the EGB support website. Consequently, EGB users must navigate various sources to obtain information on its proper use and functions. Moreover, there is open access to the EGB support website and most of the material found at this website is instructional and primarily aimed at ***"how to"*** use the software.

Given that this material provides general use instructions on how to use the software in M-DCPS, publishing it on the web (in front of the firewall), where it is available to the public makes navigation information easily available to those with dishonest intent. (Please refer to Finding No. 3)

RECOMMENDATIONS:

1.1 The District should incorporate existing EGB policies, procedures and best practices into a centrally managed EGB manual. This document should be centrally managed and updated when new policy is implemented and would strengthen controls over proper use of the product. The manual should be made, by reference, a part of the M-DCPS Network Security Standards and the District's Acceptable Use Policy.

MANAGEMENT RESPONSE:

ITS will incorporate by reference any centrally managed document into the Network Security Standards (NSS) and the Acceptable Use Policy (AUP). Procedures for use of the EGB were created based on the requirements listed in the District's Network Security Standards and the Acceptable Use Policy. ITS believes, however, that the EGB is a teacher tool and teachers must be as cognizant of the protection of the electronic version as they are of their paper version.

1.2 The District should also consider placing all tutorial material behind its firewall to make unauthorized use more difficult.

MANAGEMENT RESPONSE:

Information Technology Services (ITS) agrees with this recommendation in principal and will begin the process of putting this documentation in the Portal. Putting it behind the firewall will be much more difficult and will put an extra burden on staff, forcing them to install and use VPN just to read the documentation for using the grade book.

1.3 As a deterrent, the District should consider placing a "System Access/Use Notification" on the EGB user authentication landing page, advising of access/use policy, minimum browser requirements, the consequences of accessing EGB inappropriately or without authorization, and reminding that passwords are confidential.

MANAGEMENT RESPONSE:

ITS agrees with this recommendation and will begin the process of developing a "Splash"/disclaimer screen for users to read as they arrive at the landing page.

2. A CENTRALIZED EGB TIME-OUT POLICY AND LIMITING USER ACCESS TO A SINGLE EGB SESSION WOULD IMPROVE PROTECTION OF SENSITIVE STUDENT DATA

REFERENCED STANDARDS

NIST SC-10 (Network Disconnect):

The information system terminates the network connection associated with a communications session at the end of the session or after a specified time period of inactivity.

NIST AC-2.5 (Account Management | Inactivity Logout):

The organization requires that users log out when the organization-defined time period of expected inactivity or description of when to log out.

NIST AC-10 (Concurrent Session Control):

The information system limits the number of concurrent sessions for each account and/or account type to an organization-defined number.

NIST AC-11 (Session Lock):

The information system prevents further access to the system by initiating a session lock after a specified time period of inactivity or upon receiving a request from a user and retains the session lock until the user reestablishes access using established identification and authentication procedures.

NIST AC-12 (Session Termination):

The information system automatically terminates a user session after a specified condition or trigger events requiring session disconnect.

M-DCPS NETWORK SECURITY STANDARDS Revision, October 15, 2012 (4.1.2.7, Staff Security Responsibilities)

Application software that has built-in security functions must have these functions activated when this software involves confidential data. In addition, new software purchased to handle confidential data should have security capabilities as documented in sections 5.1 User ids and Passwords and 4.0 Non-Mainframe System Security.

A time-out for sensitive information systems resulting from user inactivity is an industry best practice. We interviewed school staff and teachers and found uncertainty as to whether or not a time-out mechanism existed for the EGB product. Sixteen percent (16%) of respondents indicated that EGB did time out, 48% answered that it does not time out, and 36% were not sure.

Upon testing, we determined that EGB sessions remained active unless the computer was powered off or the user explicitly logged off. Consequently, a user who walks away from an active session would provide open access to student information. Depending on the user's authorized level of access (e.g., Electronic Gradebook Manager), the school's entire student population could be exposed to unauthorized access and manipulation of student information.

We also tested and confirmed that multiple EGB sessions could be launched by the same user on different computers. This increases the likelihood of having an unattended EGB session running on a remote work station concurrently with an attended session. The risk that comes with the ability to initiate multiple EGB sessions, particularly when performed by a user with elevated access, such as an Electronic Gradebook Manager, is compounded by the lack of a timeout function.

We further tested the EGB application for restriction on access and found that if a user logs into EGB, completes any desired tasks in EGB, then moves on to another website by entering a new web address into the browser or simply closes the browser without explicitly logging off of EGB, the browser's BACK feature will return the user to an active EGB session.

RECOMMENDATION:

2.1 The District should work with the vendor to configure additional functionalities and security features into the EGB application in use at M-DCPS to ensure that:

- **EGB sessions automatically time-out or terminate after a specified period of inactivity. This could be achieved through a session lock as opposed to session termination.**

- **Multiple active sessions of EGB are not allowed and that an existing active session is automatically terminated before allowing another session to be opened by the same user.**

- **EGB sessions automatically terminate if a user leaves the session without explicitly ending it.**

MANAGEMENT RESPONSE:

ITS staff believes putting the EGB in the Portal would provide users with the Portal timeout, and would be a smoother transition for the user than having a separate timeout set in the application itself. We have confirmed that data entered into the EGB is saved automatically and so a lock of the account would leave the application open and the data updated after a user signs back in. This is important because originally we were told that the EGB would lose data entered prior to an automatic timeout if they have not manually performed a save. This would have been a major inconvenience for staff and would probably end up being a union issue. In addition, by having the application in the Portal, staff will have been required to read and sign off on the District's policies annually, including the NSS and the Acceptable Use Policy. This should have the effect of reinforcing their responsibilities as staff.

