Internal Audit Report

Electronic Bidding and Contract Letting

TxDOT Office of Internal Audit
**Objective**
Review of process controls and service delivery of the TxDOT electronic bidding process.

**Opinion**
Based on the audit scope areas reviewed, control mechanisms are effective and substantially address risk factors and exposures considered significant relative to impacting operational execution and compliance. The organization's system of internal controls provides reasonable assurance that most key goals and objectives will be achieved despite significant control gap corrections and improvement opportunities identified. Control gap corrections and improvement opportunities identified are likely to impact the achievement of the organization's business/control objectives, but management has agreed to corrective action plans to address the relevant risks within 6 months.

<table>
<thead>
<tr>
<th>Overall Engagement Assessment</th>
<th>Satisfactory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding</td>
<td></td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>Control Design</td>
</tr>
<tr>
<td>Finding 1: Data Security</td>
<td>x</td>
</tr>
</tbody>
</table>

Management concurs with the above finding and prepared management action plans to address deficiencies.

**Control Environment**
The TxDOT Construction Division (CST) contracts with a vendor who provides the client interfaces and data warehousing for the Electronic Bidding System (EBS). Although CST management incorporates controls in the electronic bidding process to assist with data entry and accuracy of input, considerable reliance is placed on the vendor to provide a secure environment. CST management assigns roles and responsibilities related to the EBS to assure the integrity and confidentiality throughout the bidding process.

**Summary Results**

<table>
<thead>
<tr>
<th>Finding</th>
<th>Scope Area</th>
<th>Evidence</th>
</tr>
</thead>
</table>
| 1       | Electronic Bid: Data Security | Utilization by the Construction Division (CST) of the 2010-2013 attestation reports noted the following::  
  - 4 of 4 (100%) annual attestation reports had no evidence of review by CST  
    - 2 of 4 (50%) annual attestation reports (fiscal years 2011 and 2012) were not requested for review by CST  
  Attestation reports are used to help provide assurance of an outside contractor's design and operating effectiveness of IT controls. |
Audit Scope
The audit focused on the electronic systems supporting the construction and maintenance monthly contract letting process. The systems were reviewed to verify bidders using the electronic processes are verified, data transmission is complete, and stored data is secured.

The audit was performed by Omar Elsaad, Patti Drummer, Ike Okoli, and Karin Faltynek (Engagement Lead). The audit was conducted during the period from March 24, 2014 through May 30, 2014.

Methodology
The methodology used to complete the objectives of this audit included:

- Reviewing State and Federal laws and standard operating procedures
- Interviews with key personnel such as the TxDOT letting administrator and letting officials
- Testing controls in the Electronic Bidding System
- Reviewing electronic bid transmissions between April 2, 2013 and April 3, 2014
- Examining data security environment (i.e., attestation reports of IT controls) of outsourced electronic bid service provider

These procedures were applied as necessary to perform the audit fieldwork.

Background
This report is prepared for the Texas Transportation Commission, TxDOT Administration, and Management. The report presents the results of the Electronic Bidding and Contract Letting Audit which was conducted as part of the Fiscal Year 2014 Audit Plan.

Highway construction and maintenance contracts are awarded through a sealed bid process. Electronic bidding, introduced in 2009, allows contractors to submit bids remotely while still in a secure environment. Electronic bids are collected and stored by a third party vendor in an electronic vault. This process provides several advantages to both bidders and TxDOT. Bidders benefit from ease of submission and controls embedded in the electronic process which also verifies completeness of the submitted bids. The review of sealed bids for fiscal year 2013 showed that approximately 81% of bids were submitted electronically.

The outsourcing of electronic data storage (i.e., the electronic vault) requires TxDOT to obtain assurance that controls are in place with the vendor to protect the data. Such assurance can be obtained by reviewing the vendor’s Statement on Standards for Attestation Engagements (SSAE) 16 reports.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and in conformance with the International Standards for the Professional Practice of Internal Auditing. 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. Recommendations to mitigate risks identified were provided to management during the engagement to assist in the formulation of the management action plans included in this report. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on

A defined set of control objectives was utilized to focus on operational and compliance goals for the identified scope areas. Our audit opinion is an assessment of the health of the overall control environment based on (1) the effectiveness of the enterprise risk management activities throughout the audit period and (2) the degree to which the defined control objectives were being met. Our audit opinion is not a guarantee against operational sub-optimization or non-compliance, particularly in areas not included in the scope of this audit.
Detailed Findings and Management Action Plans (MAP)

Finding No. 1: Data Security

Condition
The Construction Division (CST) did not utilize a process to verify adequacy of controls for the Electronic Bidding System (EBS) hosting partner. The EBS hosting partner should provide an annual attestation report, otherwise known as an SSAE 16 report, which provides an independent assessment on the design and operating effectiveness of the IT internal controls at the EBS hosting partner (i.e., outside vendor). These reports were not reviewed or always obtained from 2010 - 2013 to obtain independent assurance that the vendor’s controls were adequate.

