FDOT

Florida Department of Transportation

RICK SCOTT
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

ANANTH PRASAD, P.E.
SECRETARY

July 21, 2014

Ananth Prasad, P.E.
Secretary
Department of Transportation
605 Suwannee Street
Tallahassee, Florida 32399-0450

RE: **Auditor General Report No. 2014-088**
Department of Transportation
Electronic Estimate Disbursement (EED) System

Dear Secretary Prasad:

As required by Section 20.055(5)(h), Florida Statutes, attached is the six month status of corrective actions taken as reported to us by the responsible action officials for the subject audit. This update details the implementation or current status of each audit recommendation. If you have any questions, please call me at 410-5823.

Sincerely,

Robert E. Clift,
Inspector General

RC: cm

Enclosure

cc: Kathy Dubose, Staff Director, Joint Legislative Auditing Committee
Melinda Miguel, Chief Inspector General, Executive Office of the Governor

FLORIDA DEPARTMENT OF TRANSPORTATION
6-month Follow-up to the
Office of the Auditor General
Information Technology Operational Audit-Department of Transportation
Electronic Estimate Disbursement System (EEDS)
Report #: 2014-088

Finding No. 1: Application and User Controls: Transaction dates, as defined in State law and the DFS FLAIR Procedures Manual, were not consistently recorded for payment request transactions processed in the EED System.

The DFS FLAIR Procedures Manual defines the transaction date as the latter of the date the invoice (payment request) is received or the goods and services were received, inspected, and approved for payment. Section 215.422(1), Florida Statutes, requires that invoices (payment requests) submitted to an agency of the State shall be recorded in the financial systems of the State, approved for payment by the agency, and filed with the Chief Financial Officer not later than 20 days after receipt of the invoice and receipt, inspection, and approval of the goods or services (transaction date). Section 215.422(3) (a), Florida Statutes, provides that each agency shall keep a record of the date of receipt of the invoice (payment request); dates of receipt, inspection, and approval of the goods or services; date of filing of the approved invoice; and date of issuance of the warrant in payment thereof. Additionally, Section 215.422(6), Florida Statutes, states that each agency shall be responsible for the accuracy of information entered into the DFS financial systems for use in monitoring agency compliance with time limits and interest penalty provisions of State law.

Our audit disclosed that the transaction dates related to payment request transactions from SiteManager that were processed by the EED System were not consistently recorded with the dates as defined in State law and the DFS FLAIR Procedures Manual. Therefore, the EED System was submitting inaccurate payment request data to the DFS financial systems. This applied to both EED auto-pay transactions and EED auto-manual transactions. We noted the following control deficiencies for both EED System auto-pay transactions and EED System auto-manual transactions:

- Auto-Pay - For SiteManager payment request transactions that were released and processed by the EED System auto-pay method, the dates that District Office staff released the transactions in the EED System were incorrectly recorded in the EED System as the transaction dates which, in turn, were automatically submitted to FLAIR for payment processing.

- Auto-Manual - For SiteManager payment request transactions that were processed by the EED System auto-manual method, the dates that Disbursement Operations Office staff approved (promoted) the transactions for payment were recorded in the EED System as the transaction dates, contrary to Section 215.422(3) (a), Florida Statutes. Once promoted, transactions are automatically submitted to FLAIR for payment processing.

To corroborate our understanding of the inconsistent recording of transaction dates, we examined 20 SiteManager payment request transactions that were loaded and processed by the EED System during the period January 1, 2012, through October 31, 2012, and found that 18 transactions had incorrect transaction dates recorded in the EED System.

We did not examine CITS payment request transactions because we had no assurance that the transaction dates recorded in CITS and loaded into the EED System were valid. CITS invoice documents did not have an invoice date field and the dates identified as invoice dates in the CITS database were inconsistent with the dates on related documentation. Additionally, the dates on the invoice transmittal forms could be manually modified. Given these circumstances, we were unable to determine a viable method to discern the correct transaction dates in CITS.

We further noted through additional audit procedures that inaccurate transaction dates that were allowed to be loaded or posted in the EED System were being recorded in FLAIR. These transaction dates frequently did not adhere to the requirements specified in State law and the DFS FLAIR Procedures Manual as the latter of the date the invoice (an accurate payment request that meets contract specifications and DFS contract payment requirements) was received or the goods and services were received, inspected, and approved for payment. The use of inaccurate transaction dates limits DFS management's ability to adequately monitor for prompt payments. Additionally, the inaccurate transaction dates may cause DFS prompt payment calculations to be in error, potentially resulting in underpayment by the Department of interest penalties due to vendors (contractors).

Recommendation: The Department should ensure that the transaction dates are accurately reported in the EED System in accordance with State law and the DFS FLAIR Procedures Manual.

Initial Agency Response:

Agree. The SiteManager estimates may produce inaccurate transaction dates and we will take the appropriate corrective actions to ensure appropriate transaction dates are being used in the EED system. The processes will then be validated during the Department's Quality Assurance Reviews.

6-month Agency Follow-up Response:

OOC agrees the SiteManager estimates may produce inaccurate transaction dates and are working on the appropriate corrective actions to ensure appropriate transaction dates are being used in the EED system. The processes will then be validated during the Department's Quality Assurance Reviews.

Completion Date: Estimated 12/1/2014.

Finding No. 2: Application and User Controls: EED System construction and consultant payment request transactions and payment information submitted to and received from FLAIR and other Department databases were not always reconciled by the Department.