By way of explanation, the original planned sign-in appeared to be secure - this is why the EGB was not placed behind the Portal. However, there was a flaw whereby staff could save a shortcut that bypasses the security of the sign-in. Technical staff was unable to prevent exploitation of this vulnerability, despite multiple attempts to stop it.

ITS will explore the possibility of preventing multiple sessions with the vendor and whether a session can be ended automatically without loss of data.

3. EGB CAN BE ACCESSED FROM NON-SECURE DEVICES AND NETWORKS

REFERENCED STANDARDS

NIST SC-7 (Boundary Protection):
The information system monitors and controls communications at the external boundary of the system, at key internal boundaries within the system, implements sub networks for publicly accessible system components that are physically / logically separated from internal organizational networks and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
NIST AC-8 (System Use Notification):
The information system displays to users a notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: users are accessing an information system; usage may be monitored, recorded, and subject to audit; unauthorized use of the information system is prohibited and subject to criminal and civil penalties; use of the information system indicates consent to monitoring and recording; retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

The EGB login web page can be accessed by anyone by simply typing the appropriate web address into any browser, on any device, and from any location as long as wired or wireless internet connectivity is available, including unsecure networks.

We asked teachers in our sampled schools if they accessed EGB from outside their school. Thirty-six (36%) responded “yes,” while 64% said “no.” Extrapolating these results across the District’s roughly 21,000 full-time instructional teachers, suggest that a statistically estimated 7500 District teachers routinely access EGB from home or other networks and devices that are not subject to the

District’s control mechanisms, which include firewall, network access authentication, and anti-virus/anti-malware software.

It is important to note that, in addition to user logon, the EGB website provides for standard encryption using secure sockets layer (SSL) between the user and server. The concern addressed in this finding is not encryption between the user and the server. Rather, the concern is that EGB can be accessed from unsecure devices and networks due to where the server is logically placed.

Lastly, certain web browser versions are not supported or recommended by the EGB vendor. The vendor has published minimum browser requirements needed for full functionality as well as to support minimum security as stated by the manufacturer.

RECOMMENDATIONS:

3.1 The District should consider limiting EGB access exclusively through portal sign-on, as opposed to typing the address. This would significantly improve EGB security by requiring two controlled, sequential authentication steps by the user.

MANAGEMENT RESPONSE:

ITS believes putting the EGB into the Portal seems to be the most practical solution. It would increase security appreciably while any increase to required support would be minimal.

3.2 As a deterrent, the District should consider placing a "System Access/Use Notification" on the EGB user authentication landing page, advising of access/use policy, minimum browser requirements, the consequences of accessing EGB inappropriately or without authorization, and reminding that passwords are confidential, as published in a comprehensive EGB manual.

MANAGEMENT RESPONSE:

ITS can implement a "splash" screen reminding EGB users of their rights/responsibilities as outlined in the NSS and the AUP.

4. TEACHERS MAY BE UNAWARE OF CHANGES MADE BY USERS WITH ELEVATED EGB ACCESS

REFERENCED STANDARDS
NIST AU-10 (Non-Repudiation): *The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed an action.*

A GBM is a user with elevated privileges, allowing unrestricted access to all student information in EGB. GBMs function as the school's primary contact and manager of EGB and have the ability to review and modify information within EGB. For example, a GBM may modify or submit a student's grade on behalf of a teacher due to that teacher's absence. To accomplish this, a GBM "impersonates" the teacher and, in effect, "is the teacher" for the duration of the impersonation. When impersonating the teacher, the GBM has complete access to the teacher's class schedule and the ability to make changes to any of the instructor's student information.

We interviewed over 200 teachers and staff of which 73% indicated that they would be unaware of data that had been changed by a GBM. They indicated that some changes made by a GBM would not be obvious or known to them unless, they intentionally returns to a prior date within EGB and by chance notice the change based on their memory, or were following up on a change request. In a secondary school setting where a teacher may have over 100 students, it would be difficult or unlikely to notice an unrequested change.

Eight percent (8%) of respondents indicated that they were aware of or had experienced a situation where

EGB data had been changed inappropriately. These experiences came in different forms with some respondents more forthcoming than others as to where and when these instances of inappropriate changes occurred, many of which took place several years ago. We may follow up on those statements in a separate review in the future.

RECOMMENDATION:

4.1 The District should work with the vendor to implement an automatic, system-generated notification (such as an email) to the impersonated teacher whenever a GBM impersonates the teacher or modifies student data. In addition, EGB is currently configured so that updates made by an attendance manager are indicated by the field containing the change being highlighted and "locked." This feature should be duplicated to highlight changes made to student grades by anyone other than the assigned teacher.

MANAGEMENT RESPONSE:

ITS agrees that the vendor should implement a control that allows for a teacher to be notified if a grade is changed by an individual other than the teacher themselves.

