Department of Administrative Services

MBE Certification Program Audit

Audit Period: January through December 2018

Results Summary:

<table>
<thead>
<tr>
<th>Objective</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBE Certification Process</td>
<td>Improvement Needed</td>
</tr>
<tr>
<td>MBE Recertification Process</td>
<td>Improvement Needed</td>
</tr>
</tbody>
</table>

* Refer to Appendix A for classification of audit objective conclusions.
Executive Summary

Background

The Ohio Department of Administrative Services (DAS), Equal Opportunity Division (EOD), Business Certification and Compliance Unit conducts certification of minority-owned businesses, making them eligible to participate in the state's socially and economically disadvantaged business initiative programs. The Minority Business Enterprise (MBE) program is designed to assist minority businesses in obtaining state government contracts for goods and services. Companies eligible for MBE certification must be owned and controlled (a minimum of 51% ownership) and a member of one of the following minority groups: Black or African American, American Indian, Hispanic or Latino, or Asian. Approximately 1,400 companies are certified as MBE vendors. Pursuant to ORC 125.081, the MBE program establishes a 15 percent set-aside procurement goal for state agencies, boards, and commissions in awarding contracts to certified MBE businesses.

During the audit, OIA identified opportunities for DAS to strengthen internal controls and improve business operations. OIA conforms with the International Standards for the Professional Practice of Internal Auditing. OIA would like to thank DAS staff and management for their cooperation and time in support of this audit.

This report is solely intended for the information and use of agency management and the State Audit Committee. It is not intended for anyone other than these specified parties.

Scope and Objectives

OIA staff was engaged to perform an assurance audit related to the controls over the agency's MBE Certification process. This work was completed December 2018 through March 2019. The following summarizes the objectives of the review:

- Evaluate the design and effectiveness of controls for certifying minority-owned businesses and ensuring businesses' compliance with MBE requirements.
- Evaluate the design and effectiveness of controls for re-certifying minority-owned businesses and ensuring businesses' compliance with MBE requirements.

Detailed Observations and Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. Low risk observations were discussed with individual agency management and are not part of this report. However, the low risk observations were considered as part of the audit objective conclusions.
Observation 1 – MBE Certification is not Consistently Stated in OAKS

Ohio Revised Code Section 125.081 (B) states, in part: “the agency shall set aside a number of purchases, the aggregate value of which equals approximately fifteen per cent of the aggregate value of such purchases for the current fiscal year for competition by minority business enterprises (MBE) only.” Agencies are required to submit quarterly reports to the Equal Employment Opportunity Coordinator detailing the purchases made from MBE suppliers to ensure on pace to meet the MBE purchase requirements. Agencies prepare their reports by running data from the Ohio Administrative Knowledge System (OAKS), specifying purchases with suppliers who have been certified as an MBE vendor.

MBE certification and recertification applications are reviewed and approved or denied by the DAS Equal Opportunity Division and the information is recorded in the PIMS system. DAS uses PIMS to track the status of MBE certification applications and to store company documents. Each night, PIMS interfaces with OAKS to update supplier information with changes approved in PIMS. OAKS should then state the current MBE status for all suppliers. However, from a sample of 25 MBE suppliers tested that applied for MBE recertification in 2018, for four (16%), the OAKS MBE status did not agree to PIMS.

Incorrect MBE supplier status in OAKS could lead to state agencies filing inaccurate MBE purchasing records. The risk of agencies not being compliant with MBE spending requirements increases as agencies may not receive credit for MBE purchases. Also, MBE suppliers may miss opportunities if not identified as MBE in OAKS.

Recommendation

Determine the root cause of OAKS not receiving updated MBE information from PIMS. Correct the issues identified and test the interface to verify the MBE information is properly transferred to OAKS. Test multiple types of MBE scenarios to ensure all types of transactions are properly updated in OAKS. Determine the number of suppliers that did not have MBE status updated in OAKS. Review purchases made with these suppliers to ensure agencies received the appropriate credit for MBE purchases.

