INTERNAL AUDITOR'S REPORT

SOUTH CAROLINA
DEPARTMENT OF TRANSPORTATION

COLUMBIA, SOUTH CAROLINA

FOLLOW-UP TO THE OFFICE OF CHIEF INTERNAL AUDITOR'S AUDIT OF THE SITEMANAGER CONSTRUCTION MANAGEMENT SYSTEM

REPORT DATE: JANUARY 17, 2017

CONTENTS

FOREWORD

In 2007, Act 114 of the South Carolina General Assembly created the Office of the Chief Internal Auditor (OCIA) as a function of the South Carolina Department of Transportation Commission to establish, implement, and maintain the exclusive internal audit function of all departmental activities. The General Assembly transferred the function, beginning July 1, 2016, pursuant to Act 275, to the South Carolina Office of the State Auditor. We established the division of Internal Audit Services as an independent, objective assurance and consulting function designed to add value and improve the operations of the South Carolina Department of Transportation (SCDOT). This report covers one of a number of engagements that we carried forward from the January 2016 audit plan developed by the OCIA with input from SCDOT management.

South Carolina
Office of the State Auditor

George L. Kennedy, III, CPA
State Auditor

INTERNAL AUDITOR'S REPORT

January 17, 2017

Ms. Christy A. Hall, Secretary of Transportation
and
Members of the Commission
South Carolina Department of Transportation
Columbia, South Carolina

We have completed a follow-up to the Office of the Chief Internal Auditor's (OCIA) audit of the SiteManager Construction Management System. The objective of this follow-up was to determine the status of the recommendations detailed in the report dated June 24, 2010.

We planned and performed our follow-up with due professional care in order to obtain sufficient, appropriate evidence to provide a reasonable basis for our observations and conclusions. For purposes of this report, observations are defined as insufficient actions by management to effectively respond to the OCIA's prior audit findings. We noted no observations as a result of our testing.

George L. Kennedy, III

George L. Kennedy, III, CPA
State Auditor

EXECUTIVE SUMMARY

BACKGROUND

The Office of the Chief Internal Auditor (OCIA) reviewed the SiteManager Construction Management System to determine the effectiveness and efficiency of the system in managing construction projects and to determine the adequacy of internal controls to protect access to and integrity of information. That audit included the following objectives:

- Evaluate the controls in place to protect access and integrity of application information.
- Evaluate the controls in place for information processing.
- Evaluate controls related to data output.
- Evaluate controls related to the user access rights to the application to include terminated employees and transfers.
- Evaluate the controls in place for program changes.
- Ensure that the department has a disaster recovery plan and that the application is tested and updated regularly.

OBJECTIVES

The objective of this follow-up was to determine the status of the recommendations detailed in the SiteManager report dated June 24, 2010.

SCOPE

The follow-up audit was limited to a review of Management's Response to the findings and recommendations detailed in the original report. The audit scope covered the current SiteManager processes in place during the fiscal year ending June 30, 2017.

METHODOLOGY

To accomplish our audit objective, we reviewed policies and procedures related to SiteManager, obtained and reviewed support documentation, and conducted interviews with management and staff of the SCDOT Construction Office. We reviewed SiteManager processes, policies, procedures, reports and queries. We performed relevant test work on documentation supporting management's actions addressing the OCIA recommendations.

CONCLUSION

We determined that 12 of the 12 OCIA recommendations have been fully implemented. Details of our follow-up are described in the OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS section of the report.

OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS

Recommendation 1

The Office of the Chief Internal Auditor (OCIA) recommended that the policies/procedures provide a flow chart to represent business processes and the flow of data between different processes and entities. The illustration should explain the course or movement of information and flow of information in the construction process based on inputs and outputs. Also, the flowchart should illustrate technical or business processes with the data flowing from one process to another and the results. OCIA recommended that other precautions (validations) be implemented directly into the application to enforce referential integrity (prevents users from changing or deleting a record if matching records exist in a related table) throughout the input of data in SiteManager. This will ensure that inconsistent data is not allowed to enter the system or update the master file.

Management Response

Management agreed with the need for a flowchart to show the workflow processes, especially representing how data is moved from one system to another and the outputs from each. Management also asserted that SiteManager enforces referential integrity throughout the application, maintaining parent and child relationships and preventing those primary keys from being deleted or changed. Management further acknowledged the need to clean up the master lists for Contractor Equipment and Personnel to help reduce duplication in those areas

Status: Implemented

We were able to conclude management has taken actions to depict the data input and output for SiteManager. We also confirmed the existence of referential integrity within SiteManager.

OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS (CONTINUED)

Recommendation 2

OCIA recommended having as many pre-populated fields (e.g., Contractor Name, Location) as allowed by the software to prevent data entry errors. OCIA also recommend adding prompting to the Daily Work Reports' Contractors, Contractors Equipment, and Work Items tabs to ensure that areas aren't overlooked or skipped and to ensure the uniformity of data entry. The list should be scrubbed for erroneous inputs.

Management Response

Management responded that as a result of SiteManager being jointly developed by a number of entities nationwide, SCDOT was unable to modify the source code. Management further asserted that SCDOT was working with the Transport Users Group (TUG) to have a number of the recommendations from the SiteManager audit to be incorporated into future versions of the generic application.

Status: Implemented

The Daily Work Report (DWR) within SiteManager is utilized to document activity on a construction project. The DWR includes information such as items of work performed, quantities installed, number of contractor and inspection personnel present, and equipment utilized. The DWR should also include any significant events, conversations, and other such related activity that occur during the workday.

The information entered on the DWR is expected to be detailed, accurate, and thorough to ensure that those not associated with the project on a daily basis can fully understand the events as they occurred. A DWR should be generated each calendar day starting with the Notice to Proceed date and continuing until the project is complete.

The DWR also has various sections such as information **(DWR Info.)**, Contractors' equipment **(Contractor Equip.), Daily Staff,** and **Work Items** which contain fields that are automatically populated. For example in the DWR information section, the **No Work Items Installed, No Contractors On Site,** and **No Daily Staff On Site** fields or boxes will automatically populate based upon information that is entered in the balance of the identified DWR sections.

In the Contractor's tab, once the Contractor has been selected and the number of hours worked and the number of persons worked is entered, related fields such as number of supervisors, number of workers and contractor hours worked will automatically populate. In the Daily Staff tab the only information required is the "Staff Member" and "Reg. Hours" worked. The S/C field is automatically populated, depending upon whether the staff member is a State employee (S), or a Consultant (C).

Recommendation 3

OCIA recommended the development of an automated feature to assure that incorrect data are identified, rejected, and not allowed to enter the system or to update the master file. In addition, OCIA recommended the implementation of a system to ensure that mistakes are tracked and those uncorrected are properly identified and corrections pursued. This would ensure erroneous data is detected.

Management Response

Management asserted that since the release of the SiteManager report in June 2010 the agency no longer uses PES/LAS. Projects are currently entered into P2S. Then they are put together in a contract by the Letting Prep office in AASHTO Project Preconstruction. The projects are placed into Bid Xpress by an information consultant and bid by contractors. The bids are analyzed by Director of Construction, Bid Analysis Engineer, and others. The projects are then moved to SiteManager and each step of the way, the data is moved as a package, maintaining the same information throughout the process. If data such as the contractor or specific dates are missing, the contract cannot be activated in SiteManager.

Management also stated that Daily Work Reports are approved by the Resident Construction Engineers in the form of Diaries. SiteManager will not include quantities on an estimate that have been authorized in a diary.

Status: Implemented

We identified the current data validation process and found that contract data is loaded into SiteManager using the Pre-construction Contract data load process (PRELOAD) user interface. When contract data is loaded into SiteManager from the Pre-construction system, SiteManager verifies that the required data is present and acceptable. If a Contract fails the validation process, SiteManager generates error messages and displays them on the Interface Load Message Window. After the Contract status changes to active, the data loaded from Pre-construction cannot be modified.

We also found that SiteManager has a built-in application feature to ensure records such as contractor payments or estimates do not include any quantity or pay items that have not been authorized by the Resident Construction Engineer (RCE). Daily Work Reports (DWRs) and Diaries are created to document the work that is done daily on the Contract. The data recorded in a DWR or Diary is the Contract activity data. The documentation of Contract activity includes daily information about the weather, the personnel who worked at the construction site, the hours worked, and the equipment used. This data is collected in the field by the Inspectors working on the Contract. The RCE uploads and authorizes the Daily Work Reports in the form of Diaries to the SiteManager Server database.

OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS (CONTINUED)

Status: Implemented (Continued)

We also noted that SiteManager has a number of fields which are automatically completed or populated based upon the completion of related records. For example, the DWR information tab contains three (3) autofill boxes "No Work Items Installed," "No Contractors On Site," and "No Daily Staff On Site". These fields are populated automatically based upon information that is entered in the balance of DWR tab records such as "Contractors Equipment," "Contractors," and "Daily Staff". The Pay Items' "Amount Filed" is automatically calculated as well from data entered in the "Quantity" and "Unit Price" fields.

We identified a data verification user interface that ensures requisite data is present prior to activation into SiteManager. SiteManager also has built-in application features which prevent the addition to records without proper authorization. A number of fields within SiteManager are pre-populated which prevents the processing of erroneous data.

OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS (CONTINUED)

Recommendation 4

OCIA recommended that the system owner/administrator ensure that all users know whom to contact if issues occur with SiteManager.

Management Response

Management stated that the SiteManager's user manual would be updated to provide users contact information for assistance with the application.

Status: Implemented

The Director of Construction (DOC) office has updated the SiteManager Version 3.7a Training and Reference Manual for field personnel to identify contact information for further assistance.

OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS (CONTINUED)

Recommendation 5

OCIA recommended that users be made aware of SCDOT and Information Technology Services' (ITS) ability to customize reports to their specification. Also, OCIA recommended that all users be made aware of the SiteManager Users' Group. The user group can serve as an avenue to recommend formatting edits that would make the reports more user friendly. Also, the user group would provide an avenue to discuss issues and as a resource for users.

Management Response

Management responded that the SiteManager Users' group will meet quarterly to discuss user related issues, reporting needs and system update information.

Status: Implemented

We were able to confirm a SiteManager User's Group meeting was held. The group determined that future communications would be made via phone or email. We also were able to identify reports related to the SiteManager User's Group meeting.

OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS (CONTINUED)

Recommendation 6

OCIA recommended that the RCE terminate contract authority after contract completion to ensure unauthorized users do not have access after the fact.

Management Response

Management asserted that SCDOT employees require contract authority after contract completion to ensure authorized users do not have access after the fact. Management stated that removing contract authority would prevent users from accessing records of past work performed by contractors. Management also asserted that safeguards are in place to prevent inspectors from altering data once approved by the RCE.

Status: Implemented

We were able to determine that The Resident Construction Engineer (RCE) provides Contract Authority to contract personnel. This authority allows project personnel to enter and process contract information in SiteManager during the life of the contract. In the original SiteManager's Audit Report we recommended termination of contract authority after the project completion. Management responded that the retention of contract authority was needed to access records of past work. Management also asserted that safeguards such as a Daily Work Reports (DWR's) were in place to prevent record alteration.

A Daily Work Report (DWR) acts as the primary means of documenting activity on a construction project. DWR's include information such as items of work performed, quantities installed, number of contractor and inspection personnel present, and equipment utilized. DWR's should also include any significant events, conversations, etc. that occur during the workday. The information entered on the DWR should be detailed, accurate, and thorough to ensure that those not associated with the project on a daily basis can fully understand the events as they occurred. A DWR should be generated each calendar day starting with the Notice to Proceed date and continuing until the project is complete. The DWR's enable inspectors to capture work performed at the job site on a laptop and upload it for review and approval.

Prior to approving the DWR, the RCE must review it. The RCE can also add any additional information concerning that particular day's activity on the project in the Remarks field of the Diary. After all remarks by the RCE have been entered the DWR is reviewed for approval and saved. Once a DWR has been saved it is locked and cannot be edited.

We were granted read-only access to SiteManager. We were able to view the Main Panel of SiteManager. However, when we attempted to open an approved DWR, the following message was received "Daily Work Report Will Be Opened As Read Only." We were unable to change, modify, edit or delete the approved DWR.

We were able to test and affirm a safeguard is in place which prevents the unauthorized modification of saved records in SiteManager.

Recommendation 7

OCIA recommended implementation of program editing so inspectors are limited to using what is already created in the system as eligible equipment to encourage uniformity.

Management Response

Management responded that as a result of SiteManager being jointly developed by a number of entities nationwide, SCDOT was unable to modify the source code. Management further asserted that SCDOT was working with the Transport Users Group (TUG) to have a number of the recommendations from the SiteManager audit to be incorporated into future versions of the generic application.