Effect/Potential Impact
CST had no assurance the vendor was providing adequate control over confidential bid data. Without the knowledge of any potential control issues being addressed in the SSAE 16 report, mitigating controls may not have been introduced by TxDOT.

Additionally, not reviewing the annual attestation report can lead to the following:
- Reduced data reliability due to potential unaddressed control weaknesses
- Non-compliance with State requirements for data security assessment

Criteria
- TAC 202.72 “Managing Security Risks” requires an annual assessment of IT controls that cover high risk operational areas such as high dollar and confidential information
- TAC 202.25 “Information Security Resources Safeguards” requires general safeguards to be in place where electronic data is stored

Cause
A review process was not in place due to the following:
- The Service Level agreement (SLA) between TxDOT and the EBS hosting partner did not discuss when to request or submit an attestation report
- CST did not define or assign responsibility to review the annual attestation reports
- CST does not perform and document a risk assessment of information resources

Evidence
The annual attestation reports for the last 4 years of the contract (2010-2013) were available to the department; however, the following was noted:
- 4 of 4 (100%) annual attestation reports had no evidence of review performed by the CST project manager
  - 2 of 4 (50%) annual attestation reports (fiscal years 2011 and 2012) were not requested from the hosting partner for review by the CST project manager
Management Action Plan (MAP):

MAP Owner(s):
Roxana Garcia-Zinsmeyer, P.E., Section Director, Construction Division
Brian Hohle, Manager, Contract Letting and Contractor Pre-qualification Branch

MAP 1.1:
The Construction Division (CST) Contract Letting and Contractor Pre-qualification Branch will develop an information resources risk assessment process to identify and classify the potential threats and risks associated with the Electronic Bidding System (EBS) throughout its operation. This process will help identify the appropriate controls for reducing or eliminating risks during operation.

The documented risk assessment will, at the minimum, include:

- Identifying the key processes to achieving our business objectives
- Identifying the internal and external activities (risks) that will hinder achieving the key processes and their likelihood and impact
- Identifying the controls (activities) in place to mitigate the identified risks at both:
  - CST Letting Branch
    - User complementary controls
  - EBS hosting partner
    - Review SSAE 16 Attestation Report
    - Request assistance from subject matter experts, if necessary
- Monitor controls for effectiveness and make changes as appropriate
- Complete this process annually by the end of January for continuous improvement

Completion Date:
December 15, 2014

MAP 1.2:
Update the Service Level Agreement (“SLA”) between TxDOT and Electronic Bidding System (EBS) hosting partner to add as deliverables:

- Annual submission of SSAE 16 Report prepared by the independent service auditor
- General IT control activities at the EBS hosting partner that are designed, and in place, to protect and secure the data
- Define the Record Retention Policy for electronic bids at the EBS hosting partner

Completion Date:
September 15, 2014
Observations and Recommendations

Audit Observation (a):  Continuity Planning

The Construction Division (CST) has not documented its process to provide technical support for the contractor desktop application to electronic bidding vendors. This process is exclusive to and performed by one employee who is eligible for retirement.

Effect/Potential Impact
In the event of a sudden departure of the only current employee providing technical support services to vendors, the agency may temporarily find it difficult to continue providing electronic bidding services and support at an efficient operational level. A reduction in electronic bid support services may force the vendors to use the alternate manual bid option which will require more CST resources to process. Approximately 81% of all submitted bids are now electronic, representing $3.7 billion of contracts let in Fiscal Year 2013.

Recommendation
To support business continuity, CST should
- document the technical support services process provided to vendors who bid electronically
- routinely review the documentation for improvement
- provide training in the support of the contractor desktop applications to appropriate support personnel
- assign backup personnel for technical support
Summary Results Based on Enterprise Risk Management Framework

<table>
<thead>
<tr>
<th>ERM Component</th>
<th>Control Activities</th>
<th>Scope Areas Evaluated</th>
<th>Electronic Bid: Validation</th>
<th>Electronic Bid: Data Transmission</th>
<th>Electronic Bid: Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organizational Tone</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forecasting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Goal-Setting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cost-Benefit Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business Continuity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evaluations/Analysis</td>
<td>(a)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management Action Plans</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control Activities</td>
<td>Policies/Procedure Development &amp; Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Approvals/Authorizations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supporting Evidence/Records Availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Segregation of Duties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Safeguarding Assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information &amp;</td>
<td>Information Classification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Information Input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information Processing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Output/Reporting and Messaging</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td>Exception Reporting Review</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reconciliations/Root-Cause Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Peer Reviews</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management Representations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Closing Comments
The results of this audit were discussed with Construction Division management. We appreciate the assistance and cooperation received from the Construction Division employees contacted during this audit.