Management Response

The PIMS - OAKS interface has been working as per design. However, a service ticket has been created to investigate this incident reported. Investigation involves analyzing the parameters/conditions on handshake (forward and feedback loop) between PIMS and OAKS application via the interface and finding the root cause for the lack of update of MBE status of few suppliers in OAKS application. Once the root cause is determined, next steps will be taken to apply any required code changes to avoid these kinds of errors in the future and a best approach to update the existing missing or incorrect status MBE in OAKS.
Observation 2 – Access to PIMS is not Documented

Effective business processes include documented policies and procedures addressing access to sensitive information in PIMS. This should include assigning system access to employees and periodically reviewing employees with system access for appropriateness. Management should review and update the policies and procedures to ensure they are current and relevant. Agencies should designate an employee as the authority to grant and remove system access, document the granting and removal of access, and perform periodic reviews of the employees with system access.

Companies applying for Minority Business Enterprise certification complete applications through the Ohio Business Gateway. The applications are then transmitted to the PIMS system utilized by the DAS. Companies separately submit supporting documentation. Sensitive information from the application and supporting documentation such as banking information, social security numbers, disability information and employee W-2 forms are occasionally uploaded and stored by the Compliance Officers in PIMS.

The Business Certification and Compliance Unit (BCCU) Manager within the EOD grants access and removes access to PIMS when employees enter or leave the Division. Granting and removal of access is done by email or phone call and there is no documentation of the Manager’s approval. OIA obtained a listing of current PIMS users and it presented a total of 178 individuals with system access. Since PIMS is also used by other DAS sections, users with inappropriate access could not be determined.

Lack of documentation for granting and removing system access increases the risk of employees obtaining unauthorized access to sensitive information. Lack of periodic reviews of access to sensitive information increases the risk of sensitive information being lost or stolen.

Recommendation

Review the listing of PIMS users and limit access to companies’ sensitive information in PIMS to employees that need access to sensitive data to perform job duties. Implement a formal approval process for granting and removing access to PIMS and document the approvals to grant or remove system access. Implement periodic reviews of the assigned user access to ensure the employees assigned access require continued access to perform job duties. Remove employees’ access if no longer needed to perform job duties. Periodically review procedures developed to determine if effectively ensuring the safety of the sensitive information maintained in PIMS and update procedures as necessary to reflect current operations.
Management Response

All EOD users in PIMS application have either one of the three EOD specific roles based on the application module(s) they need access to and also on their authority or permissions to read, update or delete data in the application. PIMS application is highly robust in security and users’ access is controlled to very finer level. Only EOD users have access to EOD modules of the PIMS application. The process for adding and removing users is done through a service ticket requested by Application Owner(s), EOD Director or designee. Appropriate application Service Owner(s)’s team members upon receiving the service ticket, creates/remove users in the application and assigns necessary roles. New users login to the application using the temporary password provided. The application prompts the new user to change the password immediately following the first successful login. Permissions are revoked on users deemed to be removed.

Quarterly, DAS Application Services Team will submit to the Application Owner(s), EOD Director or designee a listing of all individuals and their security role for review, modification, or deletion.

<table>
<thead>
<tr>
<th>Risk*</th>
<th>Remediation Owner</th>
<th>Estimated Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>EOD Director/Application Owner</td>
<td>May 1, 2019</td>
</tr>
</tbody>
</table>

Observation 3 – MBE Certification Applications not Processed Timely

Businesses wishing to participate in the MBE program should expect their applications to be processed in a reasonable timeframe to allow the business to be made available to state agencies seeking to purchase from MBE businesses. Per Ohio Administrative Code Section 123:2-15-01(B)(1), businesses are required to “submit their application 30 days prior to bids being open”, allowing DAS time to process the applications. If all required documents are not submitted timely, DAS is required to administratively close or disapprove the application. A well-designed process includes establishing deadlines for processing applications and handling/documenting delays affecting processing applications.

To monitor application processing timeliness, DAS Compliance Officers monitor the status of applications utilizing dashboards in PIMS. Weekly, Team Leaders review status reports to determine the status of outstanding applications. DAS has established 100 days from receipt of the application to be a reasonable amount of time to complete application processing. From a sample of 25 MBE company applications received by DAS in 2018, eight (32%) were not processed within the reasonable time established. The applications not processed in a timely manner ranged from 100 days to 262 (average of 143) days. No documentation exists in the companies’ PIMS account or hard copy files to indicate whether the delay was due to the
applicant not supplying the required information, difficulties scheduling on-site reviews, or internal DAS delays.