Input controls related to system interfaces consist of those controls over the timely, accurate, and complete processing of information that is exchanged between applications. Interface controls include procedures that are intended to provide reasonable assurance that only correct data is accepted into the system and input errors are recognized and corrected. Such procedures typically include batch totals, reconciliations, and control totals. Whereas, output controls related to system interfaces consist of controls and related procedures to ensure, among other things, the integrity of the data throughout the transport process. Such procedures typically include reconciliations between the source and target applications to ensure the interface is complete and accurate.

Our review of EED System interface processes involving EED System construction and consultant payment request transactions and payment information submitted to and received from FLAIR and other Department databases disclosed that payment request transactions and payment information were not always being reconciled. EED System error reports existed to log some EED System errors. However, there were no reports that logged errors in the EED System load and database paid date transfer processes to ensure that only complete and accurate data was being loaded and processed in the EED System or sent to FLAIR and other Department databases. Without an effective method to reconcile EED System construction and consultant payment request transactions and payment information submitted to and received from FLAIR and other Department databases, the risk is increased that inaccurate and incomplete information may be processed, payment request transactions may not be appropriately updated, or errors may not be timely detected.

Recommendation: The Department should implement reconciliation processes to provide reasonable assurance that errors in the interface of information among the EED System, FLAIR, and other Department databases, should they occur, are timely detected and corrected by the Department.

Initial Agency Response:

Agree. Reconciliation between other Department databases and EED are required and will enhance the EED system to produce reconciliation reports to show that transfers of data are being timely detected, reconciled, and corrected by the Department. However, we have mitigating controls in place to make sure that vouchers are timely and accurately approved by the Department of Financial Services.

6-month Agency Follow-up Response:

OOC agrees reconciliation between other Department databases and EED are required and is working with the EED programmers to enhance the EED system so that reconciliation reports show that transfers of data are being timely detected, reconciled, and corrected by the Department.

Completion Date: Estimated 9/1/2014.

Finding No. 3: Application and User Controls: Payment request transactions loaded from the SiteManager interface into the EED System with inaccurate cost detail data were not identified, corrected, and reprocessed through normal processing that included appropriate approvals.

Effective interface processing procedures ensure that any errors that occur during the interface run are identified and corrected. Adequate error handling procedures during data entry provide reasonable assurance that errors and irregularities are detected, reported, and corrected. Appropriate controls include procedures to ensure that errors are identified, corrected, and reprocessed through normal processing. Through our review, we determined that payment request transactions that were loaded into the EED System with inaccurate cost detail information were not being identified, corrected, and reprocessed through normal processing.

For SiteManager progress estimate payment requests approved and received from the District Offices, EED automated processes used cost detail data as the basis for systematically generating FLAIR payment request transactions that were then interfaced to FLAIR for DFS payment processing. However, when payment request transactions failed the EED System edits and Disbursement Operations Office staff chose to process the progress estimate, staff manually entered the FLAIR payment request transactions using the EED System auto-manual method, bypassing the automated processes that used the cost detail transaction data to systematically generate the related FLAIR payment request transactions. Consequently, the previous approvals by District Office management were invalidated and the new payment request transactions were not subject to a subsequent documented approval by appropriate independent Department management.

The risk of modifying previously approved payment request transactions without resubmitting the transactions through normal processing and not obtaining approval from appropriate independent Department management is that unauthorized and inappropriate payment request transactions may be processed and submitted to FLAIR without detection.

Recommendation: The Department should implement controls to ensure that all modifications to payment request transactions are approved by appropriate independent Department management before submission to FLAIR.

Initial Agency Response:

Agree. Modifications of FLAIR account coding do not require the transaction go back through SiteManager, the originating system. In order to help clarify the situation we have removed the certification language on the SiteManager estimates that stated the authorized official was certifying the FLAIR account coding was valid. The authorized officials are only certifying that the goods and services were received and all required contractual requirements were met. The Office of Comptroller has the ultimate responsibility of ensuring that the appropriate funds are used, implementation of funding priorities, project costing, and disbursement of state funds. Some funding policies are temporary and do not warrant extensive modification to the system (for example, uses and timing of use of Federal Economic Stimulus Funding under ARRA – American Recovery and Reinvestment Act). Additionally, the Disbursement Operations Staff control the coding behind the automated processes that determine the FLAIR transaction details, and any manually entered transactions using the auto-manual process still go through the same EED edits as an automated transaction. The Department has assessed the risk and past performance and determine that the controls in place are sufficient.

6-month Agency Follow-up Response:

Completed.

Finding No. 4: Application and User Controls: Automated coding processes within the EED System introduced inaccurate system-generated information to the payment request transactions.

Application input controls ensure that only correct data is entered into a system and include processes that ensure data is validated and edited as close to the time and point of origination as possible. Interface (input) controls include edit checks and validations that help ensure the data received from other systems is accurate and complete. These controls help to ensure that problems with interfaced data are recognized and that appropriate corrections are made in a manner that ensures the correction is verified, authorized, and reprocessed as part of normal processing and does not compromise the original transaction's authorization levels.

Our review of EED System input and processing controls disclosed that payment request transactions were being loaded and processed in the EED System with inaccurate system-generated information. Because of the large number of payment request transactions, the EED System was developed with automated coding processes to increase the accuracy of the transactions and limit the amount of manual intervention to process payments. As a result of the automated coding processes and the logic used by these processes, some of the payment request transactions processed in the EED System contained inaccurate information. Examples included:

- As discussed previously in Finding No. 1, the EED System program logic assigns inaccurate transaction dates.