5. SHORTENING THE EXISTING NETWORK PASSWORD EXPIRATION INTERVAL WOULD IMPROVE EGB SECURITY

REFERENCED STANDARD
NIST IA-5 (Authenticator Management): *The organization manages information system authenticators by: (sections f. and g.)* *f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;* *g. Changing/refreshing authenticators as per organization-defined time period by authenticator type;*

Currently, the District has a network password expiration policy in place where users must change their password at certain intervals throughout the year. EGB login is directly tied to this policy and is therefore subject to the existing change interval.

In February 2011, a State of Florida Auditor General report (2011-099) recommended that the District's network password expiration occur more frequently than what was then in current practice. In September 2011, a follow-up review of the District's adoption of that recommendation was completed by the Office of Management and Compliance Audits, which supported the Auditor General's recommendation. During the conduct of this audit, we noted that the password expiration policy had not changed as recommended.

By shortening the network password expiration policy as recommended, EGB and overall network security is improved.

RECOMMENDATION:

5.1 Although the District complies with the above referenced standard, we believe that the existing policy should be revisited. The District should consider decreasing the number of days incrementally to arrive at an interval that balances security, technical support overhead, and the school calendar as recommended by both the referenced Auditor General and internal audit reports in order to strengthen EGB password security.

MANAGEMENT RESPONSE:

Password expiration has been discussed within the District many times. Expiring passwords at the recommended level is considered a best practice within the information security community. However, experience has shown that in a District this size there are a number of password-related issues that affect the timely processing of instructional activities. This has caused us to back off this particular security practice and substitute the extra security provided by extra characters in the password.

District staff always has difficulty when passwords expire at inconvenient times. Some of these times include:

- *Just before a classroom instructional activity, causing an unforeseen delay or modification to the way the teacher must present the material,*
- *As testing is about to begin,*
- *At FTE time,*
- *At scheduling time,*
- *At grade reporting time,*
- *As deadlines approach on a particular project, or*
- *At high level meetings (such as the School Board) start.*

The District used the recommended level beginning with the mainframe systems, and continued it as applications moved to the network/web app/Intranet. However, as more and more District staff, including teachers began requiring access it was found that staff often struggled with password changes. Support requirements increased exponentially, even with our password self-help tool, and that support could not be provided in as timely a fashion as needed to allow for critical deadlines in systems above. In addition, all these applications and processes occur multiple times and at different portions the school year. As a result, the District chose to go to the current expiration so that for the most part, expirations can generally be set to occur at less strategic time during the school year.

6. CHARTER SCHOOLS' AWARENESS OF AND COMPLIANCE WITH ESTABLISHED EGB POLICIES AND PROCEDURES NEED IMPROVEMENT

REFERENCED STANDARDS
NIST AC-3 (Access Enforcement): *The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.* **NIST AC-6.7 (Least Privilege, Review of User Privileges):** *The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.* *The organization reviews the privileges assigned to validate the need for such privileges; and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.*

Charter schools are not required to use the District's EGB product but may elect to do so. Currently, the standard charter school contract provides for the option of using the District's EGB product. Charter schools that choose to use the District's EGB are bound, by contract, to comply with the District's EGB policies and procedures.

Of the seven charter schools visited during the conduct of this audit (representing 13% of the 51 sampled schools), six charter schools (85%) had some type of non-compliance with existing M-DCPS policies and best practices relating to EGB security.

Discrepancies such as incompatible role and the number of users were noted for users with elevated EGB access. Similar non-compliance was observed regarding other SOR applications used to support and manage data generated from EGB.

In addition, no evidence of periodic review of user-assigned privileges was presented for audit. In fact, none of the charter school principals were aware of where to obtain reports about systems access granted to charter employees.

All charter schools visited indicated that they were unsure about policies, procedures, or best practices regarding the number of users or roles. However, charter school principals were receptive to our recommendations.

RECOMMENDATIONS:

6.1 The district should communicate to and orientate charter schools on its EGB policies and procedures, including emphasizing to charter school principals the need to control elevated EGB and SOR access. Specifically, charter schools should be required to adopt and mirror existing controls in use at the district as stipulated in their contract.

MANAGEMENT RESPONSE:

In collaboration with ITS, the Office of Charter School Support will communicate to and orientate charter schools on its EGB policies and procedures, including emphasizing to charter school principals the need to control elevated EGB and SOR access.

6.2 The District should ensure that all existing charter school users have access to all policies, procedures, and best practices in use by the District for EGB. Future distribution to charter schools of EGB policies, procedures and best practices or notification of updates by the District should be documented.

MANAGEMENT RESPONSE:

The Office of Charter School Support can facilitate trainings regarding the EGB and the related policies, procedures, and best practices in use by the District as well as document the transfer of such information as well as acceptance.

7. SOME EGB AUTHORIZATIONS LISTED ON THE DISTRICT'S RACF REPORT ARE NOT RELIABLE

REFERENCED STANDARDS
NIST AC-3 (Access Enforcement): *The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.* **NIST AC-6 and 6.7 (Least Privilege, Review of User Privileges):** *The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational mission and business functions.* *The organization reviews the privileges assigned to validate the need for such privileges; and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.* **M-DCPS NETWORK SECURITY STANDARDS Revision, October 15, 2012 (Staff Security Responsibilities)** *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 like grade change.*

Two key EGB authorizations are delegated to school staff by the principal – EGB manager and EGB attendance manager. Granting EGB authorization to staff results in the user being placed into the appropriate network group, allowing the user to manage specific areas of EGB.

