



Office of the Chief Internal Auditor

Audit Report

*South Carolina Department of Transportation
SiteManager Construction Management System
(A10-004)*

June 24, 2010

Table of Contents

**Office of the Chief Internal Auditor
Audit of SiteManager Construction Management System**

June 24, 2010

TABLE OF CONTENTS

	<u>Page</u>
Transmittal Letter	i
Executive Summary	iii
Audit Findings and Recommendations	1
Department Response	11

Transmittal Letter



OFFICE OF THE CHIEF INTERNAL AUDITOR

October 14, 2010

Commission of the South Carolina Department of Transportation

The Honorable Lawrence K. Grooms, Chairman
South Carolina Senate Transportation Committee

The Honorable Hugh K. Leatherman, Sr., Chairman
South Carolina Senate Finance Committee

The Honorable Phillip D. Owens, Chairman
South Carolina House Education and Public Works Committee

The Honorable Daniel T. Cooper, Chairman
South Carolina House Ways and Means Committee

Dear Gentlemen:

The Office of the Chief Internal Auditor has completed an operational audit of the SCDOT SiteManager Construction Management System as of June 24, 2010. In accordance with Section 57-1-360, we are transmitting to you this report of our audit findings.

We conducted this operational audit in accordance with Generally Accepted Governmental Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for these findings and conclusions.

Please don't hesitate to contact us if you have any questions or comments.

Respectfully submitted,

Robert W. Wilkes, Jr., CPA
Chief Internal Auditor

Executive Summary

EXECUTIVE SUMMARY

The SiteManager Construction Management System is a computer application used to manage construction contracts and as a repository of critical contract records. SCDOT Inspectors are responsible for processing Daily Work Reports (DWR). The Resident Construction Engineer (RCE) is responsible for processing and approving the Daily Work Reports and Monthly Pay Estimates as well as the following:

- Assigning inspectors
- Adding substantial work complete date
- Completing the Project Closeout Packet

SiteManager keeps a record of detailed information on work performed. The Inspector enters the item of work, quantity, and location of the installed item. Change orders are created, as needed, to compensate the contractor for work performed that is outside the scope of the initial contract. These changes result from items not on the initial estimate of project quantities, overruns in quantities, deletion of quantities from the contract, adjustments in contract unit price, specification changes, and/or adjustments in contract time.

Upon entry of the substantial work complete (SWKC) date and preparation of the built plans, the RCE prepares the Project Closeout Packet. This process finalizes the funds required for each project and releases any unused resources for future projects.

The Director of Construction (DOC) suggests 270 days for completion of a project from SWKC to the completion of the project closeout process and the DOC final signature. This process relies on multiple offices and departments to work collectively in order to coordinate activities.

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. We conducted this audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Our objectives were as follows:

- 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

We interviewed employees, selected samples, and documented the process and its controls. We have developed twelve recommendations related to efficiencies and controls in managing construction projects and the adequacy of internal controls to protect access and integrity of information. These recommendations are summarized below:

- Implementation of precautions to enforce referential integrity and development of a flowchart to display business processes
- Creation of pre-populated fields and prompting to assist with data entry
- Development of an automated feature to ensure that incorrect data are identified, rejected, and not allowed to enter the system. Development of a system to track errors and ensure those uncorrected errors are properly identified and corrections pursued
- Inform all users of whom to contact if issues occur with SiteManager
- Inform users of SCDOT and ITS' (Information Technology Services) ability to customize reports to their specification and increase awareness that the SiteManager Users' Group exists
- Termination of contract authority after contract completion
- Implementation of program editing to ensure inspectors are only able to use what is already created in the system as eligible equipment
- Enhancement of password requirements
- Implementation of an account lock after three unsuccessful log-in attempts and display a warning message for unauthorized personnel upon successful log-in
- Development of procedures to deactivate inactive users and purge terminated employees on a regular basis. Change the "on call" engineers and inspectors that may be used in the future to the SUSPEND (de-activated users) access level. Require the system to automatically log off after the terminal remains inactive for 15 minutes. Creation of a log to track administrative account usage and security violations
- Encourage application owner to discuss program changes to better assist users
- Creation of a written disaster recovery plan

The findings and recommendations will be discussed in greater detail in the Audit Findings and Recommendations section of the report.

