STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

LINDSEY PERRY, CPA, CFE
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

September 21, 2018

The Honorable Anthony Kern, Chair
Joint Legislative Audit Committee

The Honorable Bob Worsley, Vice Chair
Joint Legislative Audit Committee

Dear Representative Kern and Senator Worsley:

Our Office has recently completed an initial followup of the Arizona Commission for Postsecondary Education regarding the implementation status of the 28 audit recommendations (including sub-parts of the recommendations) presented in the performance audit report released in December 2017 (Auditor General Report 17-113). As the attached grid indicates:

- 5 have been implemented;
- 1 has been implemented in a different manner;
- 11 are in the process of being implemented; and
- 11 have not been implemented.

Our Office will conduct an 18-month followup with the Commission on the status of those recommendations that have not yet been fully implemented.

Sincerely,
Dale Chapman, Director
Performance Audit Division

cc: Dr. April L. Osborn, Executive Director
Arizona Commission for Postsecondary Education

Arizona Commission for Postsecondary Education members

Arizona Family College Savings Program Oversight Committee members

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

Arizona Commission for Postsecondary Education
Auditor General Report 17-113
Initial Follow-Up Report

Recommendation	Status/Additional Explanation
Finding 1: Commission and Oversight Committee should further strengthen 529 program oversight	
1.1 The Oversight Committee should review its rating categories and subcategories and determine where additional descriptions of expected performance or measurable standards would be appropriate, and then modify its rating instrument and/or rating guidance accordingly.	**Implementation in process** In March 2018, commission staff provided the Oversight Committee with information from the Commission's investment consultant that may help oversight committee members better define rating categories and expected performance for the 529 program providers. In March and May 2018, the Oversight Committee discussed how it rates the 529 program providers and asked commission staff to provide further information regarding how 529 plans in other states rate providers. As of August 2018, commission staff reported that they are gathering this information for the Oversight Committee members.
1.2 The Commission should develop and implement policies and procedures for regularly assessing, evaluating, and modifying the types of information that the Oversight Committee receives as part of the annual performance review. As part of this process, commission staff should continue to solicit feedback from the Oversight Committee to determine what information would be most useful for its review.	**Implementation in process** The Commission has drafted a policy for its annual performance review process that directs commission staff to continuously solicit feedback from the Oversight Committee to determine what information would be most useful for its annual performance review of the 529 program providers. In addition, the Commission reported that by the end of September 2018, it plans to develop and implement more specific procedures for staff to regularly assess, evaluate, and modify the types of information it provides to the Oversight Committee for the annual performance review.
1.3 The Commission should ensure that all provider contracts include provisions that require the providers to participate in an annual performance review and to provide commission staff with performance review reports that contain specified information.	**Not implemented** The Commission reported that it will make all audit recommendation additions to the provider contracts when the contracts are due for renewal in 2020 and 2021, or sooner if another business need arises and requires a contract amendment. Until that time, the Commission indicated that it anticipates the 529 program providers will continue to actively participate in the annual performance review process and provide annual performance review reports, although the providers are not contractually obligated to do so.
1.4 The Commission should continue implementing its procedures for verifying that providers have paid the Commission the fee amounts specified in their contracts.	**Implemented at 6 months**

Recommendation	Status/Additional Explanation
1.5 The Commission should continue to implement its procedures for reviewing the account balances of 529 beneficiaries on a quarterly basis and further modify its written procedures to designate staff responsible for this task.	**Implemented at 6 months**
Finding 2: Commission should take steps to better protect confidential and sensitive electronic data	
2.1 The Commission should limit staff access to only the confidential and sensitive electronic data needed for their job duties by:	
a. Completing its shared drive organization project, including assessing the structure and content of the shared drive, identifying any duplicate content, and removing any unnecessary documents;	**Implementation in process** The Commission has completed some steps in its shared drive organization project, including assessing the structure and content of the shared drive. The Commission reported that it plans to complete the project, including removing duplicate files and implementing the new structure, by June 2019.
b. Developing and implementing procedures for protecting its electronic data based on the level of risk associated with the data, including classifying the data as confidential or public, and developing a data classification inventory that is updated regularly;	**Not implemented** The Commission indicated that it is researching and reviewing state-wide policies and best practices for protecting and classifying data; however, it has not yet developed or implemented risk-based procedures for classifying and protecting its data.
c. Reviewing staff duties to determine the access staff need to confidential and sensitive electronic data, including access to electronic data from prior years that is not needed for current work; and	**Implementation in process** The Commission has reviewed staff duties and determined which staff need access to the various types of data on the shared drive. However, the Commission has yet to determine how data from prior years will be assessed and classified and stated that it anticipates starting to classify all of its data in February 2019.
d. Limiting staff access to confidential and sensitive electronic data based on the results of this review and working with ABOR to implement this access.	**Not implemented** See explanation for Recommendation 2.1c.