To enable and assist administrators in managing access, ITS produces a monthly report listing staff with elevated access to EGB. The Resource Access Control Facility (RACF) report is the only resource principals have available in order to review delegated EGB authorizations. Established practice requires principals to review the report monthly and make any necessary changes.

To make administrative review easier, some of the more critical authorizations (particularly the ones subject to audit) are extracted from the total report and compiled onto dedicated pages listing, for example, users who have elevated EGB access at the school.

Our review of 51 schools compared the relevant network groups with the RACF report. Inconsistencies were found throughout where the two sources did not match. For example, dedicated pages did not match the listings in the overall report or the network groups. Specifically, members of the network groups were not consistently listed on the dedicated pages. We found approximately 71 instances of this condition within the sample group. This is significant, since users who have elevated access to EGB may go undetected.

We tested users who were members of the network group but not listed on the dedicated pages and concluded that the users did indeed have elevated EGB access and in some cases, the principal was unaware.

Due to the exigent nature of the condition discovered and upon confirmation, we immediately brought it to the attention of the District's data security team prior to the publication of this report. As a result, they were able to identify the cause and correct it, therefore generating an accurate report for use by administrative reviewers.

In addition, the RACF report available to charter schools lacks employee job description detail, making proper role determination by a reviewing administrator more difficult. Furthermore, some former District and charter school employees with elevated access, who had been terminated for an extended period of time, continued to appear on the report.

Lastly, RACF report run dates are not consistent. For example, at the time of this review, all previous runs of the report were generated on a different date for each of the seven archived months reviewed, as opposed to being run on a set date each month (e.g., the last day of the month). Such consistency would result in predictability and assist school principals in their task management related to review of the RACF report.

RECOMMENDATIONS:

7.1 The administration should consider incorporating the established practice of monthly RACF review into the recommended comprehensive EGB manual. Also, the District should consider including RACF policy statements on the RACF authorization report for easy reference by reviewing administrators.

MANAGEMENT RESPONSE:

This requirement is currently listed in the Network Security Standards (NSS) section 4.1.4 (Authorizations and Access), bullet 2 and section 5.0 (Staff Security Responsibilities), bullet 13, which require that the most recent report always be printed, reviewed, signed, and kept by the local supervisor for audit purposes. Reviewing every month is implied by the act of always printing off the most recent listing. Compliance with the NSS is required by Board Policy 7540.04 - STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY and other Board policies.

7.2 The District should review the RACF authorization report generated for charter school users and determine if employee job description detail can be populated onto the report to help ensure proper role determination by reviewing administrators.

MANAGEMENT RESPONSE:

The District has distinct HR systems for M-DCPS and Charter employees. The current system of record for M-DCPS employees is SAP-based, and back-feeds PERS. The

Charter HR system, ACES, is a stand-alone, disparate system that provides employee information in a different format but does have a form of job description for Charter staff. It should be noted that we have no way of knowing how accurate the job description entered into ACES is. In order to provide the same information for both M-DCPS and Charter employees, the job would need to be significantly reworked, and/or a rewrite/modification to ACES would be required. It might also require that the charter schools use job titles, descriptions, etc. that are similar to what the District uses. Both options would potentially require significant investment of time and technical resources. ITS will analyze what it will take to modify the programs.

In addition, the Charter School Office would have to be the District department to do a review of Charter School Authorizations or require the local site supervisors to do it. ITS cannot make a determination of what authority the Charter School Office has in this area.

7.3 The job producing the RACF report should be scheduled to run consistently on the same day of each month to provide predictable report availability to administrators.

MANAGEMENT RESPONSE:

The job in question that produces CONTROL-D report T0802E0101 is run on the second Tuesday of every month. The reason for the schedule takes into account a number of concerns, such as additional jobs scheduled to run at various other intervals weekly and the need to appropriately manage/distribute system overhead to ensure successful and efficient completion of critical business functions. Issues include not running at times other important systems are running (like Payroll), not running on nights when it could not finish in time to activate CICS by at 5:30 AM, job dependencies that require other processes be finished (like HR updates to handle terminations), etc. In addition, other RACF jobs also run automatically on Tuesdays. The result would be the same if this job was moved to the end of the month – it would not always run on the 28th, 30th, or 31st. It would need to run on the last Tuesday of the month, as Tuesday runs have been determined to be the day that have the least effect on other systems. Moreover, to run on the last day of the month, some of the programming would have to be changed, the CNTL-D system would require major schedule modification, and other production jobs would have to be moved to make sure there is no conflict.

8. ELEVATED EGB AUTHORIZATIONS REQUIRE COMPLIANCE REVIEWS

REFERENCED STANDARDS

NIST AC-3 (Access Enforcement):

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

NIST AC-6 (Least Privilege), AC-6.5 (Privileged Accounts), AC-6.7 (Review of User Privileges):

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

The organization restricts privileged accounts on the information system to organization-defined personnel or roles.

The organization reviews the privileges assigned to validate the need for such privileges; and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

M-DCPS Weekly Briefing # 7784

To provide operational language for access to the electronic Grade Book Manager (WGBM) and Attendance Manager (WGBA). By via of this weekly briefing, the following operational policy must be enforced, immediately.