- When the source input system did not provide dates for certain fields, such as CITS service from, CITS service to, and SiteManager estimate cutoff, the EED System program logic defaults to an inaccurate date

- If a cost function had multiple encumbrance lines, in the encumbrance file, with different expenditure object codes for a project, the EED System and its related automated coding process selected the cost detail information based on which encumbrance line was added first. Using this method, the Department expensed items using a first-in, first-out method. The EED System expenses all of the first encumbrance line that matches the project and function before continuing to the next line without ensuring that the expenditure is associated with the appropriate expenditure object code.

Although these examples are not significant when taken individually, when considered together, along with the absence of prepayment and monthly postpayment voucher audit reviews and inadequate Department reviews as discussed in Finding No. 5 below, the control risk becomes more significant. Allowing payment request transactions to be loaded and processed in the EED System with inaccurate system-generated information increases the risk that payments for construction and consultant contracts will not be accounted for accurately.

Recommendation: The Department should implement input and processing controls to enhance the integrity of payment request transaction information and to ensure that only accurate payment request transaction information is entered and processed for payment.

Initial Agency Response:

Agree. Date logic may assign inaccurate transaction dates and will take corrective actions where appropriate. We agree that the system generally uses the oldest funding first when processing a payment. Construction contracts are not tracked at a granular object code level and the only difference is between the classifications of design versus construction. Based on our analysis of risk, we do not see the cost benefit of both the SiteManager and EED system to track expenditures by object code.

6-month Agency Follow-up Response:

OOC agreed that date logic may assign inaccurate transaction dates and will take corrective actions where appropriate as mentioned in Finding 1.

Completion Date: Estimated 12/1/2014.

Finding No. 5: Application and User Controls: Data processing controls, including review and monitoring procedures, were inadequate to ensure the accuracy and appropriateness of payment request transactions processed by the EED System.

Data processing controls include procedures that ensure that data is processed completely and accurately, that data retains its validity during processing, and that effective independent review and monitoring procedures are in place. The Disbursement Operations Office's data processing controls needed improvement to provide effective review and monitoring of payment request transactions processed by the EED System. Specifically:

- Voucher reviews were not performed in sufficient detail to ensure that only authorized, approved, and accurate SiteManager payment requests were being loaded and processed in the EED System, submitted to FLAIR, and paid. Disbursement Operations Office voucher reviews included only matching the vouchers to the related SiteManager estimates and verifying that the payment requests had been signed, indicating approval. The reviews did not include verification of other relevant information such as transaction and approval dates and did not ensure that the payment request approval was from an authorized employee.

- The EED SiteManager vouchers had an electronic approval signature of the Disbursement Quality Assurance Manager who did not perform voucher processing or reviews. The signature should be of the person who actually performed the review or approval of the review, not the manager of a different section who was not involved in the review process.

- We also noted that the same employees within the Disbursement Operations Office who were responsible for EED SiteManager payment request modifications, using the auto-manual method, were performing the voucher reviews, resulting in some employees performing incompatible job duties.

- Quality review procedures performed bimonthly by the Quality Assurance Section within the Disbursement Operations Office consisted of selecting only 10 EED SiteManager and 10 CITS payment request transactions each month, notwithstanding that there were over 22,000 EED SiteManager and CITS payment requests processed using the EED System from January 1, 2012, through October 31, 2012. Our inquiry of the quality review procedures disclosed that the Quality Assurance Section did not perform the review procedures in sufficient detail to ensure the accuracy of the relevant information (i.e., Disbursement Operations Office management informed us that the payment request transactions were not reviewed to ensure that the estimate included such information as authorized signatures, transaction dates, and contract certification [approval] received dates). The lack of adequate data processing controls, including effective review and monitoring procedures, for payment request transactions processed by the EED System increases the risk that the payment request transactions may result in inaccurate or inappropriate payments.

Recommendation: The Department should improve data processing controls, including effective review and monitoring procedures, to ensure the accuracy and appropriateness of EED System payment request transactions.

Initial Agency Response:

Agree. The Department should implement additional data processing controls.

- The Department will take the appropriate corrective actions to ensure appropriate transaction dates are being used in the EED, and will create a process for documenting the authorized approver to make sure SiteManager estimates are signed by an authorized official.

- As discussed with the Department of Financial Services, the voucher signature represents that the payment has gone through the Department's processes and is ready for disbursement and entry in the Department's general ledger. After risk analysis, the Department has determined that adding a new level of approval to the process is not cost beneficial.

- Although voucher reviews were done by the same employee that processed estimates in the EED system, the payments originate in either the CITS or SiteManager system. Both systems also require two or more separate users to approve the payment before it is transferred to EED. Based on our risk analysis it has been determined that the mitigating controls minimize any risk and that the addition of staff to segregate this process would not be cost beneficial.

- The Department is reviewing and strengthening the QAR procedures to mitigate risk.

6-month Agency Follow-up Response:

OOC agreed that date logic may assign inaccurate transaction dates and will take corrective actions where appropriate as mentioned in Finding 1.

The Department is continuing to review and strengthen the QAR procedures to mitigate risk.

Completion Date: Estimated 12/1/2014.

Finding No. 6: Application and User Controls: Procedures for ensuring timely contract payments needed improvement.

