OBM | Office of Internal Audit

# Department of Education
# Teaching Licensure Audit

**Audit Period: January through December 2017**

## Results Summary:

| Objective | Conclusion |
|---|---|
| **Licensure Issuance** | **Well-Controlled with Improvement Needed** |

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

**Report number: 2018-ODE-02** **Issuance date: April 19, 2018**

# Executive Summary

## Background

The Ohio Department of Education (ODE) oversees a public education system consisting of 610 public school districts, 49 joint vocational school districts (JVSDs), and approximately 370 public community schools. ODE administers the school funding system, collects school fiscal and performance data, develops academic standards and model curricula, administers the state achievement tests, issues district and school report cards, administers Ohio's school choice programs, provides professional development, and licenses teachers, administrators, treasurers, superintendents, and other education personnel.

As of March 2017, there were approximately 318,000 licensed educators in Ohio. Educators include teachers, principals, superintendents and other persons serving schools (e.g. school nurses, coaches, substitute teachers, treasurers, etc.). The educator licensing process was fully implemented to an online application effective January 2014. There are 22 educator license categories with approximately 149,000 licensure applications processed in calendar year 2017.

During the audit, OIA identified opportunities for ODE 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 ODE 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 licensure processes. This work was completed December 2017 through March 2018. The scope of this audit included the following areas for the period of January through December 2017:

Key Licensure Processes to include:

- Teaching
- Administrator
- Coach
- Pupil Services
- Aides

The objective of the engagement was to evaluate the design and effectiveness of controls for license issuance

# 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 – Lack of CPI Monitoring and Inappropriate Access

Ohio Revised Code 1347.15(B)(6) requires state agencies to "notify each person whose confidential personal information (CPI) has been accessed for an invalid reason by employees of the state agency." Therefore, agencies must perform periodic and timely monitoring of accesses made to CPI and access controls to systems to prevent or detect unauthorized access. Policies must be kept up-to-date to reflect necessary rules or laws.

Ohio Department of Education (ODE) maintains an information security and data protection and privacy policy, Policy ISP-007-Data Protection and Privacy, which states that CPI may only be collected, stored, processed or accessed if necessary for legitimate reasons, the person accessing the information is authorized to do so and the access does not violate any Ohio Administrative Code rules, state or federal laws, or any agency policies. ISP-007 also requires information owners to develop a process to regularly review access to systems or files for unauthorized access and to ensure information is handled according to the policy. Per the policy, an information owner is an ODE manager or executive who determines the purpose for processing personal data and who makes decisions about the security mechanisms to be used to protect such data. However, ODE has not updated the policy since March 2011 and it references rescinded Ohio Administrative Code sections. The policy also indicates that the next policy review was scheduled for July 31, 2015.

ODE Office of Educator Licensure (OEL) does not have a policy or developed process to address CPI monitoring of staff to ensure CPI is not accessed for non-business related purposes. OEL does not require its staff to leave comments to document access purposes in the licensure system, Connected Ohio Record for Educators (CORE), if accounts are accessed for purposes other than approving credentials.

Additionally, OEL has no process to regularly review user access to CORE and user access was most recently reviewed in 2015.

OIA obtained a listing of CORE users, as of February 2018, with final credential approval authority from ODE IT and noted the following:

- One of 12 (8%) users with the "CE Consultant Role-User" is not an active employee.

- One of 18 (6%) users with the "PC Intake Officer Role-User" is not an active employee.

According to OEL, these users were never ODE employees and never accessed the system. OEL is in the process of revoking access rights to both users.

Lack of CPI and user role access monitoring increases the likelihood of noncompliance with statutory requirements and may result in misuse or unauthorized access to CPI without timely detection which may negatively impact the agency's reputation. Outdated policies may weaken the control environment and result in a breakdown in the control structure. Not requiring users to add comments to CORE when accounts are accessed makes it difficult for management to determine if access is for business-related purposes. Additionally, from a customer service perspective, lack of comments may delay application processing as it does not allow staff to know who has spoken with the applicant(s) in the past and reasons for contacts.

**Recommendation**

Create and implement a formal CPI monitoring procedure to detail procedures to complete reviews, documentation to review, review frequency, responsibilities for conducting reviews, and supporting documentation to maintain as evidence of review completion. System reports, where possible, should be utilized to determine if CPI was accessed outside of normal business hours (i.e. after hours, weekends, holidays), which may indicate inappropriate access.