- *A maximum of 5 staff approvers may be granted access to the WGBM and WGBA application, as defined below:*
- *Principal, Assistant Principal, Registrar or person identified as the registrar*
- *One primary Gradebook Manager/Attendance Manager (Instructional or Clerical), One Clerical selected by the principal, Hourly individuals identified for this purpose may be utilized*
    - *Access must be limited to administrators, instructional or clerical personnel, only. This excludes personnel such as, but not limited to: Security, Bus Drivers, Microsystem Technicians/Computer Specialists, Cafeteria Personnel, Custodial Staff*
- *Management & Compliance Audits will be reviewing appropriate access to these applications.*

REFERENCED STANDARDS (continued)

M-DCPS NETWORK SECURITY STANDARDS Revision, October 15, 2012 (4.0, Non-mainframe System Security)

Programmatic methods are to be used to control access to non-mainframe resources. These methods include defining specific users or groups to specific system resources, and use of the "least privilege" concept for access to all system-level resources such as the operating system, utilities, and databases. "Least privilege" is defined as a default of no access to these resources and the requirement of explicit permission and authorization by the owner based on need.

In 2010, Internal Audits recommended that School Operations develop a policy regarding elevated EGB access. The resultant policy states which roles and the number of staff that may be given elevated access to EGB. Established practice requires principals to review the RACF report (see Finding 7) on a monthly basis, make and annotate the changes, and file the report for audit purposes.

Our review indicates that enforcement of this policy is haphazard, resulting in an excess number of staff (exclusive of the primary or backup user) with elevated access to EGB. Of the 51 schools visited, approximately 19 (37%) were found to have exceeded established policy regarding the number of users with elevated EGB access.

Our interviews indicate that some staff with elevated access either never use the system in a manager capacity or were unaware that they had elevated access.

The principle of least privilege (PoLP) is a commonly accepted standard for computer and data security, recommending that system users have only those privileges which are essential to perform that user's duties, and therefore helping to limit exposure to risk.

RECOMMENDATION:

8.1 Principals should be required to review the RACF authorizations report on a monthly basis to determine compliance with established policy regarding the role and number of staff members with elevated EGB access. Monthly review would help mitigate the large number of users who have elevated access, but claimed to never work with the system. Users that do not support the system should have manager-level access canceled.

MANAGEMENT RESPONSE:

The NSS requires periodic review of the RACF reports that list all staff access. This includes but is not limited to administrative access to the EGB. The report is produced on a monthly basis and is available to the local site supervisors of all locations, including school principals. A requirement to review these reports every month for EGB access would have to come from School Operations.

9. STANDARDS FOR REPORTING STUDENT ATTENDANCE SHOULD BE DEVELOPED

Student attendance information is transferred daily from EGB to the SOR using various codes to describe each student's attendance classification. For various reasons, student attendance may change from what was initially submitted by the home room teacher at the beginning of the day. Changes to student attendance data are usually executed by the EGB manager.

Our interviews with employees revealed five different methods in use by staff for the daily reconciliation of student attendance once the data has been uploaded from EGB to the SOR:

1. The attendance manager communicates with teachers via phone or email and uses the information received to update student attendance.

2. A report is printed by the EGB manager using the SOR, centrally posted, and annotated by teachers throughout the day to indicate changes. This is the most frequently used method. Due to the compressed format of the legacy report, notations and other indications made by teachers are often difficult to understand. About 30% of both teachers and staff that must interpret the report expressed displeasure with its compactness and propensity for legibility errors.

3. The EGB manager prints a report using the SOR and places it in each teacher's physical mailbox. Teachers review and annotate the report, then return it to the EGB manager who uses it to update attendance information, reducing errors over the two methods previously described.

4. A report is printed from the SOR, scanned, and emailed by the EGB manager to all teachers for response in order to indicate changes. Teachers and staff interviewed preferred this method, which also created a verifiable email trail and reduced errors, over the preceding method.

5. A “Teacher Attendance Download System (TADL)” software is used by the EGB manager to provide a customized (specific to the teacher) attendance report sent via email to teachers for response in order to indicate or approve changes. Schools utilizing this method showed overwhelming support for both the verifiable email trail as well as the customized report showing only students assigned to a particular teacher instead of all attendance discrepancies for every student on that day.

   Based on our analysis of the processes described to us during our interviews with teachers and EGB managers that are tasked with accurately interpreting and posting student attendance information and our review of the documents used in these processes, we have concluded that there is a need to redesign the student attendance reconciliation process. The aim of the redesign would be to:

   - Reduce the number of documented student attendance reporting errors

   - Properly document the reason for changes to a student’s attendance information

   - Ensure that student attendance information in EGB matches the SOR

   - Improve overall security and accountability to the daily attendance reconciliation process

- Bring consistency to how attendance changes are managed by establishing a uniform method for reconciling student attendance data in both systems district-wide

RECOMMENDATION:

9.1 The administration should review the various methods used for reconciling student attendance and select or develop a functionally effective and appropriate method to be used district-wide and document the method in the EGB manual.

MANAGEMENT RESPONSE:

ITS staff, and District decision-making in general, has tended towards allowing schools to have the latitude to use the attendance mechanism that works for them. Developing a single process will require input from School Operations and the Attendance Office. Recommended reports for reconciliation procedures are currently included in the document Attendance Manager Reference Guide and Procedures.