Controls should provide reasonable assurance that transactions are properly recorded with the correct data in a timely manner. During our audit, we noted instances where Disbursement Operations Office procedures for ensuring timely contract payments needed improvement. Specifically:

- During our review of a final construction estimate, Disbursement Operations Office staff disclosed that staff had not reviewed the related contract documentation to ensure that the payment was made timely. Section 337.141(2) through (4), Florida Statutes, establishes the length of time within which the Department is required to pay final construction contract estimates before a vendor (contractor) is entitled to late-payment interest. Upon further audit inquiry, Disbursement Operations Office management stated that it is District Office management's responsibility to communicate a required payoff date so that Disbursement Operations Office staff can ensure a timely payment. However, the Department's Web site and Disbursement Operations Office management responses for other audit issues indicate it is the responsibility of the Disbursement Operations Office to ensure timely payments. If Disbursement Operations Office staff do not specifically review for timeliness of payments, the risk is increased that construction estimates may not be timely paid and that the Department may incur late-payment interest penalties.

- The voucher monitoring process performed by Disbursement Operations Office staff to ensure the timely payment of vouchers included verification that a voucher was paid, but there was no evidence maintained to indicate that a detailed review was performed to ensure that each payment request on the voucher was timely paid. Disbursement Operations Office management stated that, in addition to monitoring voucher aging reports, staff also relied on DFS dropped-payment notices and warrant distribution procedures, as well as contractor inquiries, to help provide assurance that payment request transactions dropped by FLAIR would be discovered and paid. The practice of recording payment request transactions as paid in the EED System and other Department databases before the warrant is issued, combined with the possibility of staff not performing a detailed review of all payment requests on the vouchers, increases the risk that an EED System payment request transaction could be dropped prior to or during FLAIR payment processing and not be timely discovered and paid.

Inadequate EED System payment processing review procedures, such as those discussed above, increases the risk that EED System payment request transactions may result in no payment or may result in untimely payments.

Recommendation: The Department should implement adequate review procedures to ensure timely payments for payment request transactions processed by the EED System.

Initial Agency Response:

Agree. Transaction dates recorded in EED may be inaccurate and the Department will take the appropriate corrective actions to ensure appropriate transaction dates are being used in the EED as discussed in Management Response to Finding No. 1.

We agree evidence of the voucher monitoring process had not been maintained. Although our current practices revealed timely payments, our procedures will be reviewed to strengthen where possible.

6-month Agency Follow-up Response:

OOC agrees that the Departments use of transaction dates and voucher procedures need improvement as written in the report.

The transaction dates are being addressed as mentioned in Finding 1. The voucher procedures are currently being reviewed to strengthen where possible.

Completion Date: Estimated 12/1/2014.

Finding No. 7: Application and User Controls: Payment request transactions were processed by the EED System for a contract type that was not approved by DFS for EED System processing.

Business process controls are the automated and manual controls applied to business transaction flows and relate to the completeness, accuracy, validity, and confidentiality of transactions and data during application processing. Validity controls provide reasonable assurance that all recorded transactions actually occurred, relate to the organization, and were properly approved in accordance with management's authorization and that output contains only valid data. A transaction is valid when it has been authorized and when the master data relating to that transaction is reliable.

The Department was granted approval by DFS to process payment request transactions through the EED System. This approval was limited to all District and Statewide construction contracts (voucher processing site 09) in SiteManager and all professional services contracts (voucher processing site C) in CITS. However, our audit disclosed that Disbursement Operations Office staff did not ensure that payment request transactions for other non-DFS approved contract types were restricted from being processed by the EED System.

Although only construction and consultant contracts were authorized by DFS and Department management to be processed through the EED System, we noted that payment request transactions for two District Office maintenance contracts were processed by the EED System, submitted to FLAIR, and paid. District Office staff had misclassified these maintenance contracts as construction contracts and the contracts were accepted and added to the Approved-for-EED contract list by Disbursement Operations Office staff. Subsequent to our audit, the Department requested and obtained approval from DFS to begin processing selected maintenance contracts through the EED System. The maintenance contracts that are now allowed to be processed by the EED System are required to be based on the estimated completion of work and must undergo an engineering review and reconciliation (final estimates review process). Although maintenance contracts that meet the specified criteria are now allowed to be processed in the EED System, this authorization was not in effect at the time the two contracts discussed above were inappropriately submitted to and processed by the EED System and were not detected as being misclassified as construction contracts. Without appropriate reviews of the contract types associated with the payment request transactions being processed, the risk exists that the Department may continue to inadvertently process inappropriate payment transactions through the EED System without detection.

Recommendation: The Department should implement independent review procedures to ensure that payment request transactions processed through the EED System are limited to the contract types approved by DFS.

Initial Agency Response:

The Department (OOC) determined that the contracts were construction related, were estimate based and followed the final estimate process; thus appropriately meeting the criteria to be processed in the EED system.

In order to address the Auditor General's concern, on July 31, 2013, the Department received written approval from the Department of Financial Services to process Maintenance contracts in the EED system. With that approval DFS has granted the Department authority to process Professional Services contracts, and Construction/Maintenance contracts that meet the criteria of being estimate based and subject to the final estimates review process. The approval has removed any questions with the Department's authority to process all future professional services and estimate based contracts through the system.

6-month Agency Follow-up Response:

Completed.

Finding No. 8: Security Controls: Access procedures for granting or removing access privileges to the EED System needed improvement. Also, as similarly noted in prior audits of the Department, most recently our report No. 2011-174, some Department security procedures were outdated.