Audit Findings and Recommendations

AUDIT FINDINGS AND RECOMMENDATIONS

The SiteManager Construction Management System is an American Association of State Highway and Transportation Officials (AASHTO) product that provides a platform for data entry, tracking, and reporting of contract data from contract award through finalization. SiteManager interfaces with other departmental applications. Proposal and Estimate System (PES) downloads to SiteManager but other systems use SiteManager data (e.g., Primavera - construction project scheduling, CITRIX Portal reporting, card file system, Integrated Transportation Management System (ITMS), Construction Management System (CMS), and Contract Bid Estimate System (CBES). When a contract is awarded, the award letter and contract copies are mailed. The contract information is downloaded to SiteManager from the Proposal and Estimates System (PES). The contractor signs the contract with proof of insurance along with the bonding signature to obligate completion of contract. The Director of Engineering executes the contract. The Program Manager II forwards an email to the Engineer/Associate Engineer II with a file number for activation. The Engineer/Associate Engineer II reviews the contract for accuracy and enters charge code, contract ID, select major items (line item(s) over 10% of the total contract), and activates the contract.

After activation of the contract, the Resident Construction Engineer (RCE) assigns inspectors to the project. The Lab Quality Assurance department generates a sample requirements list based on the pay items notifying the inspector of how many samples he/she has to acquire. The lab enters pass/fail for each sample in SiteManager. The RCE or designee enters certifications (materials must meet a certain standard). A pre-construction meeting is held with the RCE, contractor, inspectors and utilities representatives to discuss pole removal, starting point, etc. The RCE forwards the notice to proceed date (starting point for diary) via intranet to an Administrative Specialist II. The inspector and foreman compare quantity notes (foreman gives verbal approval). If necessary, a change order is created for estimates beyond contract negotiations (e.g., adjustments in contract unit price, adjustments in contract time).

For contract payments, the RCE forwards an estimate (hard copy) to the contractor for review. A Contractor Concurrence Form is signed after providing justification and explanation of payment. The RCE approves estimates (daily work reports) daily. The Assistant District Construction Engineer (ADCE) approves the estimate via SiteManager. The RCE forwards a hard copy of the estimate to the accounting department for payment. Accounting pays the contractor according to the estimate and keeps a ledger system to track the funding of the project.

In preparation for completion of the project, there is an inspection with the contractor, construction office, RCE, District Construction Engineer (DCE), Director of Construction (DOC), Federal Highway and Administration (FHWA) representative (if federal funds are involved), and lead inspector. As part of this inspection, the group will perform a walk through and prepare a “punch list” (items that require correction, repair, or replacement). The “punch list” must be completed within thirty days after the substantial work complete (SWKC). The RCE enters the substantial work complete date into SiteManager.

Once the project is completed, the RCE prepares “as-built plans” and submits them to the As-Built Plans Office at Headquarters with a copy to the Resident Maintenance Engineer. The RCE prepares a project closeout packet of information (final estimate, contractor concurrence form of

final quantities, etc.) and forwards the packet to Contract Administration. The RCE completes key dates in SiteManager. Contract Administration verifies a complete project closeout packet.

The SiteManager Construction Management System audit was subdivided in the following areas to determine effectiveness and efficiency: input controls, processing controls, data output controls, access controls, program change controls, and disaster recovery. The findings and recommendations for each area are referenced in detail below.

Input Controls

Finding 1

We reviewed the *SiteManager Version 3.7a Training and Reference Manual for Field Personnel* and *SCDOT Construction Manual* (Section 101.6, SiteManager Considerations). Both provided detailed and useful instructions for entering information into the SiteManager system. The reference manual provided pictorial assistance for better understanding. SiteManager policies/procedures provide step-by-step instructions of all parts of the application. We determined department personnel continuously verify data inputs during various stages of the process; however, there are not any written policies and procedures established to ensure that incorrect data are identified, rejected, and not allowed to enter the system or update the master file. For example, once the contract information is uploaded to SiteManager from PES, the only established procedure is that the Engineer/Associate Engineer II verifies the information for accuracy.

Recommendation 1

We recommend 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. We recommend 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.