Recommendation	Status/Additional Explanation
2.2 The Commission should develop a formal contract or SLA with ABOR, in accordance with IT best practices and standards for vendor management, that specifies the level of IT services ABOR will provide the Commission. This contract or SLA should include requirements for:	
a. Terminating the network server access of former employees in a timely manner;	**Implementation in process** As of August 2018, the Commission had not yet developed a formal contract or Service Level Agreement (SLA) for IT services. According to the Commission, it is researching options for obtaining its IT services through an interagency agreement with ABOR or the Arizona Department of Administration and plans to select an IT services provider by June 2019. In the meantime, the Commission has developed procedures for how it will work with ABOR to terminate IT access of commission staff leaving employment with the Commission by the end of day on the final day of employment.
b. Adequately protecting passwords that provide access to the 529 data stored on ABOR's network servers by more frequently resetting passwords and storing them only in unobservable locations;	**Implementation in process** As indicated in the explanation for Recommendation 2.2a, the Commission has yet to develop a formal contract or SLA for IT services. However, the Commission has established a procedure for resetting passwords that provide access to the 529 data on ABOR's network server every 6 months. Auditors observed that these passwords have been changed at least once in the past 6 months and that passwords were no longer stored in observable locations. Auditors will assess continued implementation of the recommendation at the 18-month followup.
c. Establishing a process for working with ABOR's IT staff for password retrieval if commission staff lose or forget passwords that allow access to the shared drive; and	**Implemented in a different manner at 6 months** The Commission developed an automated procedure for retrieving passwords if commission staff lose or forget their passwords that does not rely on ABOR IT staff.
d. Developing and implementing a contingency plan for the electronic data stored at ABOR that includes requirements for saving backup copies off-site and testing backup copies more frequently.	**Not implemented** As indicated in the explanation for recommendation 2.2a, the Commission has yet to develop a contract or SLA with ABOR that requires ABOR to develop a contingency plan such as saving backup copies of data off-site.

Recommendation	Status/Additional Explanation
2.3 The Commission should develop and implement time frames for when it will notify ABOR's IT administrator to terminate former employee access and a procedure for requesting that passwords be reset.	**Implementation in process** The Commission developed an internal time frame for resetting passwords and for notifying ABOR's IT administrator prior to the employee leaving so that ABOR can terminate the former employee's access by end of day on the employee's last day. Additionally, the Commission had reset employee passwords at least once in the previous 6-month period. However, as of August 2018, auditors had identified one person who had not worked for the Commission in over 1 year who still had an active password. According to the Commission, it will work with ABOR to remove this person's access to the network server. Auditors will assess continued implementation of this recommendation at the 18-month followup.
2.4 The Commission should discontinue its practice of saving a list of commission staff passwords that is accessible to multiple staff.	**Not implemented** Although the Commission has limited access to its list of commission staff passwords to only its business manager, the Commission has not discontinued its practice of saving this list.
2.5 The Commission should continue with its plans to:	
a. Modify its AzGrants portal contract to require the contractor to submit a SOC or other IT security audit report annually to provide the Commission with assurance that its confidential and sensitive electronic data is safe;	**Implemented at 6 months**
b. Implement a procedure for reviewing the IT security audit information including following up on any IT security concerns identified; and	**Implementation in process** The Commission has begun to implement procedures for reviewing the IT security audit information it receives annually from the AzGrants portal contractor. For example, in January 2018, the Commission reviewed the results of the contractor's annual SOC report, and in June 2018, commission staff confirmed with the contractor that issues the SOC report identified were resolved. However, the procedures do not require commission staff to obtain evidence that its contractor adequately addressed the identified issues and lacks time frames for when it will request that information.
c. Amend its contract to require the AzGrants portal contractor to periodically submit evidence that it is complying with the IT security requirements specified in the contract, such as providing documentation of backing up the data weekly.	**Implemented at 6 months**