Sound IT management includes the establishment of security policies and procedures that describe management's expectations for controlling the Department's IT operations. Written policies and procedures help ensure that management directives are clearly communicated, understood, accepted, and followed by all staff. Our review of the Department's security procedures, including system backup procedures, disclosed that some procedures needed improvement as noted below:

EED System Access Procedures

Although the Department had Department wide access control procedures, these procedures did not specifically address access to the EED System and related IT resources. The Disbursement Operations Office had not implemented adequate written procedures for granting or removing update access privileges to the EED System application and database for Disbursement Operations Office and District Office users. The Disbursement Operations Office did not have written procedures for assigning or removing access to the EED System. The District Office access custodian maintained a list of access groups and related IT resources to assist her in the assignment of access to the EED System for District Office users; however, our review disclosed that the access information she maintained was outdated and inaccurate.

Outdated Department Security Procedures

As similarly noted in prior audits of the Department, most recently our report No. 2011-174, some Department procedures made reference to State law or Florida Administrative Code rules that had been repealed or superseded.

Specifically:

- Department procedures, Topic No. 325-060-555-a, Access to the Department's Computer Network Resources, dated August 8, 2007; Topic No. 325-A80-221-a, Authorization to Request Migration of Code to the Production Environment, dated August 18, 2003; and Topic No. 325-A00-005-b, Access and Use of Production Environments, dated February 11, 1999; included references to Section 282.3055, Florida Statutes, which was repealed effective July 1, 2011.

- Department procedure, Topic No. 325-060-555-a, Access to the Department's Computer Network Resources, dated August 8, 2007, included references to Chapter 60DD-2, Florida Administrative Code, which was replaced by Chapter 71A-1, Florida Administrative Code, on November 15, 2010.

- Department procedure, Topic No. 325-A01-020-b, Mainframe Backup Procedure, dated April 13, 1998, included a reference to Chapter 44-4, Florida Administrative Code, which was repealed in June 1998.

The lack of accurate written EED System access procedures and the above-described outdated Department security procedures limit the assurance that management's expectations will be properly and consistently communicated, understood, and carried out.

Recommendation: The Department should establish and implement adequate written access procedures for the EED System, update existing procedures, and periodically review all procedures to ensure that the procedures are current and reflect management's expectations.

Initial Agency Response:

Agree. As of June 17, 2013 the Department has updated its process for requesting access, access changes, and access terminations to the EED system. Regarding outdated security procedures, the Department recently converted 18 of its technology related policies and procedures to a manual format to streamline the review and update process. This effort was finalized on July 9, 2013. During the conversion process minor updates were made to correct outdated references. The Department is now in the process of making substantive updates to the Manual as appropriate.

6-month Agency Follow-up Response:

Completed.

Finding No. 9: Security Controls: The Department did not perform adequate periodic reviews of user access privileges to the EED System application and related IT resources.

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights (privileges) periodically based on risk, access account change activity, and error rate. Periodic reviews of user access privileges help ensure that user access privileges remain appropriate.

Our audit disclosed that the Department did not perform adequate periodic reviews of user access privileges to the EED System application and related IT resources. The reviews of user access privileges that were performed were limited in scope and frequency. As indicated by the excessive access privileges disclosed in Finding Nos. 10 and 11 below, the lack of periodic reviews of access privileges, along with the absence of adequate written procedures for granting or removing update access privileges to the EED System application and database disclosed in Finding No. 8 above, increase the risk that inappropriate access privileges may not be timely detected or remediated and may result in inappropriate or unauthorized changes to data and programs.

[1] During the 2012 Legislative Session, HB 5011 that abolished AEIT and reassigned the functions and duties of AEIT to a new State agency was passed by the Legislature and presented to the Governor for signature. The bill was vetoed by the Governor on April 20, 2012. However, AEIT underwent defacto dissolution as the 2012 General Appropriations Act made no appropriations for the funding of positions in AEIT. As of the completion of our audit, rulemaking authority and responsibility for promoting or enforcing compliance with existing AEIT rules had not been established.

Recommendation: The Department should perform adequate periodic reviews of user access privileges to the EED System application and related IT resources to ensure that user and system account access privileges remain appropriate and that any unnecessary access privileges detected are timely deactivated.

Initial Agency Response:

Agree. As of June 17, 2013, the Office of Comptroller and the Office of Information Systems added the Electronic Estimates Disbursement (EED) System to the Automatic Access Request Form (AARF) System. Pursuant to Section 2.9.1 Chapter 2, Access to the Department's Computer Network Resources, of the Information Technology Resource User's Manual, Topic No. 325-000-002, users' systems access shall be validated on an annual basis. Further, upon the approval of proposed changes to Chapter 2, all enterprise applications which require authentication shall be requested through the AARF System. Lastly, the Office of Information Systems has implemented a monthly termination validation process by which terminated users are validated in the AARF System as well as the Department's mainframe and network identity management systems to ensure the timely revocation and deletion of access.

6-month Agency Follow-up Response:

Completed.

Finding No. 10: Security Controls: Some Department employees, contractors, and outside agency employees (i.e., primary data center employees) had been granted update access privileges to the EED System application, production source code and JCL libraries, and database that were not necessary for their assigned job duties and did not enforce an appropriate separation of duties.