Finding 2

We reviewed the item quantity report (summary of all items reported from DWR), the estimate item detail report (from the quantity report for vendor payment), and the change order report (changes to the contract with justification) and found that they provided an adequate audit trail. Also, the reports provide a means for the vendor to review or keep track of previous work and paid items. Program editing is used in some areas of SiteManager. For example, the "Work Begin Date" cannot be a date in the future. The computer will generate an error message if entered incorrectly. Prompting, which is used to aid data entry by providing examples of values for input, is built into very few data input routines.

Recommendation 2

We recommend having as many pre-populated fields (e.g., Contractor Name, Location) as allowed by the software to prevent data entry errors. We recommend adding prompting to the Daily Work Reports' Contractors, Contractors Equip, 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.

Finding 3

Once the Program Manager retrieves contract information from PES and downloads to SiteManager, the Program Coordinator enters the execution date and other information for the contract. The Program Coordinator forwards an email to the Engineer/Associate Engineer II with file number for activation. The Engineer/Associate Engineer II reviews for dates, card file, and contract for accuracy. The only established procedure used to assure that incorrect data are identified is the review from the RCE, ADCE, and/or District Engineering Administrator (DEA). There is not an automated feature to ensure that incorrect data are rejected and not allowed to enter the system or to update the master file. SiteManager does not detect erroneous data. We discovered that there is not a system in place for tracking uncorrected mistakes. Tracking uncorrected mistakes would ensure correct billing and identify other issues that may interrupt the progress of the project.

Recommendation 3

We recommend 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. Also, we recommend that a system is put in place to ensure that mistakes are tracked and those uncorrected are properly identified and corrections pursued. This would ensure erroneous data is detected.

Processing Controls

Finding 4

We surveyed the SiteManager User Group (approximately 61 users) to ask if they knew whom to contact to have problems resolved quickly. Of the 37 users that responded, 15 (41%) replied "no" and 22 (59%) replied "yes".

Recommendation 4

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

Data Output Controls

Finding 5

The SiteManager Users' Group is comprised of SiteManager users from the eight counties (Abbeville, Edgefield, Greenwood, Laurens, McCormick, Newberry, and Saluda) in District Two. We emailed the SiteManager Users' Group (approximately 61 users) to ask the following questions concerning the reports generated. 12 of 61 (19.7%) responded.

- Item Quantity Report Relevant? All answered yes.
- Estimate Item Detail Report Relevant? 8 of 12 (66.6%) answered yes. Three do not use. One used the optional form of the detailed report called Citrix.
- Item Work Report Relevant? 11 of 12 (92%) answered yes. One does not use it. One of the yes responses indicated that the report needs the road number with each line item. Cross referencing the data wasted time.
- Installed Work Report Relevant? 11 of 12 (92%) answered yes. One does not use it.
- Change Order Relevant? 10 of 12 (83.3%) answered yes. Two did not use.
- Reports accurate, reasonable, reliable, useful? All agreed that the reports are accurate, reasonable, reliable, and useful. The users suggested the following:
 - Item Quantity Report show the units of measure
 - Item Work Report display the location of work item in addition to the station number
 - Make the reports easier to find in SiteManager
 - Item Quantity Report is difficult to read

SCDOT can customize reports due to some of the reports being written in Report Template Facility (RTF) format. RTF enables the user to edit various sections of the RTF Report facility in Enterprise Architect. This functionality is used to customize a report's look and feel for the user. Also, we determined that ITS has the ability to edit reports currently available via Citrix (desktop application software on the server) within the SiteManager Report application. ITS will duplicate a report found within SiteManager application in the Oracle Reports environment then customize that report as requested.

Recommendation 5

We recommend that users be made aware of SCDOT and ITS' ability to customize reports to their specification. Also, we recommend 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.

Finding 6

In reviewing how the RCE determined who should have contract authority and ensuring that contract authority is terminated in a timely manner, we determined that the RCE, DEA, and ADCE determined who should have contract authority. The RCE granted contract authority to the inspector who will handle the project and others who may be required to enter data. The RCE terminated contract authority, but not on a consistent basis.

Recommendation 6

We recommend the RCE terminate contract authority after contract completion to ensure unauthorized users do not have access after the fact.

Finding 7

We reviewed who authorizes, creates, and enters the unique equipment ID numbers. We determined that having unique equipment ID numbers is not as important as the quantity of equipment and naming convention. Inspectors may input equipment into the application without being descriptive which increase inconsistency.

