ARIZONA Auditor General
Making a Positive Difference

# Arizona Commission for Postsecondary Education
## 36-Month Follow-Up Report

The December 2017 Arizona Commission for Postsecondary Education performance audit and sunset review found that the Commission should further strengthen Arizona Family College Savings Program (529 Program) oversight and better protect its confidential and sensitive electronic data. The Commission's status in implementing the recommendations is as follows:

## Status of 28 recommendations

| | |
|---|---|
| Implemented: | 10 |
| Implemented in a different manner: | 1 |
| In process of being implemented: | 4 |
| No longer applicable: | 11 |
| Not yet applicable: | 1 |
| **Not implemented:** | **1** |

Unless otherwise directed by the Joint Legislative Audit Committee, this report concludes our follow-up work on the Commission's efforts to implement the recommendations from the December 2017 report.

## 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.

**No longer applicable**—Effective September 30, 2020, Laws 2020, Ch. 88, transferred the administration, duties, and oversight for the 529 Program from the Commission to the Office of the Arizona State Treasurer. In addition, although the Commission had previously implemented Recommendations 1.2, 1.4, 1.5, and 2.2b, all recommendations associated with the 529 Program are no longer applicable because of the aforementioned change.

**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.

**No longer applicable**—See explanation for Recommendation 1.1.

**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.

**No longer applicable**—See explanation for Recommendation 1.1.

**1.4** The Commission should continue implementing its procedures for verifying that providers have paid the Commission the fee amounts specified in their contracts.

**No longer applicable**—See explanation for Recommendation 1.1.

**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.

**No longer applicable—**See explanation for Recommendation 1.1.

## 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 is continuing to implement its shared drive organization project to help ensure staff access to confidential and sensitive electronic data is appropriately limited. For example, the commission is assessing the structure and content of its data so that it can better determine whether it needs to eliminate or restrict staff access to specific data. Additionally, the Commission reported that it plans to adopt a shared drive that will have permissions set for individual staff to help ensure staff can access only the confidential and sensitive electronic data needed for their job duties.

**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;

**Implementation in process—**The Commission is in the process of implementing the data classification policy that it developed prior to our last followup. For example, as required by its data classification policy, the Commission completed a risk analysis for some of its data in 2020, including determining if data needed to be reclassified and if employee access to the data was still necessary. However, the Commission has yet to classify and inventory all its data as required by its data classification policy, but reported that it plans to do so by December 2021.

**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

**Not implemented—**Although the Commission had previously taken some steps to address this recommendation, the Commission reported that it has postponed its efforts to review and assess staff access to confidential sensitive electronic data because it has not yet classified all its data (see explanation for Recommendation 2.1b) and because of the recent changes to its responsibilities that reduced the number of Commission staff (see explanation for Recommendation 1.1). However, the Commission reported it plans to review and determine appropriate staff access to confidential and sensitive electronic data by June 2022.

**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 yet applicable—**See explanation for Recommendations 2.1a and 2.1c.

**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;

**Implemented at 24 months**

**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;

**No longer applicable—**See explanation for Recommendation 1.1.

**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.

**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.

**Implemented at 24 months**

**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.

**Implemented at 24 months**

**2.4** The Commission should discontinue its practice of saving a list of commission staff passwords that is accessible to multiple staff.

**Implemented at 24 months**

**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

**Implemented at 24 months**

**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**

## 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;

**No longer applicable—**As of November 2020, the Arizona Department of Administration's Central Services Bureau assumed cash handling responsibilities for the Commission, including opening mail. In addition, although the Commission previously implemented Recommendations 1b,1c, and 2, these recommendations are no longer applicable because of the aforementioned change.

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

**No longer applicable—**See explanation for Recommendation 1a.

c. Include guidance for limiting access to the safe to only those staff who need access for their job duties.

**No longer applicable—**See explanation for Recommendation 1a.

2. The Commission should train staff on cash-handling procedures as needed.

**No longer applicable—**See explanation for Recommendation 1a.

3. The Commission should continue to develop and implement written policies and procedures that fully address all aspects of processing loan repayments.

**Implemented at 24 months**

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—**In our previous follow-up reports, the Commission indicated that it had not performed AzLEAP audits because it had not implemented a secure method for transmitting electronic student record data between participating AzLEAP institutions and the Commission. However, it has since developed and implemented a secure method for doing so and reported that it plans to begin AzLEAP audits in June 2021.

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, in consultation with its Assistant Attorney General, is working with the Governor's Office to determine whether and when it will be granted an exemption to the rule-making moratorium to update its rules for AzLEAP oversight.

## 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.

**No longer applicable—**See explanation for Recommendation 1.1.

## 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**

## 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.

**Implemented at 24 months—**The Commission consulted with its Assistant Attorney General and concluded that A.R.S. §15-1852(B)(6) was no longer applicable. The Commission reported recommending that the Legislature eliminate the statute and the Legislature did so in 2019.