Effective access controls include measures that limit employee, contractor, and outside agency employee access privileges to only what is necessary in the performance of assigned job duties and enforce an appropriate separation of incompatible duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

AEIT Rule 71A-1.007(3), Florida Administrative Code, provides that workers, including employees and other individuals whose conduct is under the direct supervision of an agency, shall be authorized access to agency IT resources based on the principles of "least privilege" (the principle that grants the minimum possible privileges to permit a legitimate action) and "need to know" (the principle that individuals are authorized to access only specific information needed to accomplish their individual job duties). AEIT Rule 71A-1.007(5), Florida Administrative Code, provides that, for functions susceptible to fraudulent or other unauthorized activity, an agency shall ensure separation of duties so no individual has the ability to control the entire process.

Our review of the appropriateness of access privileges to the EED System application, production source code and JCL libraries, and database disclosed that some Department employees, contractors, and outside agency employees had been granted update access privileges that were not necessary for their assigned job duties and did not enforce an appropriate separation of duties. These conditions increase the risk of errors, fraud, misuse, or other unauthorized modification of Department data.

Specifically:

EED System Application

Of the Department employees, contractors, and outside agency employees included in our tests who had been granted update access privileges to one or more EED System access groups as of October 10, 2012, and December 5, 2012, 64 had access privileges that were unnecessary or did not enforce an appropriate separation of duties.
Specifically:

Disbursement Operations Office

- Two Disbursement Operations Office employees with membership in the EED Disbursement Operations Office CO access group did not require the access privileges provided by the group to perform their assigned job duties evidenced by the nonuse or infrequent use of the access privileges.

- Four Disbursement Operations Office employees with update access privileges through membership in the EED Disbursement Operations Office CO access group had access privileges that did not enforce an appropriate separation of duties in that these access privileges provided the users with update capabilities to input and approve the same transaction, which may result in unauthorized changes being made to transactions without independent review.

District Offices

- Twenty-two employees and contractors included in the EED Districts CRS access group did not require the access privileges of the group to perform their assigned job duties.

- Thirty-two employees and contractors included in the EED Districts CRS access group needed some, but not all, of the group privileges to perform their job duties.

- Two employees included in the EED District 5 access group did not require the access privileges of the group to perform their assigned job duties.

- Two District Office employees with access custodial privileges to the EED Districts CRS access group had inappropriate access privileges that did not enforce an appropriate separation of duties. The two District access custodians had been performing end user functions in addition to their EED System access custodial duties. During our review, we also identified a system account that had unnecessary update access privileges resulting from membership in the EED Districts CRS access group.

Other audit procedures disclosed that multiple District construction employees had certified (approved), reviewed, and released the same EED System payment request transaction prior to EED payment processing, contrary to an appropriate separation of duties.

Production Source Code, Job Control Language (JCL), and EED Database

Our review of user IDs with access privileges to production source code and JCL libraries as of November 15, 2012, disclosed that 11 system programmers (outside agency employees) had unnecessary ALTER access privileges to the production source code library outside of change management software and 1 of the 11 system programmers also had inappropriate access privileges to the production source code through the change management software. In addition, 5 of the 11 above-mentioned system programmers had inappropriate ALTER access privileges to the JCL library.

System programmers having unnecessary and inappropriate ALTER access privileges to production source code and inappropriate ALTER access privileges to the JCL library is inconsistent with an appropriate separation of incompatible job duties and may result in inappropriate or unauthorized changes to the data and programs.

Our review of user IDs with database system authorities as of September 27, 2012, disclosed that two user IDs did not require database system authorities and five user IDs (belonging to 5 of the 11 above-mentioned system programmers) had inappropriate access privileges to the EED database due to a lack of separation of incompatible systems programming and database administration duties. In response to audit inquiry, Department staff indicated that the two user IDs were no longer needed.

Recommendation: The Department should limit update access privileges for employees, contractors, and outside agency employees to the EED System application, production source code, JCL, and EED database to only what is needed to perform assigned job duties, giving consideration to establishing access groups with more limited access privileges to perform users' assigned job duties. In addition, the Department should evaluate employee, contractor, and outside agency employee job duties related to the EED System to ensure enforcement of an appropriate separation of incompatible duties. Where a proper separation of duties cannot be achieved due to limited staff, the Department should implement effective compensating controls to minimize the risk of compromise to data and IT resources.

Initial Agency Response:

Agree. We agree with the findings regarding district offices and have already reviewed and updated access privileges inherited through group memberships and worked with appropriate offices to limit the scope of group access privileges.

Agree. We agree with the finding pertaining to two Disbursement Operations Office employees with membership in the EED Disbursement Operations Office CO access group and will remove their additional access immediately. The Department has performed a risk analysis and determined the mitigating controls in place are sufficient and that it is not cost beneficial to add staff in order to segregate the duties as outlined.

Disagree. We do not agree with the finding pertaining to production source code, job control language, and EED database. As requested throughout the Audit, the Department provided evidence demonstrating justification for elevated access and approval for elevated access as requested by outside agency employees and approved by appropriate Department staff. Additionally, the Department has written into section 6.4 of its Security and Use of Information Technology Resources Policy that "information technology resource users shall be granted access to information technology resources based on the principles of least user privilege and need to know." Although the Department does not agree with this finding, we will ensure periodic review of elevated accesses and take action as appropriate to remove privileges no longer needed.

6-month Agency Follow-up Response:

Completed.

Finding No. 11: Security Controls: The Department did not deactivate the access privileges of some former employees, contractors, and outside agency employees in a timely manner. In addition, as similarly noted in prior audits of the Department, most recently our report No. 2011-174, the Department did not retain relevant access control records or audit trails for a sufficient duration of time for the Department's network and EED System application, contrary to State of Florida General Records Schedule provisions.