Status: Implemented

We were able to determine that the Daily Work Report (DWR) within SiteManager captures data for a job or part of a job on a daily basis. The DWR is associated with a specific contract or contractor. Prior to creating the DWR, the inspector is responsible for creating and maintaining the Contract Master List. The Contract Master List contains detailed information for the contractor's personnel, contractor's equipment, and SCDOT daily staff expected to work on the project. If the Contractor Master List database does not contain the appropriate personnel or equipment for a contractor, they can be added to the Contract Master List database by modifying the Vendor Master List. An example of this would be if a contractor just bought a new piece of equipment and will use it on a specific project. First, the new equipment would be added to the Vendor Master list, and then it would be added to the Contract Master List for a specific contractor. Once the new equipment has been added to the Contract Master List it is associated with the selected contractor.

We noted that different pieces of equipment must have unique ID numbers. However, the same type of equipment may have multiple ID numbers creating a one-to-many relationship. The current database structure within SiteManager discourages editing program uniformity. In response to a data request, management informed us that a new version of AASHTOWARE Project Construction (replacement for SiteManager) will have generic equipment, personnel, and staff that can be added without association to a specific contract or vendor. The implementation of the new structure should promote a one-to-one relationship which promotes editing uniformity.

We were able to identify measures management has undertaken to implement recommendations for editing program enhancements.

Recommendation 8

OCIA recommended enhancing password requirements that force users to change passwords every 30-90 days. OCIA recommended that passwords be unique and meet four of the six below minimum requirements:

- *Eight or more characters*
- *Use Pass-Phrases (e.g., "I love SCDOTOBD," "My1964.5mustang," "Auditorsarebest")*
- *Upper case alpha*
- *Lower case alpha*
- *Numeric*
- *Special*

Management Response

Management stated that passwords would be set to require a minimum of eight characters and will be set to expire once every 90 days. Management also asserted that the additional security enhancements will be proposed to the TUG to be incorporated into the application.

Status: Implemented

We determined that SiteManager resides on the network server which requires initial NTS credentials login which includes username and password. The passwords must adhere to the following construction:

- Passwords should be at least 8 characters
- Passwords should be comprised of a mix of letters and numbers
- Passwords should be comprised of upper and lower case characters
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information like names, birthdays, addresses, phone numbers, locations, etc. In accordance with the SCDOT network security policy to maintain good security at minimum users must change passwords every 90 days. The organization may use software that enforces this policy by expiring users' passwords after this time period.

Once the user has signed on to NTS, additional sign-on authentication credentials (i.e., user ID and Password) are required to access SiteManager.

We were able to identify system operational parameters for SiteManager's security settings and determine that the security settings were augmented with NTS security credentials.

Recommendation 9

OCIA recommended that the user be locked out after three unsuccessful log-in attempts and that this should not be interrupted by shutting the system down. We recommend displaying a warning message upon successful log-in.

Management Response

Management responded that as a result of SiteManager being jointly developed by a number of entities nationwide, SCDOT was unable to modify the source code. Management further asserted that SCDOT was working with the Transport Users Group (TUG) to have a number of the recommendations from the SiteManager audit to be incorporated into future versions of the generic application.

Status: Implemented

We conducted an access control test to determine if SiteManager enforces an automatic log-out of the user account after unsuccessful login attempts. We attempted to log in to SiteManager with the correct username and incorrect passwords. After 3 consecutive login failures SiteManager locked the user account to the system. The system administrator intervention was required to unlock the account.

It should also be noted that we were granted read-only access to SiteManager to review and to test the built-in controls within the application. Logon to SiteManager requires two-factor authentication of user ID and password. The user ID is the first 6 letters of the user's name followed by the first initials of the first name and middle name.

The first time logon attempt to SiteManager will be "PASSWORD." We noted that SiteManager does require the user to change the default password setting after the initial logon. We noted that the new password must be 4 to 8 characters or digits. The password is also case sensitive.

OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS (CONTINUED)

Recommendation 10

OCIA recommended reviewing the user list to purge terminated employees access to SiteManager on a routine basis. OCIA recommended purging the system for terminated employees and unused "on call" engineers and inspectors. Also recommended was changing the "on-call" engineers and inspectors that may be used in the future to the SUSPEND (de-activated users) access level so the access level may be changed as needed on projects without re-entering them into the system. OCIA recommended the system automatically log off after the terminal remains inactive for 15 minutes and also recommended that a log be created to track admin account usage and security violations and be reviewed on a regular basis. Finally, OCIA recommended that a procedure be developed to deactivate inactive users on a regular basis.