10. LACK OF TIMELY ASSIGNMENT OF PERMANENT SUBSTITUTE TEACHERS IS IMPACTING EGB

REFERENCED STANDARDS
M-DCPS NETWORK SECURITY STANDARDS Revision, October 15, 2012, User IDs and Passwords *Staff must not engage in any activity that may reveal or otherwise compromise their own or another user's password.* **NIST AC-8 (System Use Notification):** *The information system displays to users a notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: users are accessing an information system; usage may be monitored, recorded, and subject to audit; unauthorized use of the information system is prohibited and subject to criminal and civil penalties; use of the information system indicates consent to monitoring and recording; retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.* **NIST, AU-12 (Audit Generation)** *The information system provides audit record generation capability for the auditable events defined in AU-2 a. (Determines that the information system is capable of auditing events); and allows [appropriate staff] to select which auditable events are to be audited by specific components of the information system; and generates audit records for the events defined in AU-2 d. (Determines that [certain] events are to be audited within the information system, along with the frequency of (or situation requiring) auditing for each identified event) with the content defined in AU-3. (The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.)*

Before a teacher begins an approved leave of absence, he or she may decide to use accumulated sick leave. This is an example of a situation where an incumbent teacher's position is technically still occupied although the teacher is physically absent from the classroom.

The District has a process whereby a principal can request that the incumbent teacher be moved into an "8200" position classification; essentially a place-holder where an employee who is or will be on leave can remain until his/her leave ends. This allows a school to backfill the position with a "permanent substitute".

A permanent substitute is an instructional employee who substitutes for the incumbent teacher, usually for 30 work days or more. Since a permanent substitute is assuming the outgoing teacher's schedule for an extended period of time, a permanent substitute requires access to EGB. Once the permanent substitute is placed into the incumbent's slot created through the 8200 process, the permanent substitute automatically receives EGB access for the classes being taught by the incumbent teacher – usually within a day.

Our fieldwork showed that the handling of permanent substitute EGB access and the ability to post student information in a timely manner was not consistent:

- Some schools may not be appropriately familiar with the 8200 procedure, the critical need to efficiently handle the leave process, and the resulting impact to EGB.

- Interviews with teachers, support staff, EGB managers, and permanent substitutes indicated that a permanent substitute gains access to EGB between a few days and up to five weeks after having begun substituting.

  This creates a condition whereby the permanent substitute must repeatedly provide student data to an EGB manager for entry into EGB or stockpile data for later entry upon obtaining access. Some permanent substitutes communicated with incumbent teachers on leave who then entered student data into EGB on behalf of the substitute.

- Some teachers on leave have shared their network password with the permanent substitute as a workaround while the substitute waits for access to EGB as described in the above narrative.

- Since EGB is tied to Parent Portal, delays in entering student data may result in parents not having the latest information on their child's progress.

In addition to interviews, a request for data was made in order to test the extent to which instructional employees on leave were accessing and/or updating EGB data. The request for data included about 300 employees during the 2012-2013 academic years. According to the vendor, currently, extraction of these data was not possible; but was expected to be resolved in the next release of the software.

RECOMMENDATIONS:

10.1 The administration should provide periodic reminders to school principals of the need to grant EGB access to permanent substitute teachers in a timely manner.

MANAGEMENT RESPONSE:

This process would have to be developed by School Operations and the Attendance Office, with input from ITS EGB support and development staff, representative school staff, and security.

10.2 All EGB users should be periodically reminded that their network password must not be disclosed and the potential consequences to EGB data. As a deterrent, the District should consider placing a "System Access/Use Notification" on the EGB user authentication landing page, advising of access/use policy, minimum browser requirements, the consequences of accessing EGB inappropriately or without authorization, and reminding that passwords are confidential.

MANAGEMENT RESPONSE:

ITS can implement a "splash" screen reminding EGB users of their rights/responsibilities as outlined in the NSS and the AUP. In addition, weekly Briefings to this effect were sent out to all employees on 06/09/2011 (#10003) and 10/04/2012 (#12694).

10.3 The District should continue to work with the vendor to ensure future releases / updates of EGB include the functionality to extract data for audit and review purposes.

MANAGEMENT RESPONSE:

ITS has noted this recommendation and will apprise the vendor of this issue.

FULL TEXT OF MANAGEMENT'S RESPONSE

MEMORANDUM **March 4 , 2014**

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

FROM: Milagros R. Fornell, Chief of Staff MF

SUBJECT: RESPONSES TO OFFICE OF MANAGEMENT AND COMPLIANCE AUDITS RECOMMENDATIONS FOR ELECTRONIC GRADE BOOK

Attached please find the responses to the recommendations made in the Audit of Electronic Grade book Security and Controls. Through my office, ITS will work with all parties involved in this audit.

I can be reached at 305 995-1206.

MRF:mja
M051

cc: Superintendent's Cabinet
Ms. Valtena G. Brown
Ms. Deborah Karcher

1.1 The District should incorporate existing EGB policies, procedures and best practices into a centrally managed EGB manual. This document should be centrally managed and updated when new policy is implemented and would strengthen controls over proper use of the product. The manual should be made, by reference, a part of the M-DCPS Network Security Standards and the District's Acceptable Use Policy.

1.1 ITS will incorporate by reference any centrally managed document into the Network Security Standards (NSS) and the Acceptable Use Policy (AUP). Procedures for use of the EGB were created based on the requirements listed in the District's Network Security Standards and the Acceptable Use Policy. ITS believes, however, that the EGB is a teacher tool and teachers must be as cognizant of the protection of the electronic version as they are of their paper version.

1.2 The District should also consider placing all tutorial material behind its firewall to make unauthorized use more difficult.