Effective IT access controls include provisions to timely deactivate employee and contractor access privileges when employment or contractual services are terminated. Prompt action is necessary to ensure that the former employee or contractor access privileges are not misused by the former employee, contractor, or others. Department procedure, Topic No. 325-060-555-a, Access to the Department's Computer Network Resources, requires prompt action to be taken in removing the IT access privileges of former users.

In addition, the State of Florida, General Records Schedule GS1-SL for State and Local Government Agencies (General Records Schedule), revised by the Department of State effective August 2010, provides that the record series Access Control Records consist of records pertaining to employee or contractor access to resources such as computer networks including, but not limited to, network account and permission records. Access control records must be retained for one anniversary year after superseded or after the employee separates from employment. In addition, the record series Audit Trails: Critical Information Systems consists of system-generated audit trails tracking events related to records in critical information systems including, but not limited to, financial transaction records. Audit trails track such information as the user, date and time of event, and type of event. Since audit trails may play an integral part in prosecution, disciplinary actions, or audits or other reviews, agencies are responsible for ensuring that internal management policies are in place for retaining audit trails as long as necessary for these purposes.

As discussed in the following paragraphs, our review of access privileges to the Department network, EED System application, and EED System database and production programs disclosed that some former employee, contractor, and outside agency employee access privileges were not deactivated in a timely manner and, in some instances the Department had not retained relevant access control records or audit trails for a sufficient duration of time.

Network

We compared the names of former employees who terminated employment with the Department during the period January 1, 2012, through October 10, 2012, to a December 13, 2012, listing of employees, contractors, and outside agency employees with network access privileges to determine whether the former employees retained access to the network and if their network access privileges were deactivated in a timely manner upon termination. Our review disclosed that, of the former employees in our comparison, five retained their network access privileges for 11 to 74 days after termination and two retained their network access privileges for 270 and 332 days after termination. According to documentation provided by the Department, the network access privileges of four of the seven former employees were not used after their termination dates. The Department, however, was unable to provide similar documentation for the remaining three former employees.

Through additional audit procedures, we noted that a former outside agency employee had retained his network domain administrative access privileges for 81 days after his employment had terminated. The access privileges of the former outside agency employee had not been used after his termination date.

EED System Application

Our comparison of the above-mentioned former employees' names to the user access lists for the EED System disclosed that three former employee user IDs remained in EED System access groups beyond the former employees' termination dates. Although one user ID was timely revoked in the mainframe security management system, the user IDs of the other two former employees remained active in the mainframe security management system for 37 and 40 days after termination, and all three user IDs continued to be included in EED System access groups.

Through additional audit procedures, we noted that two additional former employee user IDs were not timely revoked and remained active in the mainframe security management system for 6 and 27 days after termination. These two user IDs also continued to be included in EED System access groups. Furthermore, another former employee user ID continued to be included in EED System access groups since January 31, 2005; however, we could not determine when the user ID was revoked in the mainframe security management system because relevant access control records or audit trails were not retained.

Finally, our examination of users with update access privileges within the EED System access groups disclosed that the user ID of one former contractor, although revoked in the mainframe security management system on December 31, 2004, continued to be included in an EED System access group through February 4, 2013.

EED System Database and Production Programs

Our review of EED System database and production programs access privileges disclosed that one former outside agency employee retained access privileges to the EED System database and production programs for 159 days after his termination date. The EED System database and production program access privileges of the former outside agency employee were not used after his termination date.

Our review disclosed that, contrary to the Access to the Department's Computer Network Resources procedure, prompt action had not been taken in removing the IT access privileges of former users and, contrary to the General Records Schedule, the Department had not retained relevant access control records or audit trails related to the Department's network and EED System application. This was similarly noted in prior audits of the Department, most recently our report No. 2011-174. Without the timely deactivation of access privileges of former employees, contractors, and outside agency employees and the retention of relevant access control records or audit trails, the risk is increased that access privileges may be misused by the former employee, contractor, outside agency employee, or others and the Department may not have sufficient documentation to investigate security incidents, should they occur.

Recommendation: The Department should ensure that network, EED System application, and EED System database and production programs access privileges are deactivated in a timely manner. The Department should also ensure that relevant access control records or audit trails are retained for the network and EED System application as provided for in the General Records Schedule.

Initial Agency Response:

Agree. The Office of Information Systems has implemented a monthly termination validation process by which terminated users are validated in the AARF System and the Department's identity management systems for mainframe and the network to assure the timely revocation and deletion of access. The Office of Information Systems maintains system generated network events via an event tracking, monitoring, alerting, and reporting system. Certain events are generated as alerts or reports and are maintained beyond retention requirements. As a result of this finding, and in an effort to improve upon the Department's efforts in this area, the Office of Information Systems shall review its log archiving policies with the intent to expand the long-term accessibility of logs.

Additionally, the Office of Information Systems now logs certain mainframe events, and is preparing to expand logging for this technology platform. The Department has requested a mainframe review with the intent of including within the Statement of Work, a review of logging capabilities and best practices.

6-month Agency Follow-up Response:

Completed.

Finding No. 12: Security Controls: Contrary to Agency for Enterprise Information Technology (AEIT) Rules, Florida Administrative Code, the EED System primary and secondary database administrators within the Enterprise Technology Services and Support area administrated the EED System database by sharing a user identification code (user id) and corresponding password for authentication.