Ineffective controls to process applications in a timely manner increases the risk companies will not be available to state agencies looking to purchase from MBE vendors. Additionally, company information received early in the process may lose relevancy during the application processing period if not processed timely.

**Recommendation**

Consider the following when monitoring in-progress applications:

- Develop and implement procedures to ensure the Compliance Officers address document submissions in a timely manner, issue missing documents letters to the companies when required documents are not received, and reject applications when documents are not received;
- Reassign applications early in the process if it is determined a Compliance Officer has a disproportionately large workload; and
- Establish, monitor, and enforce deadlines for Compliance Officers to complete reviews of applications received.

Document the status of processing applications in PIMS and/or the applicants’ files, including letters sent to the applicant and/or received from the applicant, phone calls to the applicant, completion of steps within the review process, and reviews performed by Team Leaders.

**Management Response**

The MBE Certification Workflow Diagram indicates that when an application is received the team leader contacts the applicant by telephone and explains the certification process. In addition, an email is sent to the applicant indicating that the applicant has thirty days to submit required documents. If documents are not received within 30 days, the application is “Administratively Closed”. If documents are received within thirty-days but are incomplete the assigned officer sends a registered letter to the applicant outlining the missing documents and allows the applicant 14 days to submit the documents. If the documents are not submitted within the required time period, a 119 Hearing Letter is issued to the applicant and the application is disapproved.

**Corrective Action:** EOD will update the MBE Certification Workflow Diagram to include a requirement that the officer enters into the PIMS application Comment Section a status update response monthly for any application exceeding 100 days in progress. EOD will retrain all officers and team leaders of the new documentation requirements and the importance of closing applications immediately after 30 days have expired and required documents have not been submitted.
Weekly, the EEO program manager sends the team leaders a listing of all applications “In Progress” and the number of days since the submission of the application. Applications between 60 to 90 days “In Progress” are indicated as Yellow. Applications over 100 days “In Progress” are indicated as “Red” with a required completion date of the following week, if possible.

**Corrective Action:** EOD will update its Policy and Procedure Manual to require team leaders to update the Comment Section of the PIMS application after the weekly application status meeting indicating the reasons why the application is exceeding 100 days “In Progress” status and set a due date for completion or reassignment due to excessive workload.

All applications “In Progress” status will continue to be monitored weekly by the EEO program manager to ensure compliance and proper documentation pertaining to the status of the application based on time “In Progress”.

<table>
<thead>
<tr>
<th>Risk*</th>
<th>Remediation Owner</th>
<th>Estimated Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>EOD MBE Program Manager</td>
<td>April 15, 2019</td>
</tr>
</tbody>
</table>

Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the observations and recommendations suggested above. However, these observations reflect our continuing desire to assist your department in achieving improvements in internal controls, compliance, and operational efficiencies.

* Refer to Appendix A for classification of audit observations.
### Appendix A – Classification of Conclusions and Observations

#### Classification of Audit Objective Conclusions

<table>
<thead>
<tr>
<th>Conclusion</th>
<th>Description of Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well-Controlled</td>
<td>The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor.</td>
</tr>
<tr>
<td>Well-Controlled with Improvement Needed</td>
<td>The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.</td>
</tr>
<tr>
<td>Improvement Needed</td>
<td>Weaknesses are present that compromise achievement of one or more control objectives but do not prevent the process from achieving its overall purpose. While important weaknesses exist, their impact is not widespread.</td>
</tr>
<tr>
<td>Major Improvement Needed</td>
<td>Weaknesses are present that could potentially compromise achievement of its overall purpose. The impact of weaknesses on management of risks is widespread due to the number or nature of the weaknesses.</td>
</tr>
</tbody>
</table>

#### Classification of Audit Observations

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description of Factors</th>
<th>Reporting Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity.</td>
<td>Agency Management; State Audit Committee (Not reported)</td>
</tr>
<tr>
<td>Moderate</td>
<td>Observation has moderate impact to the agency. Exposure may be significant to unit within an agency, but not to the agency as a whole. Compensating controls may exist but are not operating as designed. Requires near-term agency attention.</td>
<td>Agency Management and State Audit Committee</td>
</tr>
<tr>
<td>High</td>
<td>Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation.</td>
<td>Agency Management and State Audit Committee</td>
</tr>
</tbody>
</table>