1.2 Information Technology Services (ITS) agrees with this recommendation in principal and will begin the process of putting this documentation in the Portal. Putting it behind the firewall will be much more difficult and will put an extra burden on staff, forcing them to install and use VPN just to read the documentation for using the grade book.

1.3 As a deterrent, the District should consider placing a "System Access/Use Notification" on the EGB user authentication landing page, advising of access/use policy, minimum browser requirements the consequences of accessing EGB inappropriately or without authorization, and reminding that passwords are confidential.

1.3 ITS agrees with this recommendation and will begin the process of developing a "Splash"/disclaimer screen for users to read as they arrive at the landing page.

2.1 The District should work with the vendor to configure additional functionalities and security features into the EGB application in use at M-CPS to ensure that:

- **EGB automatically time-out or terminate after a specific period of activity. This could be achieved through a session lock as opposed to session termination.**

- **Multiple active sessions of EGB are not allowed and that an existing active session is automatically terminated before allowing another session to be opened by the same user.**
- **EGB sessions automatically terminate if a user leaves the session without explicitly ending it.**

2.1 ITS staff believes putting the EGB in the Portal would provide users with the Portal timeout, and would be a smoother transition for the user than having a separate timeout set in the application itself. We have confirmed that data entered into the EGB is saved automatically and so a lock of the account would leave the application open and the data updated after a user signs back in. This is important because originally we were told that the EGB would lose data entered prior to an automatic timeout if they have not manually performed a save. This would have been a major inconvenience for staff and would probably end up being a union issue. In addition, by having the application in the Portal, staff will have been required to read and sign off on the District's policies annually, including the NSS and the Acceptable Use Policy. This should have the effect of reinforcing their responsibilities as staff.

By way of explanation, the original planned sign-in appeared to be secure - this is why the EGB was not placed behind the Portal. However, there was a flaw whereby staff could save a shortcut that bypasses the security of the sign-in. Technical staff was unable to prevent exploitation of this vulnerability, despite multiple attempts to stop it.

ITS will explore the possibility of preventing multiple sessions with the vendor and whether a session can be ended automatically without loss of data.

3.1 The District should consider limiting EGB access exclusively through portal sign-on, as opposed to typing the address. This would significantly improve EGB security by requiring two controlled, sequential authentication steps by the user.

3.1 ITS believes putting the EGB into the Portal seems to be the most practical solution. It would increase security appreciably while any increase to required support would be minimal.

3.2 As a deterrent, the District should consider placing a "System Access/Use

Notification" on the EGB user authentication landing page, advising of access/use policy, minimum browser requirements, the consequences of accessing EGB inappropriately or without authorization, and reminding that passwords are confidential, as published in a comprehensive policy and procedures manual.

3.2 ITS can implement a “splash” screen reminding EGB users of their rights/responsibilities as outlined in the NSS and the AUP.

4.1 The District should work with the vendor to implement an automatic, system-generated notification (such as an email) to the impersonated teacher whenever a GBM impersonates the teacher or modifies student data. In addition, EGB is currently configured so that updates made by an attendance manager are indicated by the field containing the change being highlighted and “locked.” This feature should be duplicated to highlight changes made to student grades by anyone other than the assigned teacher.

4.1 ITS agrees that the vendor should implement a control that allows for a teacher to be notified if a grade is changed by an individual other than the teacher themselves.

5.1 Although the District complies with the above referenced standard, we believe that the existing policy should be revisited. The District should consider decreasing the number of days incrementally to arrive at an interval that balances security, technical support overhead, and the school calendar as recommended by both the referenced Auditor General and internal audit reports in order to strengthen EGB password security.

5.1 Password expiration has been discussed within the District many times. Expiring passwords at the recommended level is considered a best practice within the information security community. However, experience has shown that in a District this size there are a number of password-related issues that affect the timely processing of instructional activities. This has caused us to back off this particular security practice and substitute the extra security provided by extra characters in the password.

District staff always has difficulty when passwords expire at inconvenient times. Some of these times include:

- Just before a classroom instructional activity, causing an unforeseen delay or modification to the way the teacher must present the material,
- As testing is about to begin,
- At FTE time,
- At scheduling time,
- At grade reporting time,
- As deadlines approach on a particular project, or

- At high level meetings (such as the School Board) start.

The District used the recommended level beginning with the mainframe systems, and continued it as applications moved to the network/web app/Intranet. However, as more and more District staff, including teachers began requiring access it was found that staff often struggled with password changes. Support requirements increased exponentially, even with our password self-help tool, and that support could not be provided in as timely a fashion as needed to allow for critical deadlines in systems above. In addition, all these applications and processes occur multiple times and at different portions the school year. As a result, the District chose to go to the current expiration so that for the most part, expirations can generally be set to occur at less strategic time during the school year.

6.1 The district should communicate to and orientate charter schools on its EGB policies and procedures, including emphasizing to charter school principals the need to control elevated EGB and SOR access. Specifically, charter schools should be required to adopt and mirror existing controls in use at the district as stipulated in their contract.

6.1 In collaboration with ITS, the Office of Charter School Support will communicate to and orientate charter schools on its EGB policies and procedures, including emphasizing to charter school principals the need to control elevated EGB and SOR access.

6.2 The District should ensure that all existing charter school users have access to all policies, procedures, and best practices in use by the District for EGB. Future distribution to charter schools of EGB policies, procedures and best practices or notification of updates by the District should be documented.