Recommendation	Status/Additional Explanation
Sunset Factor #2: The extent to which the Commission has met its statutory objective and purpose and the efficiency with which it has operated.	
1. The Commission should revise and then implement its newly revised cash-handling procedures to:	
a. Require appropriate segregation of duties, including guidance that mail should always be opened with two staff present, that mail should not be opened by the same person who will prepare and make the deposit, and that the electronic mail log should be restricted to only those staff who enter cash receipts into this log;	**Not implemented** Although the Commission has updated some of its cash-handling procedures, including suggesting that two staff be present to open money orders, the updated procedures do not include several other important steps. Specifically, the updated procedures do not require that mail should be opened only with two staff present and not by the same person who will prepare and make the deposit; that the electronic mail log should be restricted to only staff who enter cash receipts into the log; that cash deposits will be made on the day of collection or, when this is not practical, at the end of the business day after monies total $1,000 or more; and do not provide guidance for limiting access to the safe to only those individuals who need it for their job duties.
b. Require that cash deposits be made on the day of collection or, when deposit on the day of collection is impractical, at the end of the business day after monies total $1,000 or more; and	**Not implemented** See explanation for Sunset Factor 2, Recommendation 1a.
c. Include guidance for limiting access to the safe to only those staff who need access for their job duties.	**Not implemented** See explanation for Sunset Factor 2, Recommendation 1a.
2. The Commission should train staff on cash-handling procedures as needed.	**Not implemented** As indicated in the explanation for Sunset Factor 2, Recommendation 1a, the Commission has not made several important updates to its cash-handling procedures. In addition, although it has made some changes to its procedures, the Commission did not provide evidence that it has trained its staff on its existing cash-handling procedures.
3. The Commission should continue to develop and implement written policies and procedures that fully address all aspects of processing loan repayments.	**Not implemented** The Commission indicated that it relies on the student loan repayment procedures manual it developed during the audit to process loan repayments. However, the Commission has not updated these procedures to include all aspects of processing loan repayments, such as specifying the appropriate time frame for repayment and how to calculate interest, if interest has accrued.

Recommendation	Status/Additional Explanation
4. The Commission should implement its new AzLEAP procedures for auditing participating postsecondary institutions' student records to help ensure that eligible students received the reported disbursement of AzLEAP program awards.	**Implementation in process** The Commission has taken steps to begin auditing postsecondary institutions that participate in the AzLEAP program, such as determining the number of student records it will audit from each participating postsecondary institution based on the number of recipients at the school and drafting a form letter for notifying participating postsecondary institutions that the Commission is initiating an audit of their student records. However, the Commission indicated that it had not identified a secure method for transmitting the electronic student record data between participating AzLEAP institutions and the Commission and as of August 31, 2018, had yet to start performing audits. The Commission reported that it expects to have determined a secure method for transmitting data sometime in fall 2018.
5. The Commission should work with its Assistant Attorney General to determine whether and when it can make rule changes necessary to update its rules for AzLEAP oversight, including seeking to eliminate any rules that are no longer necessary.	**Implementation in process** The Commission reported that it has consulted with the Attorney General's Office and plans to request an exemption from the rule moratorium to eliminate any unnecessary rules. However, the Commission does not plan to make this request until fall 2019 in order to allow commission staff time to more fully review the rules and identify needed updates for AzLEAP program rules.
Sunset Factor #4: The extent to which rules adopted by the Commission are consistent with the legislative mandate.	
6. The Commission should work with its Assistant Attorney General to determine whether and when it can make rule changes necessary to update its rules for the 529 program, including eliminating rules that are no longer necessary.	**Implementation in process** The Commission reported that it has consulted with the Attorney General's Office and plans to request an exemption from the rule moratorium to update its rules for the 529 program. However, the Commission does not plan to make this request until fall 2019 in order to allow commission staff time to fully review its 529 program rules and identify needed updates.
Sunset Factor #5: The extent to which the Commission has encouraged input from the public before adopting its rules and the extent to which it has informed the public as to its actions and their expected impact on the public.	
7. The Commission should continue to implement its newly revised procedures to ensure that meeting minutes are provided to the public within 3 working days as required by open meeting law.	**Implemented at 6 months**

Recommendation	Status/Additional Explanation
Sunset Factor #9: The extent to which changes are necessary in the laws of the Commission to adequately comply with the factors listed in this sunset law.	
8. The Commission should consult with its Assistant Attorney General to determine the applicability of A.R.S. §15-1852(B)(6), and to make recommendations to the Legislature to eliminate the statute if it is not applicable to the Commission's functions.	**Not implemented** The Commission indicated that it plans to introduce statutory language to remove A.R.S. §15-1852(B)(6) during the 2019 legislative session.