Recommendation 7

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

Access Control

Finding 8

We found that all users are required to enter a password that is four to eight characters or digits in length. The passwords are required to be changed once a year. We determined that passwords are case sensitive in SiteManager but are not required to have specific criteria. We determined that passwords were not accessible or viewable to others, including administrators.

Recommendation 8

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

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

Finding 9

We determined that user IDs lock after three unsuccessful log-in attempts, but if the user shuts down SiteManager after two failed log-in attempts he/she will receive three additional attempts to access the system. We determined if a log-in (of three consecutive) attempt is unsuccessful, a generic message will display. When reviewing SiteManager for a generic message after a successful log-in attempt, we found that a warning message was not present. The last log-in date and time does not display on successful log-in.

Recommendation 9

We recommend 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.

Finding 10

We obtained and reviewed the list of all SiteManager users to include access levels. We created a spreadsheet displaying access levels with applicable tabs/screens. We determined that the following individuals/groups have access to SiteManager:

- Assistant construction engineer
- Assistant district construction engineer
- Assistant RCE
- Asst RCE (standalone mode)
- District construction engineer group
- District clerk
- District engineer administrator group
- Director of construction
- Director of maintenance
- Resident admin personnel
- Inspector - standalone
- Inspector
- District IRC group
- IT
- Material technician group
- Resident construction engineers group
- Resident construc engr standalone group
- SiteManager inquiry group
- Materials inquiry group
- SiteManager administrator
- FHWA group
- Contracts
- Contract admin approval
- Bridge construction
- Contract administration group
- DBE and special programs
- DBE office key date entry
- State construction engineer
- De-activated users
- Traffic engineering group

We sampled 203 of the 2037 users to determine if the user was a construction employee, a current employee, and/or unknown. Of the 203 sampled, 88 (43%) were not construction employees and 30 (15%) were terminated employees. Of the 88 users that were not construction employees, 39 (44%) were identified as SCDOT employees working in the engineering,

construction, maintenance, or accounting departments. 49 (56%) individuals were unidentified but have resident construction engineers group, inspector - standalone, and SiteManager administrator access levels. SiteManager can remain inactive for at least four hours and the user is not automatically logged off.

47 of 2037 (2%) users have administrator rights. In assessing the security over the admin generic account password, we determined that SiteManager utilizes SiteManager Administrator access level rather than an established admin generic account password. Also, we determined that there is not an Administrator access level usage and security violations log.

We reviewed general access to SiteManager and determined the application requires a user ID and password. We determined that the user ID is unique. We determined that there is no procedure in place to ensure that inactive user IDs are reviewed and deactivated on a regular basis.

Recommendation 10

We recommend reviewing the user list to purge terminated employees access to SiteManager. This should be performed on a routine basis. We recommend purging the system for terminated employees and unused "on call" engineers and inspectors. We recommend 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. We recommend the system automatically log off after the terminal remains inactive for 15 minutes. We recommend that a log be created to track admin account usage and security violations and be reviewed on a regular basis. We recommend that a procedure be developed to deactivate inactive users on a regular basis.

Program Change Control

Finding 11

We reviewed and verified that there are separate libraries for SiteManager. The database files are located in SMDT for production programs and SMDBT for test programs. The databases have logical tablespaces and within the tablespaces are datafiles where all of the data is stored.

We reviewed and verified that the test, staging, and production programs are maintained in separate libraries. The test database is located on server SMPORA05, the staging area is located on server SMPDPS2, and the production database is located on server SMPORA02.

The Engineer/Associate Engineer II, the Information Resource Consultant II, the Program Manager II, and the Senior Geodetic Technician have the ability to access the application in testing as well as access to the staging areas and production libraries.

In identifying audit trails of change activity for completeness, we determined changes to the program are administered by American Association of State Highway and Transportation Officials (AASHTO) via releases. SCDOT has not made changes to the application in the past three (3) years.

Recommendation 11

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

Disaster Recovery

Finding 12

SCDOT infrastructure disaster recovery is divided into two parts: Information Technology (IT) and Mainframe. For the purpose of this audit, we only reviewed the IT Infrastructure because SiteManager does not upload data to any mainframe applications. We reviewed documents for a disaster recovery plan to identify procedures for moving back from the recovery center once the disaster is over.

