ARIZONA Auditor General
Making a Positive Difference

REPORT HIGHLIGHTS
Performance Audit
December 2017

Arizona Commission for Postsecondary Education

CONCLUSION: The Arizona Commission for Postsecondary Education (Commission) administers the Arizona Family College Savings Program (529 program), which is a tax-advantaged college savings program that allows individuals to save for future educational expenses. The Commission has a Family College Savings Program Oversight Committee (Oversight Committee), which monitors and assesses the performance of Arizona's 529 program providers (providers). The Commission also administers financial aid programs, provides information about Arizona's higher education opportunities, and leads a state-wide collaboration to increase Arizona high school students' participation in higher education. We found that the Commission and Oversight Committee should further strengthen 529 program oversight, including enhancing the annual review of 529 providers and ensuring compliance with contractual and statutory requirements. The Commission also obtains and stores confidential and sensitive data for financial aid applicants and 529 program participants. We found that the Commission should take steps to better protect confidential and sensitive electronic data by limiting unnecessary staff access to this data, strengthening its agreements with external entities that store its data and provide information technology (IT) services, and requiring IT security reports demonstrating that the data is secure.

Commission and Oversight Committee should further strengthen 529 program oversight

Arizona's 529 program offers a variety of options for investing and saving for college—A 529 program is a tax-advantaged college savings program that allows individuals to save for future educational expenses for themselves or for another beneficiary. When individuals invest in a 529 account, their investment can grow tax-free, and monies can be withdrawn tax-free if used for postsecondary educational expenses, such as tuition and books. The Commission has contracted with three providers to manage Arizona's 529 program investments, and these providers offer participants multiple ways to invest and save for future higher education costs. According to the Commission, as of June 2017, Arizona's 529 program included more than 78,000 accounts with nearly $1.2 billion in assets.

Oversight Committee monitors providers' performance but can enhance its review of providers—The Oversight Committee performs an ongoing review of Arizona's three 529 providers, including formally rating the providers on their performance during an annual performance review. In evaluating the 529 providers' performance, the Oversight Committee considers various factors, such as investment performance, customer service, and ratings published by independent companies that assess 529 providers nation-wide. However, the Oversight Committee's annual performance review could be enhanced by establishing standards or performance expectations ensuring oversight committee members receive all information needed to fully evaluate providers, and including provisions in all provider contracts that require provider participation in the annual performance review.

Commission should ensure compliance with contractual and statutory requirements—The Commission is responsible for monitoring provider contract requirements, such as ensuring accurate provider fee amounts are paid to the Commission. In addition, statute requires the Commission to review 529 beneficiary account balances quarterly to ensure contributions do not exceed the maximum account balance the Commission established. Although the Commission has not consistently ensured compliance with these requirements, during the audit, the Commission developed and implemented some procedures for monitoring these requirements and should continue with its efforts to do so.

Recommendations

The Oversight Committee should review its rating categories and determine where additional descriptions of expected performance or measurable standards would be appropriate.

The Commission should:

- Develop and implement policies and procedures for regularly assessing, evaluating, and modifying the types of information the Oversight Committee receives as part of the annual performance review;

- Ensure provider contracts require providers to participate in the annual performance review; and
- Continue to implement its procedures for verifying that providers have paid the Commission the fee amounts specified by contract, and for reviewing account balances of 529 beneficiaries.

Commission should take steps to better protect confidential and sensitive electronic data

Commission responsible for confidential and sensitive electronic data—In performing its various functions, the Commission obtains and works with confidential and sensitive electronic data. For example, commission staff check applicants' eligibility for one of its financial aid programs by verifying that applicants have filed a Free Application for Federal Student Aid (FAFSA), which contains individuals' names, addresses, social security numbers, and annual income. The Commission also stores confidential and sensitive electronic data about individuals who participate in the 529 program, including names, birthdates, 529 account numbers, and tax ID numbers. Because of the nature of the Commission's confidential and sensitive electronic data, it is a potential target for misuse or malicious attacks.

The Commission has agreements with two external entities to provide IT services to the Commission. First, the Arizona Board of Regents (ABOR) provides the Commission with a "shared drive" on which commission staff can share access to 529 program and financial aid data, and an internet-accessible network server where 529 program account data can be updated by the providers and accessed by commission staff. Second, an IT consulting company (AzGrants portal contractor) provides the AzGrants portal, a website that serves various functions such as allowing recipients of commission financial aid programs to access their award information.

Commission should better protect its confidential and sensitive electronic data—Although ABOR, the AzGrants portal contractor, and the Commission have established some safeguards to protect the Commission's confidential and sensitive electronic data, additional efforts are needed. The Commission's data is protected from external attacks or other unauthorized external access using various security measures, such as a firewall that limits network traffic to approved users, and active malware/antivirus software that helps remove and prevent malicious programs. However, the Commission has not limited staff access to only the confidential and sensitive electronic data needed for their job duties. In April 2017, the Commission initiated efforts to appropriately limit staff access, such as by removing unnecessary documents from its shared drive, and should continue with these efforts. These steps should also involve developing and implementing procedures for protecting its electronic data based on the level of risk associated with the data and then determining needed staff access to this data based on its level of risk.

In addition, the Commission should develop a formal contract with ABOR that includes data security requirements, such as terminating access to the shared drive for former employees in a timely manner and establishing time frames for changing passwords that allow access to ABOR's network server. Finally, the Commission has not required its AzGrants portal contractor to provide documentation demonstrating that it has complied with the IT security requirements specified in its contract, such as evidence of database maintenance, nor does it require that the contractor obtain an independent audit that assesses the contractor's data security measures. As of May 2017, the Commission had developed an informal agreement with the AzGrants portal contractor to obtain an annual independent audit and plans to formalize this requirement in its contract. Additionally, in November 2017, the Commission began requesting that the AzGrants portal contractor periodically submit evidence of complying with the contract's IT security requirements and should continue with its plan to formalize this requirement in its contract.

Recommendations

The Commission should:

- Limit staff access to only the confidential and sensitive electronic data needed for their job duties by continuing with its efforts to remove unnecessary documents, developing and implementing procedures for protecting its electronic data based on the level of risk associated with the data, and then determining staff access to this data;
- Develop a formal contract with ABOR that includes requirements for terminating the network server access of former employees in a timely manner and adequately protecting passwords; and
- Continue with its plans to modify its AzGrants portal contract to require the contractor to provide IT security audit reports to the Commission annually and to periodically submit evidence of complying with the contract's IT security requirements.