6.2 The Office of Charter School Support can facilitate trainings regarding the EGB and the related policies, procedures, and best practices in use by the District as well as document the transfer of such information as well as acceptance.

7.1 The administration should consider incorporating the established practice of monthly RACF review into the recommended comprehensive EGB manual. Also, the District should consider including RACF policy statements on the RACF authorization report for easy reference by reviewing administrators.

7.1 This requirement is currently listed in the Network Security Standards (NSS) section 4.1.4 (Authorizations and Access), bullet 2 and section 5.0 (Staff Security Responsibilities), bullet 13, which require that the most recent report always be printed, reviewed, signed, and kept by the local supervisor for audit purposes. Reviewing every month is implied by the act of always printing off the most recent listing. Compliance with the NSS is required by Board Policy 7540.04 - STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY and other Board policies.

7.2 The District should review the RACF authorization report generated for charter school users and determine if employee job description detail can be populated onto the report to help ensure proper role determination by reviewing administrators.

7.2 The District has distinct HR systems for M-DCPS and Charter employees. The current system of record for M-DCPS employees is SAP-based, and back-feeds PERS. The Charter HR system, ACES, is a stand-alone, disparate system that provides employee information in a different format but does have a form of job description for Charter staff. It should be noted that we have no way of knowing how accurate the job description entered into ACES is. In order to provide the same information for both M-DCPS and Charter employees, the job would need to be significantly reworked, and/or a rewrite/modification to ACES would be required. It might also require that the charter schools use job titles, descriptions, etc. that are similar to what the District uses. Both options would potentially require significant investment of time and technical resources. ITS will analyze what it will take to modify the programs.

In addition, the Charter School Office would have to be the District department to do a review of Charter School Authorizations or require the local site supervisors to do it. ITS cannot make a determination of what authority the Charter School Office has in this area.

7.3 The job producing the RACF report should be scheduled to run consistently on the same day of each month to provide predictable report availability to administrators.

7.3 The job in question that produces CONTROL-D report T0802E0101 is run on the second Tuesday of every month. The reason for the schedule takes into account a number of concerns, such as additional jobs scheduled to run at various other intervals weekly and the need to appropriately manage/distribute system overhead to ensure successful and efficient completion of critical business functions. Issues include not running at times other important systems are running (like Payroll), not running on nights when it could not finish in time to activate CICS by at 5:30 AM, job dependencies that require other processes be finished (like HR updates to handle terminations), etc. In addition, other RACF jobs also run automatically on Tuesdays. The result would be the same if this job was moved to the end of the month – it would not always run on the 28th, 30th, or 31st. It would need to run on the last Tuesday of the month, as Tuesday runs have been determined to be the day that have the least effect on other systems. Moreover, to run on the last day of the month, some of the programming would have to be changed, the CNTL-D system would require major schedule modification, and other production jobs would have to be moved to make sure there is no conflict.

8.1 Principals should be required to (*review?*) the RACF authorizations report on a monthly basis to determine compliance with established policy regarding the role and number of staff members with elevated EGB access. Monthly review would help mitigate the large number of users who have elevated access, but claimed to never work with the system. Users that do not support the system should have manager-level access canceled.

8.1 The NSS requires periodic review of the RACF reports that list all staff access. This includes but is not limited to administrative access to the EGB. The report is produced on a monthly basis and is available to the local site supervisors of all locations, including school principals. A requirement to review these reports every month for EGB access would have to come from School Operations.

9.1 The administration should review the various methods used for reconciling student attendance and select or develop a functionally effective and appropriate method to be used district-wide and document the method in the EGB manual.

9.1 ITS staff, and District decision-making in general, has tended towards allowing schools to have the latitude to use the attendance mechanism that works for them. Developing a single process will require input from School Operations and the Attendance Office. Recommended reports for reconciliation procedures are currently included in the document Attendance Manager Reference Guide and Procedures.

10.1 The administration should provide periodic reminders to school principals of the need to grant EGB access to permanent substitute teachers in a timely manner.

10.1 This process would have to be developed by School Operations and the Attendance Office, with input from ITS EGB support and development staff, representative school staff, and security.

10.2 All EGB users should be periodically reminded that their network password must not be disclosed and the potential consequences to EGB data.

As a deterrent, the District should consider placing a "System Access/Use Notification" on the EGB user authentication landing page, advising of access/use policy, minimum browser requirements, the consequences of accessing EGB inappropriately or without authorization, and reminding that passwords are confidential.

10.2 ITS can implement a “splash” screen reminding EGB users of their rights/responsibilities as outlined in the NSS and the AUP. In addition, weekly Briefings to this effect were sent out to all employees on 06/09/2011 (#10003) and 10/04/2012 (#12694).

10.3 The District should continue to work with the vendor to ensure future releases / updates of EGB include the functionality to extract data for audit and review purposes.

10.3 ITS has noted this recommendation and will apprise the vendor of this issue.

Miami-Dade County Public Schools Anti-Discrimination Policy

Federal and State Laws

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

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

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

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

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

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

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

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

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

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

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

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

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

Veterans are provided re-employment rights in accordance with P.L. 93-508 (Federal Law) and Section 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.

Revised: (05.12)

INTERNAL AUDIT REPORT

Audit of Electronic Grade Book
Security and Controls

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