SCDOT began by researching options for a secondary data center for disaster recovery five years ago. SCDOT met with consultants and *SunGard* disaster recovery services. Initial cost was estimated to exceed \$1,000,000 with an ongoing monthly cost to exceed \$10,000 for facilities rental. During that time, ITS staff was in the process of deploying VMware to virtualize the server infrastructure. This resulted in the consolidation of over 100 physical servers to 19 VMware physical servers. VMware's three-year analysis for SCDOT calculated the estimated total cost of ownership comparison between the 2005 environment (with over 100 servers) and implementing the proposed VMware solution. The new solution resulted in cost savings in hardware of \$737,076.

In Spring 2008, ITS used the savings to deploy the secondary data center (Hot Site) themselves at a cost of \$636,327. This includes the storage and software license for MirrorView (provides highly available data storage across campus, across the state, or across the globe). This was purchased with funds from the regular operating budget. No additional funds were requested.

The secondary data center has been established. The first phase of disaster recovery has been deployed with the replication of SCDOT data from HQ to the secondary site. The next phase is to replicate the server infrastructure that exists at HQ to the secondary data center. This will be accomplished with the deployment of VMware's Site Recovery Manager Software. VMware Site Recovery Manager eliminates the slow manual steps of recovery, turning the complex paper run books associated with traditional disaster recovery into an integrated part of a virtual infrastructure management. By automating recovery, VMware Site Recovery Manager eliminates error-prone manual steps in the recovery process and ensures that recovery procedures will be consistently executed as intended. This allows for non-disruptive tests of recovery plans within an isolated testing environment so that we can ensure that the disaster recovery plan will execute successfully. The installation completion date is estimated for December 2011.

A disaster has many definitions (i.e., malicious program, fire, flood, earthquake, lightning, hurricane, etc.) to ITS. It is not isolated to a total destruction of HQ. For example, there was a hardware failure of one of the VMware host servers that was running SCDOT Exchange Email. The dynamic unattended failover of the Exchange server to another VMware host took place with only five minutes of downtime that very few people even noticed. Prior to the deployment

of VMware, this hardware failure would have resulted in many hours, if not days, of restoration. SCDOT has redundancy (a fault-tolerant technique where a secondary hardware and software takes over when the primary system fails, so control can continue uninterrupted) and failover (capability to switch over automatically to a redundant or standby computer server, system, or network upon the failure) within HQ. The deployment of Site Recovery Manager will extend this to the secondary data center. Until December 2011 in the event of a HQ disaster, SCDOT would need to procure servers, manually deploy them and perform some measure of restoration to establish connectivity to applications and data. This connectivity would take approximately one week.

In reviewing access to key data, tables, log, and program files, we determined that only ITS System staff had access.

The SiteManager Database on the Oracle server is backed up daily. ITS performs a full complete backup of the database as well as a compressed export database dump as indicated below:

- **Critical Files.** Backups are verified as part of the backup software procedure.
- **Accurate Inventory.** Daily backups retained two weeks on site. Weekly backups retained for one month at primary and 13 days at the Hot Site. Quarterly backup retained for one month on site and 15 months at Hot Site.
- **Tested Periodically.** ITS ensure backups are tested daily.
- **Sent Off Site.** ITS backups are multi-streamed writing onsite and offsite at the same time. The offsite facility was identified and verified but for security reasons the location will not be identified in this audit.

Recommendation 12

Even though SCDOT shows evidence of a disaster recovery plan, we recommend written documentation of a disaster recovery plan.

Department Response



MEMORANDUM

TO: Office of Chief Internal Auditor

FROM: Charles R. Eleazer *Ch. Eleazer*
Interim Director of Construction

DATE: September 28, 2010

SUBJECT: SiteManager Audit

I have reviewed the audit and would like to make the following comments regarding the SiteManager application.

- The development of SiteManager originally was a joint effort of 18 states and a Canadian province in conjunction with the American Association for State Highway Transportation Officials (AASHTO). A great deal of effort has been put into this application to ensure its security and data integrity over its twelve year lifespan.
- Since SiteManager is an AASHTOWare product, changes to the application are a lengthy and expensive process.

The following is a response to each of the twelve recommendations included in the report:

Audit Recommendation 1

We recommend 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. We recommend 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.

Response:

We agree 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. Currently, SiteManager enforces referential integrity throughout the application,

maintaining parent / child relationships and preventing those primary keys from being deleted or changed. We do see the need to clean up the master lists for Contractor Equipment and Personnel. This will help reduce duplications in those areas.