Require OEL staff to add comments in CORE any time accounts are accessed to explain the purpose and to help create an audit trail of all instances of CPI access. Such comments would not be necessary if OEL staff is performing a review to issue or renew a credential, as documentation of the review is already maintained in CORE. However, if a license was previously declined, and OEL subsequently determines the license may be issued, comments should explain the rationale.

Create and implement a formal and regular CORE user access monitoring procedure to detail review requirements, the frequency and timing of the reviews, and documentation to maintain to support completion of reviews. Obtain system-generated user role listings for those users with view and edit abilities and compare users to an active employee directory. Access should be limited to the information needed to perform assigned job duties. Terminate any inappropriate or unauthorized access rights. At least annually, and more frequently as needed, review CORE user access to ensure access rights are promptly removed when no longer needed and to validate that only authorized employees have appropriate access.

Finally, review and update Policy ISP-007 to ensure all referenced Ohio Administrative Code sections and other information is relevant.

**Management Response**

The Office of Educator Licensure (OEL) will work to document a formal CPI monitoring procedure as recommended. This policy will include documentation and means of compliance with Ohio Revised Code (ORC) section 1347.15, Access Rules for Confidential Personal Information and applicable department policies. Access to the online licensure application system, Connected Ohio Records for Educators (CORE) is currently through an individual's Security Application For Enterprise (SAFE) account. SAFE monitors and log dates and times of access by users. The policy will include quarterly reviews of SAFE log-ins, to be overseen by the SAFE Project Manager, or designee, to ensure that CPI is being accessed in accordance with Department policy and only for business related purposes. In response to the quarterly review, the SAFE Project Manager will provide a summary to the Director of the Office of Educator Licensure, or designee, and the department's Privacy Officer detailing whether or not CPI was accessed for non-business related purposes. The Director of the Office of Educator Licensure, or designee, will review the access based on applicable SAFE user roles (i.e. the SAFE roles that can access CPI). If CPI has been accessed for non-business related purposes, the OEL Director or designee will work with the Office of Legal Counsel to comply with ORC section 1347.15(B)(6).

OEL will request that part of the CORE 4 internal upgrade allow for the licensure specialists to add comments in CORE when accounts are accessed to explain the reason, however this would not include comments related to the review of licensure applications for the purposes of issuance or renewal.

Regarding reviewing user access to CORE, OEL will document the following procedures into an office policy, and begin reviewing user access quarterly. A summary of the current process is below:

Currently, SAFE role requests are being managed through the ODE IT Service Desk. Any ODE employee or contractor with a SAFE account can initiate a request to add a SAFE role to his/her account. Initially, the request needs to be approved by the user's immediate supervisor. After the supervisory approval, the request is forwarded to the business owner for that IT system (or role). Once the business owner approves the request, the SAFE role is added to the user account. At any point of time, either the supervisor or business owner can reject the request. A supervisor may initiate a request on behalf of his/her direct reports. In that case, no supervisory approval is needed. The Assistant Director of the Office of Educator Licensure is listed as the business owner for user roles in CORE.

In order to ensure that user access has been terminated for employees that have separated from the Department, OEL will document the following procedure into an office policy, and begin reviewing user access quarterly. A user can request deletion of SAFE roles through initiating a request with the ODE IT Service Desk. A supervisor can also remove a role for one of his/her direct reports also through initiating a request with the ODE IT Service Desk. During employee

| | | |
|---|---|---|
| separation, supervisors will remove any SAFE role that is assigned to that staff on the last day of their employment with the Department. | | |
| **Risk*** | **Remediation Owner** | **Estimated Completion Date** |
| **Moderate** | Director, Office of Educator Licensure | October 2018 |

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.

# Appendix A – Classification of Conclusions and Observations

## Classification of Audit Objective Conclusions

| Conclusion | Description of Factors |
|---|---|
| **Well-Controlled** | The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor. |
| **Well-Controlled with Improvement Needed** | The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives. |
| **Improvement Needed** | 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. |
| **Major Improvement Needed** | 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. |

## Classification of Audit Observations

| Rating | Description of Factors | Reporting Level |
|---|---|---|
| **Low** | Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity. | Agency Management; State Audit Committee (Not reported) |
| **Moderate** | 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. | Agency Management and State Audit Committee |
| **High** | Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation. | Agency Management and State Audit Committee |