

OCIA Audit Finding & Recommendations for Updated Responses

SiteManager Construction Management System

6/24/2010

Finding:

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:

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.

June 2010 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.

April 2015 Updated Response:

Policies and Procedures currently reflect workflow and correct usage throughout SiteManager. System administrators are unable to change the application due to its being an AASHTOWARE application, however, AASHTO Project 3.1 will be released in 2015 and will replace our current SiteManager application. The system for maintaining the master lists is expected to be improved.

Finding:

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:

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.

June 2010 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.

March 2015 Updated Response:

SCDOT will be implementing AASHTO Project 3.1 which will re-work how this data is entered.

Finding:

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:

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.

June 2010 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.

April 2015 Updated Response:

SCDOT will be implementing AASHTO Project 3.1 which will re-work how this data is entered.

Finding:

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:

Recommendation 4: We recommend that the system owner/administrator ensure that all users know whom to contact if issues occur with SiteManager.

June 2010 Response:

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

April 2015 Updated Response:

The Director of Construction office has met with district personnel to ensure the user community is aware of who to contact with any SiteManager related questions.

Finding:

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:

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.

June 2010 Response:

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

April 2015 Updated Response:

The Director of Construction Office is working closely with District Construction Engineers regarding report requirements outside of the SiteManager application. Resident Construction Engineers and county office personnel directly contact user support with any issues regarding report generation and support.

Finding:

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:

Recommendation 6: We recommend the RCE terminate contract authority after contract completion to ensure unauthorized users do not have access after the fact.

June 2010 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.

April 2015 Updated Response:

Termination of Contract Authority is subject to the discretion of the Resident Construction Engineer. During the closeout process, Inspectors are often required to go back and look at contracts to verify and answer questions regarding topics such as weather conditions and contract status during specific phases of construction. Without authority to view historical data, inspectors do not have access to this information.

Finding:

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:

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.

June 2010 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.

April 2015 Updated Response:

SCDOT will be implementing AASHTO Project 3.1 which will re-work how this data is entered.

Finding:

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:

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

June 2010 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.

April 2015 Updated Response:

SCDOT will be implementing AASHTO Project 3.1 which will use Windows authentication to adopt agency policies regarding password security.

Finding:

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:

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.

June 2010 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 Trns- port Users Group to have a number of recommendations from this audit incorporated into future versions of the generic application.

April 2015 Updated Response:

SCDOT will be implementing AASHTO Project 3.1 which will use Windows authentication to adopt agency policies regarding password security.

Finding:

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 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:

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.

June 2010 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.

April 2015 Updated Response:

Currently, terminated SCDOT employees are deactivated semi-monthly. All users are deactivated after 90 days of inactivity in SiteManager. All consultant users are deleted from the network after 30 days of inactivity. Administrator accounts occur on a continuum, with a number of user groups allowed access to different windows, with varying levels of access.

Finding:

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:

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.

June 2010 Response:

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

April 2015 Updated Response:

SCDOT is working closely with AASHTO and InfoTech with system updates and enhancements.

Finding:

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. 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:

Recommendation 12: Even though SCDOT shows evidence of a disaster recovery plan, we recommend written documentation of a disaster recovery plan.

June 2010 Response:

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

April 2015 Updated Response:

IT has a written disaster recovery plan.