Audit Recommendation 2

We recommend having as many pre-populated fields (e.g., Contractor Name, Location) as allowed by the software to prevent data entry errors. We recommend adding prompting to the Daily Work Reports' Contractors, Contractors Equip, 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.

Response:

As a result of SiteManager being jointly developed by a number of entities nationwide, SCDOT is unable to modify the source code. SCDOT is currently working with the Transport Users Group (TUG) to have a number of recommendations from this audit incorporated into future versions of the generic application.

Audit Recommendation 3

We recommend 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. Also, we recommend that a system is put in place to ensure that mistakes are tracked and those uncorrected are properly identified and corrections pursued. This would ensure erroneous data is detected.

Response:

SCDOT has a number of individuals checking for errors in the Proposal and Estimates System (PES) and the Letting and Award System (LAS) prior to its load into SiteManager. SiteManager then checks the validity of this information to make sure all data is loaded correctly into the system. Finally, data is validated during the activation process. Unfortunately, there is no way to create a system that would automatically check for errors in reporting quantities in SiteManager. We will however, continue to require Resident Construction Engineers and other SCDOT personnel to review and approve quantities installed on jobsites.

Audit Recommendation 4

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

Response:

The SiteManager user manual will be updated to provide users contact information for assistance with the application.

Audit Recommendation 5

We recommend that users be made aware of SCDOT and ITS' ability to customize reports to their specification. Also, we recommend 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.

Response:

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

Audit Recommendation 6

We recommend the RCE terminate contract authority after contract completion to ensure unauthorized users do not have access after the fact.

Response:

SCDOT employees require contract authority after contract completion to refer back to specific details in the contract. Removing contract authority would prevent users from accessing records of past work performed by contractors. Safeguards are in place to prevent inspectors from altering data once approved by the Resident Construction Engineer.

Audit Recommendation 7

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

Response:

As a result of SiteManager being jointly developed by a number of entities nationwide, SCDOT is unable to modify the source code. SCDOT is currently working with the Transport Users Group to have a number of recommendations from this audit incorporated into future versions of the generic application.

Audit Recommendation 8

We recommend enhancing password requirements that force users to change passwords every 30-90 days. We recommend 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*

Response:

Passwords will be set to require a minimum of eight characters and will be set to expire once every 90 days. The additional recommended enhancements to security will be proposed to the TUG to be incorporated into the application.

Audit Recommendation 9

We recommend 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.

Response:

As a result of SiteManager being jointly developed by a number of entities nationwide, SCDOT is unable to modify the source code. SCDOT is currently working with the Transport Users Group to have a number of recommendations from this audit incorporated into future versions of the generic application.

Audit Recommendation 10

We recommend reviewing the user list to purge terminated employees access to SiteManager. This should be performed on a routine basis. We recommend purging the system for terminated employees and unused "on call" engineers and inspectors. We recommend 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. We recommend the system automatically log off after the terminal remains inactive for 15 minutes. We recommend that a log be created to track admin account usage and security violations and be reviewed on a regular basis. We recommend that a procedure be developed to deactivate inactive users on a regular basis.

Response:

The SiteManager support team will work closely with IT services to ensure that users are deactivated upon termination and that accounts de-activated in the SCDOT network are also de-activated in SiteManager. As a security measure, global group policies have been established for all SCDOT PCs in which a workstation is locked after 15 minutes of

inactivity. We will also continue to encourage users to lock their workstations when left unattended.

Audit Recommendation 11

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

Response:

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

Audit Recommendation 12

Even though SCDOT shows evidence of a disaster recovery plan, we recommend written documentation of a disaster recovery plan.

Response:

Currently, a disaster recovery plan is in place and written documentation will be available upon completion of the full VMWare suite.

In conclusion, we would like to thank the Office of Chief Internal Auditor, especially Charvae Martin for this audit. Although many of the suggested changes are difficult in nature, this level of insight from someone “looking in from the outside” is extremely beneficial to the SCDOT. We look forward to making whatever changes we can to make comply with these recommendations.

CRE: mjs

cc: John V. Walsh, Deputy Secretary for Engineering

J. C. Watson, Chief Engineer for Operations

B. Parnell, Engineering Contracts Manager

File: Con