Management Response

Management stated that the SiteManager support team would work closely with IT Services to ensure that users are deactivated upon termination and that accounts de-activated in SCDOT network are also de-activated in SiteManager as well. Management also affirmed that as a security measure, global group policies had been established for all SCDOT's personal computer workstations to be locked after 15 minutes of inactivity. Management further stated its encouragement to users to lock their workstations when left unattended.

Status: Implemented

We spoke with a supervisor in IT Services responsible for MS-Outlook email connectivity regarding deactivated user accounts. The supervisor asserted that a process is in place to notify Human Resources and IT Services when employees are terminated. The supervisor asserted that the process is form-generated. When a SCDOT employee is separated, the supervisor submits Form HR1 to Human Resources. A global distribution email is generated from Human Resources to recipients on the notification termination list, "D8Term". When IT Services receives the "D8Term" email which notifies the recipients that the employee is no longer employed with SCDOT the employee's account can be disabled. Another IT Services supervisor is responsible for deleting network server access for terminated employees. The system administrators for the various agency applications such as SiteManager are responsible for deleting or deactivating the user account access of terminated employees.

In addition, we conducted a test and found that the system administration for SiteManager was included on the "D8Term" list.

We further found that idle connections to network access are timed out after 15 minutes of inactivity. The timeout is consistent with the Secretary of SCDOT statement dated July 25, 2016 and addresses the risk of remote access. We also conducted a timeout test and were locked out of the network after 15 minutes of inactivity.

We found procedures do exist for the deactivation of user accounts of terminated employees.

We did not find a policy which mandates the locking of workstations after 15 minutes of inactivity. However, a statement from the SCDOT Secretary does notify users of 15 minutes of inactivity which results in an automatic restart.

OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS (CONTINUED)

Recommendation 11

OCIA recommend that the application owner have discussions with AASHTO to determine what program changes are possible as an effort to better assist users.

Management Response

Management stated that the SiteManager support team will continue to work closely with InfoTech and the TUG regarding SiteManager development.

Status: Implemented

The administrative owner for SiteManager is the user group representative for SCDOT with other participating states throughout the nation. As a user group representative the administrative owner participates in an annual balloting process to determine fixes and enhancements to propose to Infotech, Inc., the developer of SiteManager. According to administrative owner, usually during the month of October votes are cast for the enhancements. Some of the enhancements may be deemed obsolete given conflicting interest among the various state users of the product.

We were able to identify Management's involvement with the developer of SiteManager to recommend enhancements.

OCIA PRIOR RECOMMENDATIONS, MANAGEMENT'S RESPONSES, AND CURRENT STATUS (CONTINUED)

Recommendation 12

Even though SCDOT showed evidence of a disaster recovery plan, OCIA recommended written documentation of a disaster recovery plan.

Management Response

Management asserted that a disaster recovery plan was in place and written documentation would be available upon completion of a full VMware suite.

Status: Implemented

VMware is an operating system that allows one to run multiple virtual machines on a single physical machine, with each virtual machine sharing the resources of that one physical computer across multiple environments. Different virtual machines can run different operating systems and multiple applications on the same physical computer. VMware also sits directly on the hardware and is the interface between the hardware and the various operating systems. It expands the hardware from the users' point of view to many different independent servers all with their own processors and memory. These virtual servers cannot be distinguished from physical servers by the end users.

Internal Audit spoke with the SCDOT IT Services Director who asserted that SCDOT currently utilizes VMware to enable external users to gain access through a virtual client to applications which are saved to the network servers. The VMware acts as a security control which does not allow the external users direct access to the network server. External users such as contractors must logon to the VMware suite to access SiteManager for project information to invoice SCDOT.

We also inquired about the existence of a disaster recovery plan (DRP) for VMware which addresses documented processes or a set of procedures to recover and protect the IT infrastructure in the event of a disaster. The IT Services Director informed us that SCDOT IT Services does have a written DRP for VMware. The Director provided an electronic copy of the DRP which enumerates the primary steps: storage synchronization; restoration of recovery site from standby; suspension of non-critical VMwares at the recovery site; creation of variable storage snapshot; and power on priority of 1, 2, 3, 4, and 5 VMwares.

Management was able to provide us with a documented DRP which enumerates specific steps SCDOT's IT Services would undertake in the event of a disaster.

10 copies of this document were published at an estimated printing cost of $1.55 each, and a total printing cost of $15.53. Section 1-11-425 of the South Carolina Code of Laws, as amended requires this information on printing costs be added to the document.