Effective access controls include a process for the unique identification and authentication of systems users. The unique identification of system users allows management to affix responsibility for system activity to an individual person. AEIT Rule 71A-1.019(11), Florida Administrative Code, provides that agency computer users shall have unique user accounts.

Our review of the EED System database access privileges disclosed that the primary and secondary database security administrators within the Enterprise Technology Services and Support area administered the EED System database by sharing one user ID and corresponding password for authentication. The sharing of one user ID and password may limit the Department's ability to assign responsibility for system actions.

Recommendation: The Department should assign a unique EED System database user ID and corresponding password to each employee who is authorized to perform database security administration functions.

Initial Agency Response:

Agree. The Office of Information Systems shall review the use of shared accounts and to the extent possible create separate user-IDs for systems administration.

6-month Agency Follow-up Response:

Completed.

Finding No. 13: Security Controls: The Department had no written authorization documentation for one user with domain administrator privileges. In addition, no written authorization documentation was retained for EED System users who had been employed for longer than five years, contrary to AEIT Rules, Florida Administrative Code and General Records Schedule requirements.

AEIT Rule 71A-1.007(1), Florida Administrative Code, provides that agency information owners shall be responsible for authorizing access to information. Effective access controls include, among other things, the use of access authorization forms to document management's authorization of user access privileges. In addition, the General Records Schedule provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment.

Our review of the appropriateness of domain administrator access privileges for 19 network administrator user accounts disclosed that there was no written authorization documentation for one user. Additionally, our review of EED System access procedures disclosed that the access authorization forms (e-mails) for EED System application access privileges were being retained for only five years. As a result, for users who remained employed for longer than five years, there were no authorization forms. The lack of authorization documentation for user access privileges may limit the Department's ability to ensure that access privileges granted to employees do not exceed what is necessary for the accomplishment of assigned job responsibilities and does not comply with the General Records Schedule requirements for the retention of access control records.

Recommendation: The Department should retain access authorization documentation so that management has the necessary documentation to ensure that access privileges granted are consistent with what management authorized and to ensure compliance with the General Records Schedule requirements for the retention of access control records.

Initial Agency Response:

Agree. We agree with the component of the finding pertaining to the retention of access authorization documentation for five years. The Department has already implemented a new process for requesting and documenting EED system access requests, access change requests, and access termination requests to comply with retention requirements. This new process was implemented on June 17, 2013.

Disagree. We do not agree with the portion of the finding pertaining to the retention of written authorization documentation for one network administrator. The user in question administered a domain no longer owned by the Department, but still logically associated with the Department's network. During audit inquiry, the Department referred the request for documentation to the appropriate state agency. The domain in question no longer exists and this is resolved.

6-month Agency Follow-up Response:

Completed.

Finding No. 14: Security Controls: The Department had not developed security software access groups at a granular level related to specific job duties for assignment of access privileges within the EED System.

The effectiveness of access controls is enhanced by the establishment of documentation that correlates access groups with specified job duties. Our audit disclosed that the security software access groups for the EED System were not adequately correlated with specified job duties.

Although the Guide describes separate functions that are the responsibilities of the Disbursement Operations Office and District Offices, the security software access groups were not defined to a granular level beyond the single access group assigned by District, the single access group for all Districts, and the two access groups in the Disbursement Operations Office. The access privileges were separated by offices, but not within the offices for specific job duties.

The lack of the correlation of security software access groups for the EED System to a granular level with specified job duties allows for inappropriate access capabilities and the assignment of incompatible job duties as previously described in Finding No. 10.

Recommendation: The Department should develop security software access groups at a granular level related to specific job duties for assignment of access privileges within the EED System.

Initial Agency Response:

Agree. The Department's access groups are not at a granular level as written in the report; however, the Department's risk analysis determined that the mitigating controls are sufficient and that a rewrite of the system to add additional levels would not be cost beneficial.

6-month Agency Follow-up Response:

Completed.

Finding No. 15: Security Controls: Certain security controls related to the EED System in the areas of inappropriate access accounts; security events logging; user authentication and network session controls; administrator accounts; privileged attributes; protection of confidential and exempt information; risk analysis; and monitoring of EED System error reports and data processing reports, including reports of manually entered transaction modifications, needed improvement. Some of the issues were communicated to Department management in connection with prior audits of the Department, most recently our report No. 2011-174.

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain security controls related to the EED System in the areas of inappropriate access accounts; security events logging; user authentication and network session controls; administrator accounts; privileged attributes; protection of confidential and exempt information; risk analysis; and monitoring of EED System error reports and data processing reports, including reports of manually entered transaction modifications, needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Department management and staff of the specific issues. Some of the issues were communicated to Department management in connection with prior audits of the Department, most recently our report No. 2011-174. Without adequate security controls related to certain network and software access, risk analysis, logging, and monitoring, the confidentiality, integrity, and availability of data and IT resources may be compromised.

Recommendation: The Department should implement appropriate security controls related to inappropriate access accounts; security events logging; user authentication and network session controls; administrator accounts; privileged attributes; protection of confidential and exempt information; risk analysis; and monitoring of EED System error reports and data processing reports, including reports of manually entered transaction modifications, to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Initial Agency Response:

Agree. The Office of Information Systems shall review appropriate security controls pertaining to event logging, user authentication and network session controls, administrator accounts, privileged attributes, protection of confidential and exempt information, and risk analysis with the goal of resolving areas of non-compliance and updating policies and procedures as appropriate.

6-month Agency Follow-up Response:

Completed.